IIWXXX

INTERNET IDENTITY WORKSHOP 30

15 YEARS 30 EVENTS

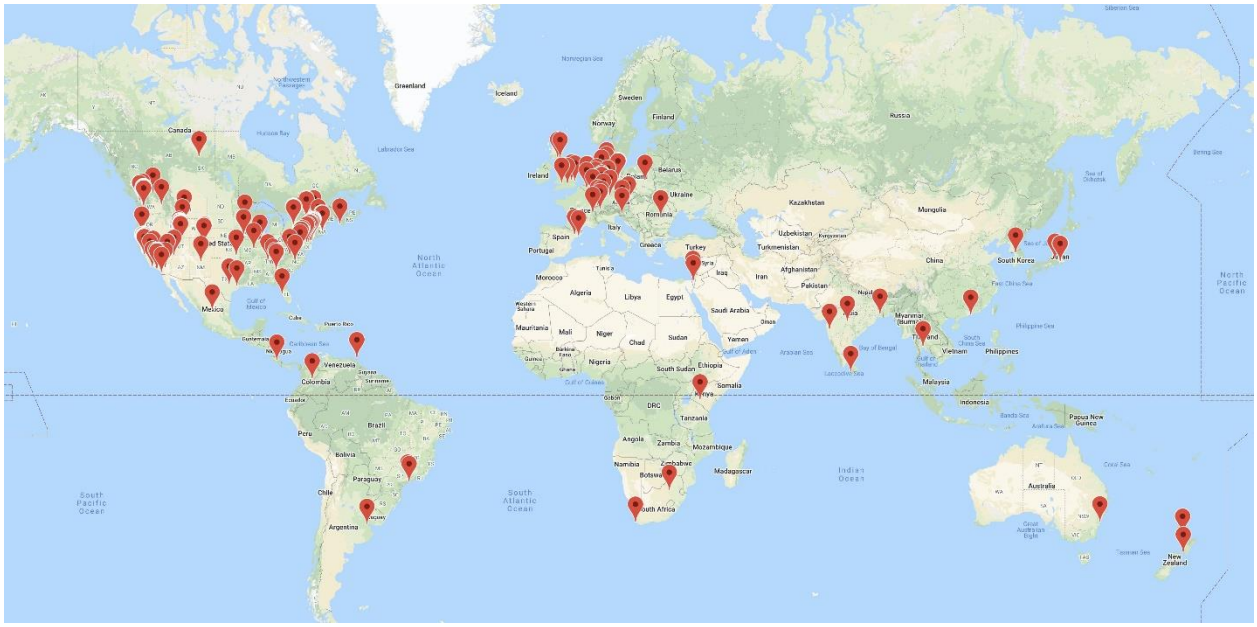
∞ ideas ∞ learning ∞ sharing ∞ surprises ∞ results ∞ solutions ∞ friendships

Book of Proceedings

www.internetidentityworkshop.com

Collected & Compiled by
LISA R. HORWITCH, HANNAH SCHULMAN and HEIDI N. SAUL

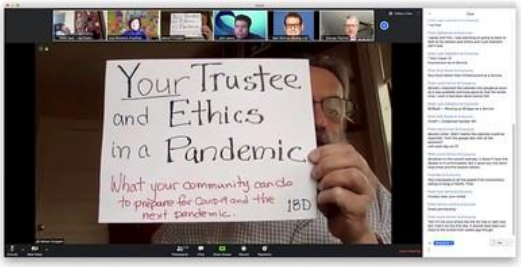
April 28,29 & 30, 2020
On Line, Near You ~ via QiqoChat



**@windley #IIW 30 underway with 330 participants from around the world.
Remarkable how well this virtual event has worked. Here's the map of attendee locations.**

IIW founded by Kaliya Young, Phil Windley and Doc Searls
Co-produced by Heidi Nobantu Saul, Phil Windley and Kaliya Young
Facilitated by Heidi Nobantu Saul, Kaliya Young, Lisa R Horwitch

REGISTER FOR IIWXXXI Online
October 20 - 22, 2020
HERE: https://iiw31.eventbrite.com



Contents

Notes in this book can also be found online at
https://iiw.idcommons.net/IIW_30_Session_Notes

Our First On Line IIW

Dear IIW Community Members,

We are pleased to announce the plan for IIWXXX in light of the Corona Virus pandemic and its impact on travel.

IIW has always been about getting things done. Missing an IIW and the important developments that are sure to happen didn't seem like an outcome anyone would be happy with. So we've been working to find a way for IIW to not just happen, but to ensure it offers opportunities for working together as it always has.

Over the past three weeks we have been developing a plan to host IIW virtually using a tool specifically designed for remote Open Space (unConference) events called Qiqo Chat (https://qiqochat.com). After reviewing the tool and how it's been used for other Open Space events, we're confident that it will allow IIWXXX to continue at the end of April with the same kinds of high-quality interactions and discussion that has been the hallmark of IIW for the past 15 years.

Over the coming few weeks, we will communicate more fully how this will work. But, we're still planning for IIWXXX to happen Apr 28-30.

- We will have an Opening Circle each day where we set the agenda,
- people will propose and host sessions, we'll hold sessions in breakout spaces,
- and after the end of sessions for the day, we'll do a Closing Circle—just like we always do.
- We will still hold Demo Sessions and the Tech Sandbox.
- We will still publish the Book of Proceedings with notes from all the sessions.
- And, since we can't have a celebratory cake, we're planning on a Commemorative T-shirt for everyone that is included as part of registering.
- We won't have Rich, our favorite barista, or a snack table, but we will still have the same high-quality discussions and working sessions that make IIW a unique event.

We're excited to try IIW in a new way and open it up to new people who might not have come otherwise. Our theme for IIW XXX is

15 Years
30 Events
∞ Friendships

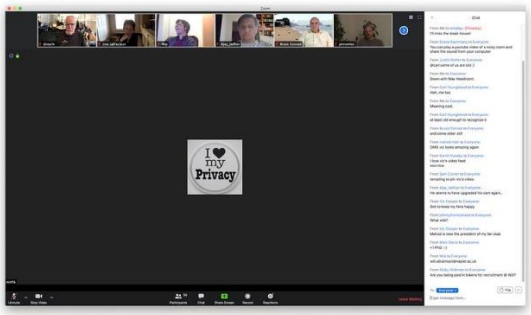
Because of those friendships, we're confident that the IIW community will come together and make the 30th IIW the best ever.

Thank you!
Kaliya, Heidi, Doc, and Phil

At IIW Online You Can….

Though we lost some of our favorite parts of meeting together at the Computer History Museum there are many things you can do at an online IIW:

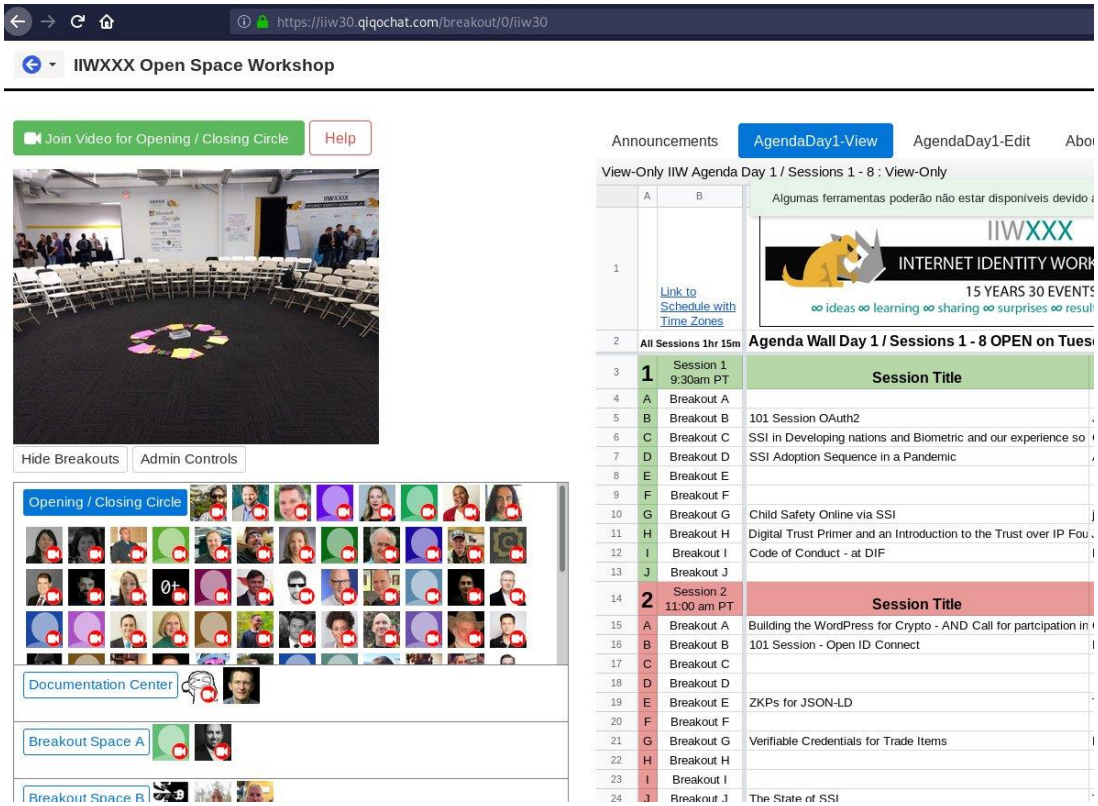
Choose Your Environment!



Be Private

Bring Your Pet!

Craft your cocktail & enjoy It when it's Cocktail Hour where You are!



Geovane Fedrechesk @geonnave
Super excited to be participating in my first @idworkshop which has just started.
Literally an opening circle in a global event.

About IIW

The Internet Identity Workshop (IIW) was founded in the fall of 2005 by Phil Windley, Doc Searls and Kaliya Young. It has been a leading space of innovation and collaboration amongst the diverse community working on user-centric identity.

It has been one of the most effective venues for promoting and developing Web-site independent identity systems like OpenID, OAuth, and Information Cards. Past IIW events have proven to be an effective tool for building community in the Internet identity space as well as to get actual work accomplished.

The event has a unique format – the agenda is created live each day of the event. This allows for the discussion of key issues, projects and a lot of interactive opportunities with key industry leaders that are in step with this fast-paced arena.

Watch this short documentary film: ***"Not Just Who They Say We Are: Claiming our Identity on the Internet"*** http://bit.ly/IIWMovie to learn about the work that has happened over the first 12 years at IIW.

The event is now in its 15th year and is Co-produced by Phil Windley, Heidi Nobantu Saul and Kaliya Young. IIWXXXI (#31) will be October 20 - 22, 2020 online on the QiqoChat platform.

Upcoming IIW Events

IIWXXXI #31
October 20 - 22, 2020
REGISTER HERE

IIWXXXII #32
Spring 2021

IIW Events would not be possible without the community that gathers or the Sponsors that make the gathering feasible. If you are interested in becoming a sponsor or know of anyone who might be please contact Phil Windley at Phil@windley.org for Event and Sponsorship opportunities information.

Thank You! Documentation Center & Book of Proceedings Sponsors JOLOCOM and Google

JOLOCOM

@GETJolocom

Google

Google

IIWXXX 3 Day Global Schedule

This page shows the times that each session will begin in your part of the world. Sessions are scheduled to be 1 hour and 15 minutes with a 15 minute break in-between each session. There is no scheduled lunch hour.

BST..... British Summer Time
WAT..... West Africa Time
CEST...Central European Summer Time
CAT..... Central African Time
EEST...Eastern European Summer Time
AEST..... Australian Eastern Standard Time
EAT..... Eastern African Time
IST..... Indian Standard Time
ICT.....Indochina Time
JST..... Japan Standard Time
NZST..New Zealand Standard Time

CONFERENCE 3 days	ALL SESSIONS 1 Hr. 15 min.	AMERICAS	EU/AFR/ISC	ASIA/PACIFIC	BREAKOUT SESSIONS TO JOIN (You can list the sessions you're hosting or attending below)
TUESDAY April 28	GRAND OPENING	PST 8:00 A.M. - 9:00 A.M.	BST/WAT 16:00	ICT 22:00	
		MST 9:00	CEST/CAT 17:00	JST 0:00	
		CST 10:00	EEST/EAT 18:00	AEST 1:00	
		EST 11:00	IST 20:30	NZST 4:00	
	SESSION 1	PST 9:30 A.M. - 10:45 A.M.	BST/WAT 17:30	ICT 23:00	
		MST 10:30	CEST/CAT 18:30	JST 1:30	
		CST 11:30	EEST/EAT 19:30	AEST 2:30	
		EST 12:30	IST 22:00	NZST 5:30	
	SESSION 2	PST 11:00 A.M. - 12:15 P.M.	BST/WAT 19:00	ICT 1:00:00	
		MST 12:00	CEST/CAT 20:00	JST 3:00	
		CST 13:00	EEST/EAT 21:00	AEST 4:00	
		EST 14:00	IST 23:30	NZST 7:00	
	SESSION 3	PST 12:30 P.M. - 1:45 P.M.	BST/WAT 20:30	ICT 2:30	
		MST 13:30	CEST/CAT 21:30	JST 4:30	
		CST 14:30	EEST/EAT 22:30	AEST 5:30	
		EST 15:30	IST 1:00	NZST 8:30	
	SESSION 4	PST 2:00 P.M. - 3:15 P.M.	BST/WAT 22:00	ICT 4:00	
		MST 15:00	CEST/CAT 23:00	JST 6:00	
		CST 16:00	EEST/EAT 0:00	AEST 7:00	
		EST 17:00	IST 2:30	NZST 10:00	
	DEMO HOUR Americas & Alsa	PST 3:30 P.M. - 4:30 P.M.	BST/WAT 23:30	ICT 5:30	
		MST 16:30	CEST/CAT 0:30	JST 7:30	
		CST 17:30	EEST/EAT 1:30	AEST 8:30	
		EST 18:30	IST 4:00	NZST 11:30	
	CLOSING Open Gifting OPENING	PST 4:30 P.M. - 5:30 P.M.	BST/WAT 1:00	ICT 7:00	
		MST 17:00	CEST/CAT 2:00	JST 9:00	
		CST 18:00	EEST/EAT 3:00	AEST 10:00	
		EST 19:00	IST 5:30	NZST 13:00	
	SESSION 5	PST 5:30 P.M. - 6:45 P.M.	BST/WAT 2:30	ICT 8:30	
		MST 18:30	CEST/CAT 3:30	JST 10:30	
		CST 19:30	EEST/EAT 4:30	AEST 11:30	
		EST 20:30	IST 7:00	NZST 14:30	
	SESSION 6	PST 2:00 A.M. - 3:15 A.M.	BST/WAT 10:00	ICT 16:00	
		MST 3:00	CEST/CAT 11:00	JST 18:00	
		CST 4:00	EEST/EAT 12:00	AEST 19:00	
		EST 5:00	IST 15:30	NZST 23:00	
	SESSION 7	PST 3:30 A.M. - 4:45 A.M.	BST/WAT 11:30	ICT 17:30	
		MST 4:30	CEST/CAT 12:30	JST 19:30	
		CST 5:30	EEST/EAT 13:30	AEST 20:30	
		EST 6:30	IST 17:00	NZST 0:30	

CONFERENCE 3 days	ALL SESSIONS 1 Hr. 15 min.	AMERICAS		EU/AFR/SC		ASIA/PACIFIC		BREAKOUT SESSIONS TO JOIN (You can list the sessions you're hosting or attending below)
WEDNESDAY April 29	SESSION 8	PST	6:30 A.M - 7:45 A.M.	BST/WAT	14:30	ICT	20:30	
		MST	7:30	CEST/CAT	15:30	JST	22:30	
		CST	8:30	EEST/EAT	16:30	AEST	23:30	
		EST	9:30	IST	18:00	NZST	2:30	
	OPENING Agenda Creation	PST	8:00 A.M - 8:30 A.M.	BST/WAT	16:00	ICT	22:00	
		MST	9:00	CEST/CAT	17:00	JST	0:00	
		CST	10:00	EEST/EAT	18:00	AEST	1:00	
		EST	11:00	IST	20:30	NZST	4:00	
	SESSION 9	PST	8:30 A.M - 9:45 A.M.	BST/WAT	16:30	ICT	22:30	
		MST	9:30	CEST/CAT	17:30	JST	12:30	
		CST	10:30	EEST/EAT	18:30	AEST	1:30	
		EST	11:30	IST	21:00	NZST	4:30	
	DEMO HOUR Europe & North America	PST	10:00 A.M. - 11:00 A.M.	BST/WAT	18:00	ICT	0:00	
		MST	11:00	CEST/CAT	19:00	JST	2:00	
		CST	12:00	EEST/EAT	20:00	AEST	3:00	
		EST	13:00	IST	22:30	NZST	6:00	
	SESSION 10	PST	11:00 A.M. - 12:15 P.M.	BST/WAT	19:00	ICT	1:00:00	
		MST	12:00	CEST/CAT	20:00	JST	3:00	
		CST	13:00	EEST/EAT	21:00	AEST	4:00	
		EST	14:00	IST	23:30	NZST	7:00	
	SESSION 11	PST	12:30 P.M. - 1:45 P.M.	BST/WAT	20:30	ICT	2:30	
		MST	13:30	CEST/CAT	21:30	JST	4:30	
		CST	14:30	EEST/EAT	22:30	AEST	5:00	
		EST	15:30	IST	1:00	NZST	8:30	
	SESSION 12	PST	2:00 P.M. - 3:15 P.M.	BST/WAT	22:00	ICT	4:00	
		MST	15:00	CEST/CAT	23:00	JST	6:00	
		CST	16:00	EEST/EAT	0:00	AEST	7:00	
		EST	17:00	IST	2:30	NZST	10:00	
	SESSION 13	PST	3:30 P.M. - 4:45 P.M.	BST/WAT	23:30	ICT	5:30	
		MST	16:30	CEST/CAT	0:30	JST	7:30	
		CST	17:30	EEST/EAT	1:30	AEST	8:30	
		EST	18:30	IST	4:00	NZST	11:30	
	CLOSING Open Gifting OPENING	PST	5:00 P.M. - 6:00 P.M.	BST/WAT	1:00	ICT	7:00	
		MST	18:00	CEST/CAT	2:00	JST	9:00	
		CST	19:00	EEST/EAT	3:00	AEST	10:00	
		EST	20:00	IST	5:30	NZST	13:00	
	SESSION 14	PST	6:00 P.M. - 7:15 P.M.	BST/WAT	2:30	ICT	8:30	
		MST	19:30	CEST/CAT	3:30	JST	10:30	
		CST	20:30	EEST/EAT	4:30	AEST	11:30	
		EST	21:30	IST	7:00	NZST	14:30	
	SESSION 15	PST	2:00 A.M. - 3:15 A.M.	BST/WAT	10:00	ICT	16:00	
		MST	3:00	CEST/CAT	11:00	JST	18:00	
		CST	4:00	EEST/EAT	12:00	AEST	19:00	
		EST	5:00	IST	15:30	NZST	23:00	
	SESSION 16	PST	3:30 A.M. - 4:45 A.M.	BST/WAT	11:30	ICT	17:30	
		MST	4:30	CEST/CAT	12:30	JST	19:30	
		CST	5:30	EEST/EAT	13:30	AEST	20:30	
		EST	6:30	IST	17:00	NZST	0:30	

DAY TWO

CONFERENCE 3 days	ALL SESSIONS 1 Hr. 15 min.	AMERICAS		EU/AFR/SC		ASIA/PACIFIC		BREAKOUT SESSIONS TO JOIN (You can list the sessions you're hosting or attending below)
THURSDAY April 30	SESSION 17	PST	6:30 A.M - 7:45 A.M.	BST/WAT	14:30	ICT	20:30	
		MST	7:30	CEST/CAT	15:30	JST	22:30	
		CST	8:30	EEST/EAT	16:30	AEST	23:30	
		EST	9:30	IST	18:00	NZST	2:30	
	IDENTITY TECH SANDBOX	PST	8:00 A.M - 9:00 A.M.	BST/WAT	16:00	ICT	22:00	
		MST	9:00	CEST/CAT	17:00	JST	12:00	
		CST	10:00	EEST/EAT	18:00	AEST	1:00	
		EST	11:00	IST	20:30	NZST	4:00	
	OPENING *Agenda Creation*	PST	9:00 A.M - 9:30 A.M.	BST/WAT	17:00	ICT	23:00	
		MST	10:00	CEST/CAT	18:00	JST	1:00	
		CST	11:00	EEST/EAT	19:00	AEST	2:00	
		EST	12:00	IST	21:30	NZST	5:00	
	SESSION 18	PST	9:30 A.M. - 10:45 A.M.	BST/WAT	17:30	ICT	23:30	
		MST	10:30	CEST/CAT	18:30	JST	1:30	
		CST	11:30	EEST/EAT	19:30	AEST	2:30	
		EST	12:30	IST	22:00	NZST	5:30	
	SESSION 19	PST	11:00 A.M. - 12:15 P.M.	BST/WAT	19:00	ICT	1:00	
		MST	12:00	CEST/CAT	20:00	JST	3:00	
		CST	13:00	EEST/EAT	21:00	AEST	4:00	
		EST	14:00	IST	23:30	NZST	7:00	
	SESSION 20	PST	12:30 P.M. - 1:45 P.M.	BST/WAT	20:30	ICT	2:30	
		MST	13:30	CEST/CAT	21:30	JST	4:30	
		CST	14:30	EEST/EAT	22:30	AEST	5:30	
		EST	15:30	IST	1:00	NZST	8:30	
	SESSION 21	PST	2:00 P.M. - 3:15 P.M.	BST/WAT	22:00	ICT	4:00	
		MST	15:00	CEST/CAT	23:00	JST	6:00	
		CST	16:00	EEST/EAT	0:00	AEST	7:00	
		EST	17:00	IST	2:30	NZST	10:00	
	SESSION 22	PST	3:30 P.M. - 4:45 P.M.	BST/WAT	23:30	ICT	5:30	
		MST	16:30	CEST/CAT	0:30	JST	7:30	
		CST	17:30	EEST/EAT	1:30	AEST	8:30	
		EST	18:30	IST	4:00	NZST	11:30	
	CLOSING CIRCLE *Open Gifting*	PST	4:45 P.M. - 5:45 P.M.	BST/WAT	0:45	ICT	6:45	
		MST	17:45	CEST/CAT	1:45	JST	8:45	
		CST	18:45	EEST/EAT	2:45	AEST	9:45	
		EST	19:45	IST	5:15	NZST	12:45	

DAY THREE

IIW 30 Opening Exercise in Small Groups

Each IIW begins with a round table exercise designed to both start the current identity conversations and connect new with long time attendees. At IIW 30 the prompt questions were focused on acknowledgment of the global pandemic (the reason we are gathering online) and how participants see it shaping how they think about identity. what has happened or been accomplished over the years that has impacted identity from each person's experience.

- How are you & where are you?
- How is the current crisis shaping how you think about identity differently AND/OR
- How is the current crisis opening new opportunities?

When groups returned to the circle, they were asked to share highlights of their conversation in the text chat function in Zoom. Below are the comments that were:

- Key words from our group - Accelerated demand for digital and the strong need for Interoperability to support business use cases
- Privacy and SSI are more important than ever
- Lots of duplicate effort for immunity/tracing VCs
- General identity proofing changes for things like I-9
- Lots of discussion about how to practically get SSI out to address COVID19 challenges
- Concerns about privacy with tracing Apps
- Our group was talking about RAILS and LAST MILE solutions for health credentials
- Lots of interest in MFA solutions to verify the user identity
- More adoption of tools requiring strong identity
- I wish we were 18 months further in tech than we are.
- Explosion of need to get credentials vetted for employment and volunteer work
- It's easier to explain verifiable credentials than EVER BEFORE
- We talked about value of identifiers in supply chain for tracking of medical devices and PPE
- Potential duplication of efforts by actors, could efforts be pooled together?
- Feeling of a sense of urgency of what we are doing
- more attention to selective data disclosure
- SSI for contact tracing
- The crisis has shown how broken our telecommunication systems are
- How governments are now PEERS with tech companies. Contact tracing now given over to google/apple
- Identity verification providers are often only semi-automated and their human workforces can be impacted by COVID
- Emerging need for trust - we need to carefully device solutions that can help establish trust
- Touched on everything from ZKP to trust

- we talked about centralization vs. decentralization!
- Identity and the balance between Centralization and Decentralization
- Quick we need that Micromachines guy from the 1980s to read the comments!
- Lots of interest in selective disclosure of personal data
- New privacy issues emerging
- Is the fed doing anything with HIPAA to facilitate reporting of personal testing for immunity IDs?
- Low-tech SSI - QR Codes
- How to create with the Wallet to be presented at "checkpoint"
- Are we leaving the non-tech behind with move to online discussions
- Need projects that let SSI be shown as an empowering technology and inclusive technology
- history is overtaking us. we've been working on this for years and because we haven't solved it entirely, the government and corporations are going to build a centralized silo instead.
- The convergence of Decentralized Consent ("Trust"), Decentralized Identity ("Assurance") and Decentralized Semantics ("Immutability") are now taking a seat at the same dinner table courtesy of coronavirus!
- Interoperability between different SSI technology stacks and protocols. How do we ensure that verifiable credentials can be supported across borders and ecosystems.
- I mentioned the fact that we are all willingly giving up our freedom of assembly (temporarily) for an important reason. This event has forced us to realize that there is always a delicate balance between different imperatives as we consider individual rights, especially in regards to identity and privacy.
- Legal developments acceleration around paper credentials turning digital in fields like medical

Session Topics / Agenda Creation

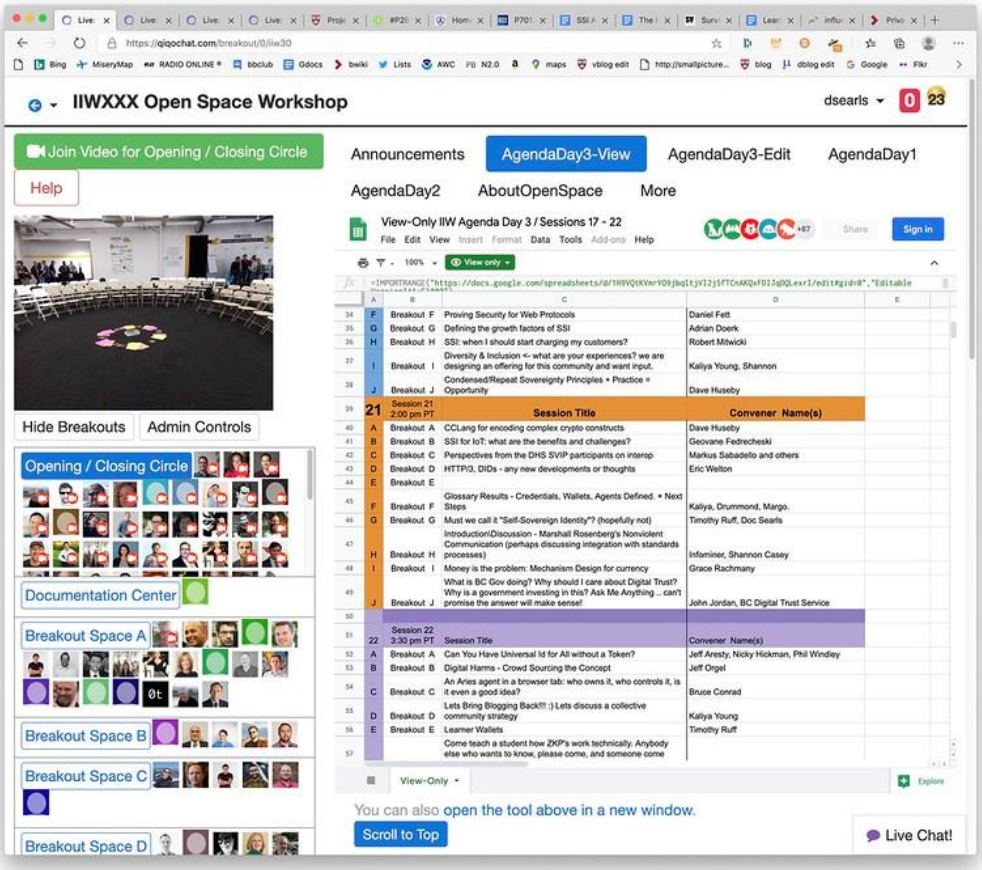


PHOTO CREDIT
@DSearls

136 distinct sessions were called and held over 3 Days.

We received notes, slide decks and/or white board shots for 133 of these sessions.

Day 1 / Tuesday April 28, 2020 / Sessions 1 - 5

Session 1
1B/ 101 Session OAuth2
1D/ SSI Adoption Sequence in a Pandemic
1F/ SSI to keep the Anonymous Open Web (keep quality content accessible)
1H/ "Digital Trust Primer and an Introduction to the Trust over IP Foundation"
1I/ 🚀 Code of Conduct - at DIF

Session 2
2A/Building the WordPress for Crypto (reusable UI) - AND Call for participation in Funding Call
2B/101 Session - Open ID Connect
2D/Authorization with SSI: How do we do AuthZ with credentials?
2E/ ZKPs for JSON-LD
2F/"KERI (A) Key Event Receipt Infrastructure. A ledger agnostic framework for decentralized identity. KERI unifies many DID methods types.
2G/Verifiable Credentials for Trade Items
2I/ COVID APPS: WHAT COULD POSSIBLY GO WRONG?

Session 3
3A/"KERI (B) Key Event Reciept Infrastructure. Key Event Receipt Infrastructure.
A ledger agnostic framework for decentralized identity. KERI unifies many DID methods types.
3B/101 Session - UMA User Managed Access
3C/Malware attacks against SSI, how SSI may be the perfect honeypot if you're not careful
3D/Identity in DxOS Collaboratively editing document in decentralized application with Groups and multiple devices.
3E/Evernym AMA
3F/Child Safety Online: SSI, VCs, governance, guardianship, GDPR
3G/VC & Open Badge Linkage
3H/Vectors of Authoritarianism

Session 4
4A/COVID Daze/Days - The HumanOS & new relationships w/connected systems & Services
4B/101 Session - SSI and Decentralized Identity
4C/Your experience with exercising your rights (e.g. downloading your data) under CCPA or GDPR
4D/"DIF Universal Resolver and Universal Registrar
4E/The State of SSI (gathering & sharing lists, stats, big news, etc.)
4F/ A verifiable public document graph to facilitate SSI
4G/Dance Party
4H/DIDComm WG Progress Update
4I/"Entity and Object Identifiers: Bringing assurance and immutability to a decentralized network"

Closing & Opening for next 4 Sessions

Session 5
5A/ Happy Hour! IEEE Special Issue on Resilience & Recovery - The role of identity?

Day 2 / Wednesday April 29, 2020 / Sessions 6 - 13

Session 6
6A/Building UIs for Decentralized Tech

Session 7
7A/Decentralized Data Economy (DDE) unconference - Europe. Initiative to bootstrap unconference format for component like TDA, PBS, MSP, SSI, VC etc..

Session 8
8A/How can we make Digital Identity a Sticky topic?
8D/Group Identity - Open Discussion
8F/Are we all wrong? Maybe full public display of all and everyone’s data, without exception, is the solution
8E/ Patient Choice using Distributed Identifiers

Closing for 4 Sessions that were held
Opening / Agenda Creation for Upcoming Sessions

Session 9
9A/ Domains of Identity <- Book coming out - 1) overview of it 2) help me figure out how sell more/share it widely
9B/ KERI (C) KACE Agreement Algorithm Recovery
9C/ Principles of User Sovereignty (1/3)
9D/ SCIM Reignition - HR and SSI
9E/ Healthcare Patient Choice with Distributed Identity Assurance
9F/ DID WG Q&A
9G/ Discussing the Future of Aries, Indy, and Ursa
9H/ Sidetree Protocol / Element DID and Friends
9I/ Understanding MyData Operators - white paper published today

Session 10
10A/GS1's decentralized approach to resolving identifiers over HTTPS
10B/ SSI Architecture Stack / Layers & Community efforts
10C/ Getting back to work: End to End Concept live prototype using Hyperledger Aries for Essential Workers
10D/ ID2020 Certification: feedback and next steps
10E/Every vault has a key that needs to be secured outside the vault. Role of central entities at the periphery (edges) of SSI ecosystem. Seeking answers to questions faced when presenting SSI to consultants/customers/users.
10F/ Fundamental Problems of Distributed Systems (2/3)
10G/ TxAuth and XYZ (and Maybe someday OAuth 3)
10H/ Deepfakes and Identity-- Problems, solutions, focus on technology

Session 11
11A/ Creating a Knowledge Product for the Community - What do you want/need information wise you don't get / takes to much time? what will you pay for???
11B/ DPoP Introduction & Current Developments
11C/ Sovrin Update
11D/ Are VCs a necessary hurdle on the path to DID adoption?
11E/ Search Warrants and Smart Devices: Encryption, Privacy and the Crypto Wars
11F/ Is consent broken? If yes, what can we do?
11G/BBS+ JSON-LD ZKPs and Aries & Indy. Your Thoughts?
11H/Tracking Identity on the Supply Chain: Curated Tour of the Report
11I/Spotting Economic Opportunity in an SSI World (3/3)

Session 12
12A/ Kiva SSI BIOMETRICS and HOW YOU CAN HELP!
12B/ What goes in Credential Subject? Let's chat Credential Ontology
12C/ Reducing Correlation in Verifiable Credentials without ZKP
12D/ Integrating DID into an app in 10 minutes
12E/JSON Web Messaging (JWM): What are they and why are they useful for secure messaging systems?
12F/ Trust / Risk Metrics in SSI - What can we learn from technical trust in order to inform human trust
12H/Determining demand & feasibility for your SSI/VC use case
12I/Building Technology and Successful Use Cases based on the most marginalized as the answer to the problem
12J/OAuth Metadata: Mix-up Machine?

Session 13
13A/ Cards Against Identity
13C/ What is a Test Credential?
13D/ True Self-Sovereignty: What Will It Take?
13E/ "IIW SSI Spotlight: 5 Priority Topics of the SSI-Community 1 wallet backup, 2 on-device credential sync, 3 public DID verification, 4 control over public DIDs, 5 third-party identities"
13F/ Minimum Positive Human Application of SSI
13G/ Contextual, trans-silo, on-demand groups (incident resolution) - pragmatic challenges to forming persistent, formal, credential-based, conversations across enterprise boundaries to solve problems.
13H/ SSI and COVID-19 health status certificates - ethics, policy and next steps
13I/ Overlays Capture Architecture (OCA)
13J/ Secure Data Store Working group - review the charter, meet the Chairs, invitation to get involved.

Closing & Opening for next 4 Sessions

Session 14
14A/ The Digital Harms Dictionary - Review of the tool and its mission
14B/ SSI and Payments

Session 15
15A/ DIDComm over satellite communication
15D/Building UIs for end users

Session 16
16B/ Supporting sovereign insurgencies - secure communities for social change - putting out fires when it is illegal to do so
16C/ Low-tech solutions - QR Code Wallets
16E/ Portable Reputation Using SSI

Session 17
17A/ Open Discussion on Email, Messaging, and SSI/DID
17B/ Hyperledger Aries - How to send messages to an unknown receiver - The Out-of-Band Protocols
17C/ Identity for All - Universal Declaration of Digital Identity
17E/ Open Source Product Strategy
17J/ Cards Against Identity - Hangover Edition

Day 3 / Thursday April 30, 2020 / Sessions 18 - 22

Session 18
18A/ Hyperledger AMA
18B/ Verifiable Credentials for Global Supply Chains
18C/ Guardianship & SSI
18D/ Your Trustee and Ethics in a Pandemic - What your community can do to prepare
18E/ KERI Implementation: Whats Next DID:UNI Method. Ref Imp. DIF Project.
18F/ Intro to the Me2B Alliance Testing Specification
18G/ Credentials should be treated like keys KMS discussion
18H/ Build an SSI Proof of Concept on Sovrin
18I/ Intro to did:web Decentralized Identifier method

18J/ Ensuring Transparency in Law Enforcement Exceptional Access
18Changpuhe Park – China Garden/ PhD positions at Identity lab based in Edinburgh - Come ask me about it.

Session 19
19A/ 101 Session: Verifiable Credential Handler (CHAPI) and DIDComm
19C/ Transaction Tokens: Optimizing Authorization across "domains"
19E/ The Future ain't what it used to be — How to approach the next few years (COVID, climate, economic depression ...)
19F/ Call for Asia Pacific collaboration
19G/ SSI and Payments Continued
19H/ Organizational Wallet
19I/ "Mouse Head Model (MHM): A global solution for safe and secure data sharing"

Session 20
20A/ Overview of VC / DID / JSON-LD Interoperability Plug Fest
20B/ Group Identity pt 2
20D/ The Future of Telecommunications is DID Comm
20E/ Magic Sandwiches
20F/ Proving Security for Web Protocols
20G/ Defining the growth factors of SSI
20H/ SSI: when I should start charging my customers?
20I/ Diversity & Inclusion <- what are your experiences? we are designing an offering for this community and want input.
20J/ Condensed/Repeat Sovereignty Principles + Practice = Opportunity

Session 21
21A/ CCLang for encoding complex crypto constructs
21B/ SSI for IoT: what are the benefits and challenges?
21C/ Perspectives from the DHS SVIP participants on interop
21D/ HTTP/3, DIDs - any new developments or thoughts
21F/ Glossary Results - Credentials, Wallets, Agents Defined. + Next Steps
21G/ Must we call it "Self-Sovereign Identity"? (hopefully not)
21H/ Introduction\Discussion - Marshall Rosenberg's Nonviolent Communication (perhaps discussing integration with standards processes)
21I/ Money is the problem: Mechanism Design for currency
21J/ What is BC Gov doing? Why should I care about Digital Trust? Why is a government investing in this? Ask Me Anything .. can't promise the answer will make sense!

Session 22
22A/ Can You Have Universal Id for All without a Token?
22B/ Digital Harms - Crowd Sourcing the Concept
22C/ An Aries agent in a browser tab: who owns it, who controls it, is it even a good idea?
22D/ Lets Bring Blogging Back!!! :) Lets discuss a collective community strategy
22E/ Learner Wallets
22F/Come teach a student how ZKP's work technically. Anybody else who wants to know, please come, and someone come teach us!
22G/ IIW30 The Session Collection and Song List
22H/ ZKPs for JSON-LD using BBS+ - Round 2
22J/ Build an SSI Proof of Concept on Sovrin (Part 2)

Day 1 Tuesday April 28 / Sessions 1 - 6

OAuth2: An Introduction (101 Session)

Tuesday 1B
Convener: Justin Richer
Notes-taker(s):

Tags for the session - technology discussed/ideas considered: #OAuth 2

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Introduction to OAuth 2.0 protocol and surrounding work.
http://oauthinaction.com/
http://oauth.xyz/ -> next generation work

SSI Adoption Sequence in a Pandemic

Tuesday 1D
Convener: Adrian Gropper
Notes-taker(s): Scott Mace & Orie Steele

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

https://bit.ly/IIW-SSI-Adoption

Scott Mace's Notes here are followed by other notes immediately below. Thank you, all.

Adrian Gropper: There is a natural sequence of steps for the example of an immunity passport is going to have to happen. A lot of it may be somewhat controversial.

This is tied to a prescription use case in the W3C standards. There is a credential prescriber that issues a credential to a subject (the patient) then verified by a pharmacist. Not that different than British Columbia use case. Which entities and individuals have to do what?

Alan Karp: Missing the ability to delegate. Someone going to the pharmacy on someone else's behalf.

Orie Steele: Case where credential subject and credential holder are different.

Alan: Would be nice if holder of prescription could delegate to a third party after the fact.

Adrian: I agree with you Alan. How might we modify the sequence? Leave it as a comment or let's discuss it.

Alan: State of New York didn't have delegation. Here, you would add a row in the table where holder of the credential will be able to delegate it. Owner of a file can change the access control list.

Adrian: In this sequence, the patient does not really need a DID at all. I consider this to be an asset in terms of adoption, because it's one less thing to deal with.

Alan: The mechanism isn't as important as the function.

Orie Steele: You could request a delegated credential from OAuth, get back a bearer token. How about transactional OAuth?

Adrian: Justin is the man. We are hopefully headed to the IETF version of the authorization server. To be standardized in OAuth 3 or whatever. Simplifying the OAuth flows, which are very difficult to use in practice. FHIR is fundamental to what's going on here. If you monitor the lists where people discuss this, it's a disaster.

Karp: Signed jots may be better for nonrepudiation than bearer tokens.

Stewart Whitman: There's a continuum between going to the hospital all the way to self-testing. How can we think about a trusted intermediary? Where is the likelihood of that continuum going to come out?...I could confound a test if it is unproctored.

Adrian: You're right.

Stewart: I formerly worked for Clear. That's great in a closed system. In an open system, that's only as valuable as what it's being bound to. Need witnesses. Like age-based verification for alcohol purchases. Easy to confound into a wallet, whether in closed loop or an SSI system.

Phil Wolff: Public health subject matter expert?

Dr. Saeme MD: immunity passport, it depends on how you use it. Immunity is normally linked to vaccination. Normally, it's confirmed by a certified doctor or vaccinator or public health provider. When it comes to COVID-19, it's really complicated to delegate that to the user. We have no specific test we can trust 100%. Even if you have recent infection, you might still be shedding virus. This is why we have to divide between immunity and the virus itself. Until we get a vaccine, we will need to do both. If you have positive immunity, you might be protected, but we don't know for how long. If you are negative, you will need to take a test that you are not carrying the virus. After 24 hours you could get the virus contamination again.

Phil: We have a rapidly-changing definition of what's useful information. The rites and rituals around how a passport might be used will vary. I only see one scenario. We need a collection of scenarios. And still protect privacy of the individual.

Dr. Saeme: When required by a government or employer, you have your own information. Public health [is different].

Adrian: It might be easier for us to view this issue if we thought about contact tracing as the problem, rather than the immunity passport. They both have the same authorization server, has the same characteristic, which is you have to solve for authorization as to what information is available to the issuer. Do you just have proximity? Or do you also have location? And this is a huge debate in Europe, where some countries are rejecting the Apple/Google method because it doesn't [include] location. My point is the authorization server serves both sides of the health record, of the interpretation made by one of these expert credential issuers. On input side, access to risk profile? On the verifier side, do they have access to the result? Law enforcement, employers? Discrimination.

Eric Welton (Korsimoro): I'm a big fan of trustee concept. Gets beyond idea of an immunity passport. The project I'm working on now, two consulting houses, close to half million employees total. Reopening

football matches in Europe, Toyko Olympics, office space, airlines. These are semi-public spaces. They're guarded. Tested upon entry. They need to do something that's better than nothing. A phase we need go through on short end where we don't have really rich issuance verification. Emirates was doing nurses at the airport. After that, moving to a place where you can bring your own data. Having someone at a Walmart or pharmacy witness a test. A lightweight risk assessment that integrates your credentials. Using the Walmart.com signing certificate. Could be done in 3 weeks. Not a strong solution, moves towards bring your own certification, proof of stuff, an integrated interpretation. I'd love to get to a place where we have a trustee-based solution. Bring your credentials.

Adrian: From perspective of these very large operators, what incentive do they have to adopt standards?

Eric: Real pain not to bring nurses into office buildings. Bring some kind of proof to move the pain point of getting tested away from the front door. They have a motivation to pursue standards to push that into the healthcare environment where it belongs. Now it becomes a small item they have to pay for, not a large one.

Adrian: They lose interest. If you're right, the cost is not in eliminating the doorman but in eliminating the nurse.

Eric: This is the path that leads us to a long-term solution.

Adrian: All this worrying about a verifiable credential is unimportant in the adoption scheme of things. Fair statement?

Eric: I've been an advocate for having a clearinghouse for the medical payload. You can get some light convergence on the encodings. Outside of that, need to use a particular standard like W3C, I don't think anybody cares, because these are semi-public environments. I already have a lot of PII about you. Security cameras. I am watching you. Not quite private. I was just at the cargo terminal at the airport here. Semi-public space. 100 vendors there but it is a highly regulated access environment. Took 20 minutes to get an on-the-spot credential. So I was allowed to walk around the facility. Those are the kinds of semi-public environments that have a slightly different set of rules than the society at large.

Orie Steele: I have a tiny demo in the DID space.

Adrian: Tell us where it fits.

Orie: Like you said, we need to be able to bind credentials to pictures. Mostly around using the VC data model in DIDs. One thing I've noticed working with CCI and W3C and DIF, not a lot of feedback on that piece. Crypto is irrelevant. I'm reaching the end of how I can contribute to the discussion as a technical person.

Stephen Curran: I've been going through your document. Seems incredibly complex. In the past we would have used paper for this. There's a bridge in Ottawa checking people bringing paper, police won't touch it. VC model is the new paper. We built the demo, I'm from the BC gov team, the big thing about that from the complexity point of view. For humans used to paper credentials, the whole VC model makes incredible sense, much more palatable for everyone to make use of and understand. That is the bigger enabler for creating an environment where something works, where we can apply SSI technology. We want verifiers to be able to trust it. We've been amazed how quick can put it together. Demo is BC safe entry, for an extended care facility, might include immunity passport or covid test. It replaces visitor logs. I focus entirely how to enable issuers and verifiers.

Adrian: In India I mentioned adhar as the biometrically-linked digital credential. I'm asking you in a situation where a government can dictate who gets to cross the bridge…I tell them you have to include an

authorization server in india stack. Need VC to be somewhat standardized. What would the Indians have to do to take up any of the standards we're talking about here?

Stephen: Don't know.

Adrian: That's my point. If you're not going to drive adoption Chinese-style…

Anil John: My mom is 90, lives in India in a state called Karola in the extreme south. Was interested in how somebody of her generation uses this technology. My mom has a piece of paper with a number on it and an incredibly bad photo. To prove her ID, she gives the paper to one of her cousins in order to get stuff. Let's be real about the magic of the india stacks. There is a set of services I'm sure that uses it. Everything else is, shall we say, flexible. I was stay away from contact tracing for now. We may be putting in place technical rails that may have unintended consequences downstream. On the immunity cert piece of it, let's get real. The fastest anybody has developed a vaccine was 4, 3 years. We're still about 18 months to 2 years out from a vaccine. Whenever I hear about immunity certs, the question in my head, just because we can do it doesn't mean that we should. Feels like a desire by technologists to move things forward. Instead of immunity certs, what is considered essential in the supply chain is very different. A lot of fragility in it. Maybe they're the one who need a mechanism to prove that they are indeed essential. Feels as though the immunity cert conversation is just so early at this point in time because of what we don't know.

Adrian: You're certainly right from a tech perspective, but wrong from a policy perspective. If we do not put in the infrastructure to manage pandemics and treatments that aren't there yet, at this point, we would be negligent. We have to run an authorization server in a way people can trust.

Anil: I agree we need a clear understanding of how to prove a certain set of entitlements. The equivalent of a doctor's note. We've had that technology for the last 10-15 years. Not as magical as SSI or UMA or OpenID Connect. Question is, if this was so important, why are we not focusing on the interoperability frameworks around existing technology?

Stephen: I agree with Adrian, although we don't know what the credentials look like, we need the infrastructure. We have 6-18 months. The demo we prepared is the combination of all the credentials that allow people to travel or go into different places.

Dr. Saeme: In many areas we have no testing or lack of sufficient testing, and the epidemic is very new. We will be dealing with this until we get a vaccine. When we get it, might take 3-4 years to immunize the 60, 70% needed to stop the epidemic. Quarantine rules oblige medical providers to inform the authorities to stop the infection. Any kind of certificate should be tightly linked to a real identity.

Slack channel: https://iiw.slack.com/archives/C012VNM1760

The key challenge for SSI is adoption

Immunity passports are a natural use case for SSI, ties back to the W3C prescription use case defined by W3C (*Never waste a crisis*)

Is delegation of credentials a possibility? where does delegation fit into the model in the link above ^.

Delegation could be something other than OCAP.

Patient does not need a DID.

Can we get Transaction Authorization Server / OAuth3 reference implementation links?

FHIR is critical to existing healthcare systems, we need to FHIR <-> OAuth3 showcase.

Encrypted JWT good for preserving privacy… when we say “bearer token” we may want to specify that we prefer the encrypted JWT format.

Here is an example of a Not Encrypted JWT for a Rapid Test, its based on this CCG work: https://github.com/w3c-ccg/vc-examples/blob/master/docs/covid-19/v2/v2.md

Regarding Liveness Detection Test: https://www.bioid.com/
^ Open ID Video based biometric facial recognition…

Secure Data Store (Identity Hubs / Encrypted Data Vaults)

https://github.com/decentralized-identity/secure-data-store

^ joint work item with W3C and DIF.

For anyone that is not aware of the COVID Credentials Initiative, the issues being discussed here, are also being grappled with here:

https://covidcreds.com

Q. How does decentralization strengthen/weaken passports/tracing?

Q. What are the incentives for standard adoption by government?

Q. Africa is working on a five minute ten-cent self-test strip, producing billions of them yearly. How well are we modeling individual self-testing and reporting?

Q. What “shovel ready” SSI infrastructure exists that can scale globally if, say, China or India or the EU said “Yes!” on Monday?

Q. What SSI solutions work on really old stupid phones used by a few billion humans? Proof points.

BC Canada’s “Safe Entry” app looks to replace visitor logs and guest pass generation. Link

Links from slack:
interop demo links for VC Data Model + DIDs
https://c19-vc.com/ (edited)
https://wallet.interop.transmute.world/ (edited)
https://verifier.interop.transmute.world/ (edited)
Here is our little blog post on it: https://medium.com/transmute-techtalk/covid-immunity-badges-dd9b8a05fa86

BC Gov Example: Here is the link - https://vonx.io/safeentry

SSI to Keep The Anonymous Open Web (Keep Quality Content Accessible)

Tuesday 1F
Convener: Joe Hsy (joe.hsy@liveramp.com)
Notes-taker(s): Will Abramson

Tags for the session - technology discussed/ideas considered:

#Privacy #SSI #Openweb #DID #Fair Value Exchange #Consumer Choice

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Attendees (feel free to add yourself):
Jason Downs
Michael Graybeal
Jan Taylor
Sterre den Breeijen
Will Abramson
Christian
Dave Huseby
Debbie Bucci
Alex Blom
Doc Searls

non-attributional is not equal to anonymous

Should this session be anonymous? Perhaps it's non attributed/pseudonymous
Real word businesses need to make money. How do we communicate the value exchange with the content consumers?

Non correlatable identifiers allow us to compartmentalize our relationships. SSI allows us to provide an identifier and a communication channel at the same time.

Today many sites are putting information behind a paywall or at least adding a login system to access their content

Also supercookies. IP Address. Many things that can correlate us across the web. All depends on how anonymous you want to be and to what lengths you want to go to maintain that.

Identity is purely transactional. It is to enable trust in these transactions. SSI brings strong potentially permanent identities. What is going to happen is not more anonymity but less. Because you are able to prove it, platforms are going to demand more proof not less.

Actually this is creating a marketplace. This is not about pseudo Nymity at all.

How can publishers continue to make money by serving high quality and relevant adds to
Potential Solutions

- Create a DID for each relationship with content producers

    - Allows people to prove they are in control of an identifier without revealing PII (authenticate DID ownership with private key)
    - Problem is a why would a publisher accept that identifier
        - What is the fair value exchange
- Joint create profiles with advertisers?
    - Profile specifies the things an individual is open to adverts for
    - Individual can have many profiles
    - One or more profiles can be associated with one or more DID's which represent the relationship with a content provider

(dsearls) FWIW, to me SSI, in respect to advertising, is to avoid either all of it, or just to get the branding (non-personalized) kind, which is also the kind that does a better job of sponsoring a publisher. The personalized kind only uses the publisher as tubing.
if the problem for advertisers and publishers is how to preserve personalization, we're talking about making a bad system worse. IMHO.
The idea that the personalized ads we get are "relevant" or "high quality" because of tracking is largely wrong. Mostly because almost all the time we are not shopping, and don't want to be treated as a shopper with a crosshairs rather than a reader who would rather not be bothered.

Is there a different way to do this that is not based on advertising. Requires a huge cultural shift. Need to get out of this model. A paywall hides content from those who can't afford it. Although through advertising model potentially people are giving away more than they might know.

Always have the ability to give something away for free.

Advertisers don't give you ads based on what you want. They want to sell you things you don't even know you wanted. Need behavioral advertising. Whole digital life is one big A/B test to influence you and push you to consume.

Ad identifiers are constantly sold and mined through pseudonymity. No point just adding another layer of pseudonymity.
Micropayments is not the only alternative model. We can keep non personalized advertising, which in fact was ALL of advertising, including online, until about 2012.
Every publisher I now subscribe to, to get inside the paywall, is tracking me MORE than before, and I am not getting any more "relevant" advertising. Nor do I want any.
At Customer Commons, we have a way for the publishers to accept OUR terms, which say "please show me ads not based on tracking me.

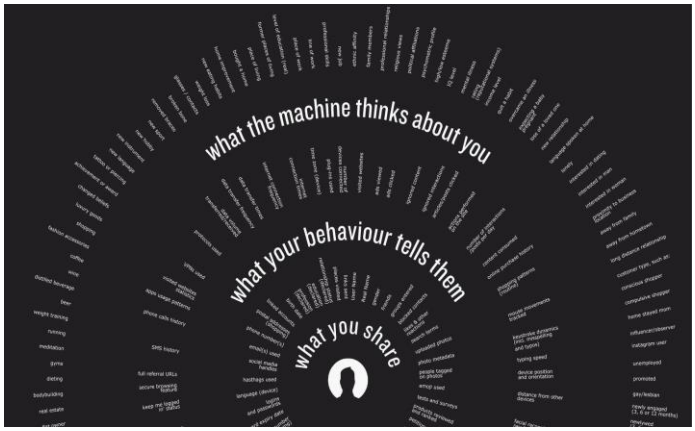
Trying to make advertising work better with SSI and DIDs is a fantasy for advertisers, not for users.

The true value of SSI is regulatory. Data is not invisible in some AI algorithm.
We have become a tool of direct marketing that we have no choice but to participate in.
SSI and DID's should not be used to make a bad system better.
Publishers actually made more money when their content was sponsored.
Advertising is not the only business model.
The web is becoming closed. You have to pay and register.
What are the other models alternate to advertising and payment.

How can we as humanity co create content that we want to be public open and accessible with no strings attached. A global public utility. A library? Content producers might want to produce content for free.

My writing about this, for anyone interested: http://blogs.harvard.edu/doc/the-adblock-war/

https://qz.com/1525661/your-digital-identity-has-three-layers-and-you-can-only-protect-one-of-them/



Tokenization of networks. Similar to Brave and BAT. Give appreciation for content that has been consumed. Tokens as a redeemable service.

We as consumers don't start from zero. We have a certain amount of virtual value to be given.

We need to be able to proffer and agree to our own terms, as individuals operating at full agency. There is nothing in the design of the Net or the Web that prevents that. Instead both support and encourage that.

Quote I think is true: Civilization is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men. - Ayn Rand http://aynrandlexicon.com/lexicon/civilization.html

Still a lot of free content. Just because there are publisher models that do advertising.

How we ask consumers - comprehension and ease of use problem.

Digital Trust Primer & An Introduction To The Trust Over IP Foundation

Tuesday 1H
Convener: John Jordan (Province of British Columbia) & Drummond Reed (Evernym)
Notes-taker(s): Ryo Kajiwara

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

PRESENTATION

[9:38] let's get started
old territory - flashbacks for some
john jordan -- introduce myself, coming to iiw since fall 2017, got into identity around 2007
today: primer with Drummond
drummond -- evernym, DID specification at w3c, linux foundation (hyperledger)

[9:40] let's wander through time looking at identity & trust broadly

In-Person Credentials
break down of trust
technology: print. it was expensive, (used to be) hard to forge
money is another form of conveyed trust
indicate where they come from

three-party model with underlying framework
issuer, holder, verifier, governance facility

signatures, ceremonies
big part of how we convey trust
"wax to fax"

Financial Services (Mastercard)
Government (Birth, Death certificates, and so on)
person needs to be known to the government in a trustworthy way

The Internet era

Problem: Trust Gap
there are only some business models that are successful on the internet: for example, E-Commerce and Online Advertising

New risks
chart: growth in insurance frauds

we tried to create "one-stop" services, but were not successful
"the login account" being the problem

The Digital Trust Era

we need to get back to the ceremonies, but be able to do this digitally
verifiable credentials model uses the same model as the physical world

Trust over IP Foundation: launching next week

Wax to Fax (to Stacks)

Windley: I call what John has labeled "technical trust" fidelity. And what he calls "governance trust" provenance. See https://www.windley.com/archives/2019/10/fidelity_provenance_and_trust.shtml

Nicky's Haiku:

*First **Trust** People*
Over red bees wax
Or a Fax
Over IP Stacks

Trust over IP
Layer 1: If there is some other party that can interfere with the communication, we need crypto. Interference with communication does not happen in real-world trust.
comment: Layer 0 needs to have an advanced version of Tor (-> privacy at transport)
Layer 2: How do we create a private communication between two parties? -> DIDComm Peer to Peer protocol
Layer 3: Credentials. Governed by the community that it is used in.
Layer 4: Applications. example: Paris Agreement (of global climate change)

Official launch will be 5/5, global session scheduled on 5/7
https://ieeexplore.ieee.org/document/9031548 - The Trust over IP Stack
https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0289-toip-stack
https://iiw.idcommons.net/The_Trust_Ove_IP_Stack_%E2%80%93_A_Path_to_Global_Interoperability_for_SSI_and_Verifiable_Credentials
---
questions/discussion

Q: how is the governance of trust over IP foundation going to work?
-> The Linux Foundation is working on many projects, and it's like one of them.
Steering Committee
Contributor/Associate level: free, available to everyone. wide open
requirement for the foundation was to have it open to everyone
If there's any kind of intellectual property to be discussed, you need to sign a document
International participation: we are having participants from all over the world. try to do asynchronous meetings as much as we can, meetings across multiple time zones, ...
Q: What is the scope of the Technical Stack WG?
-> Not to create standards at this org. Verifiable Credentials are 1.0 standard at W3C, DID is to be a standard at W3C, DIDcomm at IETF. Identifying the gap with standards and figuring out how to work with standards.
Q: How does Trust Over IP Foundation relate to DIF/W3C?
-> There is no such thing on the market that establishes trust that is purely reliant on technology. The policy is based on governance. We have to make decisions at every level of the stack. How can we have governance that is open/transparent/referenceable? Starting from governance, moving into technology. Technology is done in those groups.
Ecosystem trust and trust with blockchain is a problem of different layers.
Dependency between layers: how to do security/privacy across all the layers?

Q: Are the slides available? -> Yes, in this document! :)

Q: What are the benefits of being a paid member?
-> It's not that expensive, also depends on the size of your organization. We need a community manager (and the money is going to them)

Q: q+ to note how difficult this makes it for some companies in the space -- what are thoughts on yet another Foundation to join, strictness in technology stack, etc?
It's not clear that you are working on governance only, you're also working on technology
Does it not cause yet another fragmentation? Frustration, because it looks like undoing the work to bridge DIF/W3C/IETF… Why not use the existing framework (such as W3C Business Groups)?
->

The driver: the tent is just not big enough. Not a technical need, a human need. Some organizations do not do technical development, but we need to involve them into this discussion.
Why Linux Foundation: to make sure that money was not a requirement. Exactly like a W3C IG. Also, synergy with other projects in LF (such as hyperledger, …). Open Standards, Open Source, Open Governance.

Q: What kind of standards are going to be standardized in Governance Stack WG?
-> No standards but guidelines and best practices.

Q: Who is on the steering committee?
-> They will be announced in the live event

There's going to be another session on Trust over IP Foundation tomorrow

Raw dump of Zoom Chat:

From Manu Sporny to Everyone: (09:46 AM) haha, love the "From Wax to Fax"
From John Hopkins to Everyone: (09:46 AM) +1
From Ryo Kajiwara to Everyone: (09:46 AM) =1 +1
From Phil Archer to Everyone: (09:46 AM) That was a bad day..
From Mike Richardson to Everyone: (09:46 AM) God Save the Queen
From Michael Shea to Everyone: (09:46 AM) +1
From Drummond Reed to Everyone: (09:46 AM) +1
From Manu Sporny to Everyone: (09:46 AM) From Wax to (technology) Stacks? :P
From Chris Eckl to Everyone: (09:47 AM) UK not England!
From Drummond Reed to Everyone: (09:47 AM) Manu, I love it!
From Jan Taylor to Everyone: (09:47 AM) +1 Manu "Wax to tech stacks"
From Manu Sporny to Everyone: (09:52 AM) "Low tech wax to high tech stacks"? -- too many syllables. (yes, I'm on a rhymezone.com attempting to extend John's "wax to fax" saying to the tech sector :P)
From Drummond Reed to Everyone: (09:52 AM) Wax to fax to stacks?
From Manu Sporny to Everyone: (09:53 AM) ooh, I like that.
From Michael Shea to Everyone: (09:53 AM) W2F2T W2F2S
From windley to Everyone: (09:55 AM) I call what John has labeled "technical trust" fidelity. And what he calls "governance trust" provenance. See https://www.windley.com/archives/2019/10/fidelity_provenance_and_trust.shtml
From Nicky Hickman to Everyone: (09:55 AM)
Here's your Haiku Manu and Drummond Trust Bees Wax then fax over IP Stacks?
From Manu Sporny to Everyone: (09:56 AM) haha, love it!
From Nicky Hickman to Everyone: (09:56 AM) :-)
From Laura Jaurequi to Everyone: (09:56 AM) Ha Ha!
From Benedikt Olek to Everyone: (09:57 AM)Can we potentially get rid of the Governance body (previous slide)
From Drummond Reed to Everyone: (09:57 AM) Great question, and one we can dive into in the Q&A. Short answer is ANYONE can be a "governance authority"
From Benedikt Olek to Everyone: (09:58 AM) Thanks!
From cam-parra to Everyone: (10:00 AM) Can the steering committee be diverse this time? :)
From Maryam Shahid to Everyone: (10:01 AM) And then following that: how would that look like in an international platform's space?
From Drummond Reed to Everyone: (10:01 AM) Great questions, we'll get to both of those

From Kazue Sako to Everyone: (10:02 AM) Can you share with us the slides later? Some letters are too small to see over Zoom window on PC.
From Drummond Reed to Everyone: (10:02 AM) One key point: participation in the Trust over IP Foundation is open to any person or organization anywhere as a Contributor Member at no charge. The only requirement is to agree to the IPR rules so there is no patent trolling.
From Vic Cooper to Everyone: (10:02 AM) Or make your slides full screen
From Ryo Kajiwara to Everyone: (10:02 AM) The URL of the slides is on the notes
From Nathan George to Everyone: (10:03 AM) Sounds like Mike needs to propose a session on privacy at transport We have a lot of ideas on that The protocol should never betray you
From cam-parra to Everyone: (10:04 AM) I always worry that the interest of these foundations are towards developed countries. So diversity in leadership would be key for me to trust an organization
From gihan2 to Everyone: (10:04 AM) that's better, thans
From Drummond Reed to Everyone: (10:05 AM) Cam: Kiva is one of the founders.
From Laura Jaurequi to Everyone: (10:05 AM) Upvoting Nathan's nomination of Mike!
From Darrell to Everyone: (10:05 AM) @cam-parra - can you help drive that diversity?
From Benedikt Olek to Everyone: (10:05 AM) Is there reading on the "9(?) principles of sovereignty"?
From Kazue Sako to Everyone: (10:05 AM) Thanks, Ryo. I refreshed the screen and got the URL.
From Drummond Reed to Everyone: (10:06 AM)
@Benedikt: I think Dave Huseby is going to to a session on that topic
From Benedikt Olek to Everyone: (10:06 AM) Thanks again, Drummond :)
From Nathan George to Everyone: (10:08 AM) Now is as good a time as any to let everyone know that I have started work as Director of Engineering at Kiva leading the Protocol team there. As Cam referenced, we have a big interest in making sure these systems work well for the developing world. If you have an interest in helping, catch one of us on slack or in the gardens.
From cam-parra to Everyone: (10:08 AM) Thank you, Drummond! Again not trying to stir things :) just want to see this succeed
From Drummond Reed to Everyone: (10:08 AM) Wow, Nathan, that's huge news! Congratulations!!!
From cam-parra to Everyone: (10:09 AM) And I would love to help @Darrell where I can
From rouven to Everyone: (10:09 AM) Congrats Nathan! :)
From Matt Norton to Everyone: (10:09 AM) Way to go Nathan!
From Manu Sporny to Everyone: (10:09 AM) Congrats Nathan! :)
From Drummond Reed to Everyone: (10:09 AM) Nathan, I nominate that you and Cam run a session on Kiva and all the good things you are/will be doing there.
From Nathan George to Everyone: (10:10 AM) That is in the next time block breakout C
From cam-parra to Everyone: (10:10 AM) Have a session going on session 2
From AjayJadhav to Everyone: (10:10 AM) Hey Nathan, congratulations.. :)
From Kalyan to Everyone: (10:10 AM) Great news Nathan, heartiest congratulations!
From Jeffrey Aresty to Everyone: (10:11 AM) congratulations, Nathan
From Matt Norton to Everyone: (10:11 AM) Where do we see the most momentum in the stack? Where do we see the least?
From Michael Shea to Everyone: (10:11 AM) congrats Nathan!
From Oliver Terbu to Everyone: (10:12 AM) What is the scope of the "technical stack working groups"?
From Jsearls to Everyone: (10:13 AM) Nathan, this is really wonderful. Congrats!
From AjayJadhav to Everyone: (10:14 AM) Hi Drummond, any information on joining the foundation ?
From Gena Morgan to Everyone: (10:15 AM) How does this foundation relate to DIF?
From Manu Sporny to Everyone: (10:15 AM) ... and how does it relate to W3C? Hard to see where the swim lanes are...

From Elias Strehle to Everyone: (10:17 AM) I was just trying to clap, not raise my hand ;-)
From Drummond Reed to Everyone: (10:17 AM) @Ajay Yes, anyone in the session interested in joining, just email me at drummond.reed@evernym.com
From AjayJadhav to Everyone: (10:18 AM) Thanks Drummond
From Oliver Terbu to Everyone: (10:18 AM) Thanks john
From Me to Everyone: (10:19 AM) Elais .. ah .. :)
From Ramnath Krishnamurthi to Everyone: (10:20 AM) congrats Nathan!!
From Me to Everyone: (10:20 AM) My belief is that the existing communities such as W3C have a well understood space in helping discover and define internet standards
From Michael Shea to Everyone: (10:20 AM) Will it be possible to make this deck available later?
From Me to Everyone: (10:21 AM) Deck is available here …
https://drive.google.com/drive/u/0/folders/1R52XDeRqtPWCCPuNq-e4GNyOe7ckuPKa
From Darrell to Everyone: (10:21 AM) Desk link is in the notes as well.deck*
From rouven to Everyone: (10:21 AM) DIF & ToIP folks had a conversation last week. We agreed to create a joined document to better define scope & collaboration more explicitly. (similar to the effort DIF & W3C has down in Q1)
From Me to Everyone: (10:22 AM) There are few if any places for business people and less technical people to come and make sense of what their problem is with digital trust .. and how to evaluated their optinos
From Phil Archer to Everyone: (10:22 AM) q+ to comment on what Drummond is saying
From Michael Shea to Everyone: (10:23 AM) +1 to John J.
From Kyle Den Hartog to Everyone: (10:23 AM) What’s the expected benefits to being a paying member org (I remember one was steering committee seat, but I was thinking that was top tier) and how are those funds that are raised intended to be spent at this point?
From cam-parra to Everyone: (10:23 AM) +1 for Kyles question
From Me to Everyone: (10:24 AM) One of the first things we will nee at Trust over IP Foundation is a person to help the communities
From Nicky Hickman to Everyone: (10:24 AM) Agree @ John - there are 'bits' missing in terms of business requirements, - would be good to find a way of hooking in existing governance delivered through things like 't's & c's' and security policies - needs to be aligned around business transactions not identity or verification
From Me to Everyone: (10:24 AM) Transparency around WHY a technology is chosen is a key goal
From Me to Everyone: (10:24 AM) And WHAT the impacts of that technology choice means
From Gena Morgan to Everyone: (10:24 AM) nope
From Me to Everyone: (10:25 AM) To the members of the trust community …But those choices are for each community to make
From Darrell to Everyone: (10:28 AM) @Gena - what is your “nope” aimed at? Lots of questions/comments flying.
From gihan2 to Everyone: (10:28 AM) are this session's slides available?
From Gena Morgan to Everyone: (10:28 AM) sorry - to Phil
From Jesse Empey to Everyone: (10:28 AM) Deck is available here …
https://drive.google.com/drive/u/0/folders/1R52XDeRqtPWCCPuNq-e4GNyOe7ckuPKa
From Matt Norton to Everyone: (10:28 AM) sorry! Thought the annotations were just on my screen haha
From Gena Morgan to Everyone: (10:29 AM) @ Darrell - sorry to Phil
From gihan2 to Everyone: (10:29 AM) thanks
From Manu Sporny to Everyone: (10:30 AM) q+ to note how difficult this makes it for some companies in the space -- what are thoughts on yet another Foundation to join, strictness in technology stack, etc?
From Ryo Kajiwara to Everyone: (10:30 AM) I'm missing a lot of things on the notes; please feel free to add anything that I'm missing!

From Siva Kannan to Everyone: (10:31 AM) Related to Manu's Question, thoughts on another foundation(not on the tech side): but, how will the foundation help with the various governance frameworks - are they a set of standards for governance?
From Kyle Den Hartog to Everyone: (10:32 AM) Thanks @John for discussing that. Additionally, who are the current steering committee members at this point?
From Elias Strehle to Everyone: (10:33 AM) Could you help me understand what kind of "trust" the Trust over IP Foundation wants to ensure? Is your focus credible identity, so I can be sure that everybody on the internet is who say they are? Or also about trust that the other party does not lie/will not cheat?
From Drummond Reed to Everyone: (10:34 AM) @Elias - the "trust" in Trust over IP is the trust any two parties decide they need in a particular context. So it can be about all of those things and others.
From Manu Sporny to Everyone: (10:38 AM) q+ to separate governance from tech.
From rouven to Everyone: (10:38 AM) +1 manu :) I guess the confusion might come from this foundation being in a tech organization like the Linux Foundation
From Manu Sporny to Everyone: (10:39 AM) There is that, too :)
From rouven to Everyone: (10:39 AM) *being part of
From Me to Everyone: (10:40 AM) Linux Foundation has over 200 projects .. quite a number that are not purely technology focused
From Nathan George to Everyone: (10:42 AM) Or perhaps a more cynical response: Unfortunately all the SDOs are in a bit of an arms race to do open source work and conversely open source foundations are trying to branch out into standards and community-type groups (for example see IEEE SA Open Source). We don't want to see the community caught up in their ambitions, but if we can get resources to make things go faster we should. (Kantara and others might have ways to help too.)
From Me to Everyone: (10:43 AM) Folks … as we come to a close on this session I want to thank you all for taking the time to listen and participate. We would love to hear from you. Hope you have a great IIW and be well.
From Nathan George to Everyone: (10:43 AM) John++. Thanks for sharing all this!
From Ramnath Krishnamurthi to Everyone: (10:43 AM) Thanks John and team for sharing the deck
From windley to Everyone: (10:43 AM) Thanks John
From Michael Shea to Everyone: (10:43 AM) Thanks John & Drummond!
From Kyle Den Hartog to Everyone: (10:43 AM) Thanks John for covering this
From Elias Strehle to Everyone: (10:44 AM) Thank you!
From Me to Everyone: (10:44 AM) And thanks to the note taker who's name I missed unfortunately.
From AjayJadhav to Everyone: (10:44 AM) Thanks John

Code of Conduct – at DIF

Tuesday 1I
Convener: Balázs Némethi
Notes-taker(s): Karyl Fowler

Tags for the session - technology discussed/ideas considered:

Community building, correct behaviour, escalation of issues, training and promotion of awareness of CoC and adherence to it. Read document out loud together and solicited inputs.

Discussion notes, key understandings, outstanding questions, observations, and, if

appropriate to this discussion: action items, next steps:

- This is the first time the "final" draft of the DIF code of conduct is being put in front of the community for review/comments/feedback and acceptance.
    - The CoC lives here: https://docs.google.com/document/d/1SlsG20L2mkb22KKZl-3DEid5n5bkLVGYB3CagjDclW0/edit#heading=h.m3tl2zkfmkkv
    - Community members are encouraged to dive in and make comments/suggestions.
- This doc was written by a small collection of community members over the last ~3 months and is intended to define conduct that facilitates an inclusive environment for building and growing together.
- CoC Highlights:
    - DIF is an "open and inclusive environment"
    - Diversity is widely defined to include diversity in background, race, religion, ability, sexual orientation, gender identity, language, culture, age, technical ability, etc.
    - **"Diversity should never be put definitively out-of-scope or foreclosed as irrelevant to more urgent business."**
    - Currently relies on the DIF SC and the Working Group Chairs to help enforce this.
    - **"Conflict can be explicit or implicit, and there are many ways to contribute to a suboptimal community dynamic that can lead to conflict."**
    - Document outlines specific examples of unacceptable behavior in attempt to define types of negative "conflict" that might arise and require intervention or escalation. These include things like: trolling, harassment, soft-doxxing, divisive tone, scapegoating, implicit delegation, emphasizing a majority/minority boundary, etc.
    - also outlines "dispute escalation and resolution mechanisms" in a tiered format based on severity of issue; these levels include:
        - 0 - addressing it privately
        - 1 - talk to someone else
        - 2 - reach out to the WG Chair
        - 3 - reach out to a chair of another WG
        - 4 - reach out to the steering committee [together w/ a WG chair]
        - 5 - the nuclear option
    - Data-based conclusion
- Outstanding concerns:
    - It's really important to disseminate this CoC to the larger community and ensure everyone is committed to adherence.
    - How can we ensure this is the case?
        - One item is to make this an "official document" via the Steering Committee at DIF
        - Can also include it in all of the meeting pages and on website
    - What are other "mechanisms of inclusion" that can drive enforcement?

        - critique - this document is an external mechanism of inclusion with no obvious mechanism of enforcement
        - critique - this community is often overly biased towards being too polite versus direct
    - Suggestion to put this on Github for community dissemination
        - It would be cool to be able to transparently see the suggested changes/comments
        - Also suggested that we adapt the IPR to give it an open source license since it is useful beyond our DIF community.
            - There are constraints re: JDF (the legal entity behind DIF)
            - Ways around this?
                - Shared goal is ensuring it is licensed for easy reuse.
    - Specific phrasing suggestions:
        - Change section under "**Diverse"** to explicitly "welcome community members regardless of how they identify" before getting into the list of potentially diverse attributes.
        - Folks will inevitably come up w/ things we'd missed; how do we mitigate the risk/fallout from that?
    - Critique: How can we account for cultural differences when doing business (e.g. providing direct feedback, etc.)
        - Unsure how to address this.
        - One of the ways to differentiate "aggressive" or "loud" language has to do with the words that are said. For example, **criticizing an idea is fine, but criticizing a person is not fine.**
            - The latter is addressed in document.
    - Critique: What is wrong w/ conflict? Conflict is necessary to come to agreements/resolve complex issues. We could be more precise w/ our language here.
        - Moderators are for this. Who are the moderators? WG chairs?
        - Healthy conflict is a practice; it's not culturally ingrained in many people.
        - Conflict is fundamental in nature; ref: diplomacy and the art of assuasion - there is path to healthy conflict.
        - Examples of conflict types could be more specific - perhaps narrative or anecdotal examples
            - you *don't* want a scapegoat, but you *do* want a devil's advocate
    - **Usability of this CoC is critical**
        - It might be useful to define what types of discussions should be held in email, chat, calls, etc.

- Resources to reference on other community CoCs:
    - https://www.businessinsider.com/reactgate-react-facebook-code-of-conduct-twitter-2019-8
    - https://insight.kellogg.northwestern.edu/article/code-of-conduct-unethical-behavior
    - https://weboftrustinfo.github.io/community-resilience/code_of_conduct_long.html
    - https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/ieee_code_of_conduct.pdf
    - Me2B is using Mallory Brown's expertise/research to help support development of a CoC for their organization.

        - If they proceed, they'll open the training up to anyone in the space who is interested in joining.
        - Contact Lisa LeVasseur for more info.
        - Program title: respectful technology begins w/ ….?
            - Can't just give lip service; culture change is required.

- Lessons from Rebooting Web of Trust's attempt at implementing a CoC
    - failed miserably, but why?
    - initial impetus for creating the CoC arose from a specific issue that occurred in the community
    - the CoC did not require all org leadership buy in to buy in, address issues or enforce CoC
        - Overall, really great CoC content, but without leadership buy-in, there was no way to enforce it when issues arose
        - Lesson: **must have DIF leadership (SC) buy-in - even full consensus?**
        - Lesson: if there is an issue within the leadership [where a leader is the one actually causing the conflict], this must also be addressed
            - Enforcement requires modeling/leading by example
    - Awareness of one's own biases is hard to achieve but also proves critical for enforcement/adoption.
        - Perhaps the CoC's defined D&I + equity Training for DIF leadership mitigates this
            - Should training be expanded or offered to broader community membership?
- Content of the CoC and enforcement are two separate initiatives
    - CoC works best when paired w/ enforcement mechanism
    - valuable to maybe model enforcement after "incident response"
    - there is a tension between necessity and practicality (when it comes to training, content, etc.)
        - some communities have a specially trained "incident response" team
            - this doesn't have to be a large group; rather a small subset
            - critique of existing CoC setup: **Chairs / committee are emphatically not the right people to handle incident response**
                - So then what is the ideal makeup of this group?
- How can we connect the value of D&I to business value?
    - There is a ton of research [some is referenced in the CoC as is]
    - Please add more!
- Enforcement mechanism suggestion - have a rating system.
    - This can be implemented even mid-session
    - creates "herd enforcement" versus relying on a single individual or chair to be the sole responsible party
    - Plus this creates ongoing/historical statistics about who and how conflict is being created/persisting across the community
        - Critique for this mechanism: those w/ the least power in the room could potentially be further marginalized or singled out as the problem if the makeup of the room is not equally representative of all types of diversity [which is very difficult to control].
        - Have trained professionals.
- Critique of escalation method levels:
    - Feedback is that many of these will not work, especially level 1
        - 5 levels is too many. How can we streamline?

    - Should be more directive about contacting employers, “DO NOT DO THIS” vs “should not do this”
    - Also important to have possible implications defined for when you implement the escalation plan
        - what happens after you….?
    - dangerous to rely on the SC and WG chairs to be the enforcers; this authority gets fuzzy/complicated
        - must recognize that conflict resolution under these circumstances requires mediating/brokering of those differences; this is hard.
- Critique: this CoC if very long, yet the resources it is based on are very short
    - Is this a **new** CoC of DIF? One already exists - but it has been deemed insufficient [although it is accounted for in this new one]

- Loudness and cultural difference,
- Word thoughtful <---promising…. but not elaborated.
- Perhaps consult with Bonita Banducci, www.genderwork.com, teaches graduate gender and engineering class at Santa Clara University, School of Engineering

A survey about community experiences with diversity and inclusion and equity to build a training for the community:
https://docs.google.com/forms/d/e/1FAIpQLSeTuHVctbkaYXBEF_B3Wkvr0TMvyoySshAUk7U2r25OPwbXvA/viewform?usp=sf_link

We are working on a Diversity and Inclusion Training - If you are interested in enrolling/learning more.
https://docs.google.com/forms/d/1iV_zsm7-cpAJVXeFv-X_2IsIphXq1UWYJ3MVON21nNA/edit

Respectful

The document that is used: https://docs.google.com/document/d/1SlsG20L2mkb22KKZl-3DEid5n5bkLVGYB3CagjDclW0/edit?usp=sharing

1. **Notes from Kaliya Young:**

Code of Conduct LInk https://docs.google.com/document/d/1SlsG20L2mkb22KKZl-3DEid5n5bkLVGYB3CagjDclW0/edit?usp=sharing

Zoom Chat (partial):

Heather Vescent: Would anyone be interested in hearing how the RWOT Code of Conduct was created and then dissolved? (I was involved in it.)
https://weboftrustinfo.github.io/community-resilience/code_of_conduct_long.html

Lisa LeVasseur: We're also considering developing a code of conduct for Me2BA
Lisa LeVasseur: actually, I said that wrong: we ARE developing a cc for Me2BA

Jace Hensley: Related: https://www.businessinsider.com/reactgate-react-facebook-code-of-conduct-twitter-2019-8

Grace Rachmany: https://insight.kellogg.northwestern.edu/article/code-of-conduct-unethical-behavior

Grace Rachmany One of the ways to differ: ntiate "aggressive" or "loud" language has to do with the words that are said. For example, criticizing an idea is fine, but criticizing a person is not fine. I

From Jace Hensley to Everyone: (10:07 AM)
mahod mah: Grace: I'm moderating a rambunctious facebook group the past 2 months as a volunteer. there is a lot of aggressive language without name calling and it makes it harder to talk to each other about the topic (cover-19 science and attendant issues)
Grace Rachmany: Facebook's intrinsic design rewards that behavior.
Grace Rachmany: If, as moderator, you do not have any way to kick people out, there's not much you can do
mahod mah: grace ++ you have to be able to mute and then block people who act out
Grace Rachmany: I like the idea of different types of sanctions, like first warning is just a warning, etc. there might even be a sanction that you can't participate in something until passing a training like the one Estee was just mentioning
mahod mah: Yes.. training is key. Either do it while examples are happening. And give say, 2 warnings before blocking, or train in advance.
Grace Rachmany: Agreed. I've also volunteered to help with this but I'm not very involved because so much of the work is ultra-geeky.
mahod mah: We have people agree to 10 codes of conduct, before they can enter the community but they forget mahod mah: over time.. so you have to train in the moment and model for the rest of the people in a thread mahod mah: it's time consuming and wearing.. so being able to ditch the bad quickly and fairly is also good
Grace Rachmany: Agreeing and knowing when you're being insensitive are two different things. Having roles of people who care for the group is one mechanism of keeping people ongoingly trained.
Lisa LeVasseur: yes, the training starts with seeing one's self clearly--understanding ourselves. @grace
Grace Rachmany: We also have to be careful about who we ditch. Often there are nutcases who are the absolutely most brilliant people. I feel we need to work on resilience as well-- how do we train the group together to manage those kind of people in real-time so that we don't have to get rid of people who are just socially un-trained.
Dmitri Zagidulin: I think the Chairs / committee are emphatically not the right people to handle incident response
Jeff Orgel: The idea of diplomacy enters in here.
mahod mah: That's what moderators are for.. to manage the conflict and stand up for people who have trouble with it and keep the discussion on track, on issues, without getting personal
Lisa LeVasseur: conflict is a practice

Grace Rachmany: Again, that's an issue of mechanism design. AGREED. Email is not the ideal mechanism for this type of discussion.
Lisa LeVasseur: BTW, i'm delighted with this work. thank you for tackling it and sharing it! _()_
Grace Rachmany:It might be useful to define what types of discussions should be held in email, chat, calls, etc.
Lisa LeVasseur: noted as another reference--you may have already used this: https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/ieee_code_of_conduct.pdf
Grace Rachmany: As we read that one I noticed myself making a face that could have been considered as a microaggression.
Lisa LeVasseur:Yes--need trained facilitators or need to ensure they are trained and have demonstrated skills.
Dmitri Zagidulin: maybe follow that with a section like 'Do Not:' and actually list those

Building the WordPress for Crypto (reusable UI) – And Call for Participation in Funding Call

Tuesday 2A
Convener: Phillipe Achille Villers (Value Instrument)
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

What are the ways in which Web 3 is different than Web 2.

How do you make a workflow, using the new technology in the background, make it easy for regular users to participate in Blockchain.

How do you compete with Google/Facebook sign on.

Relevant projects:

- Beltran Berrocal
- https://medium.com/@lyricalpolymath/web3designdecisionframework-e84075816515
- https://www.youtube.com/watch?v=DhMvMTwArXA

User Interfaces, Authentication

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

How reliable are the technologies available for developers to build their services upon? Using this tech tech right now feels like a new form of vendor lockin.

Introduction to OpenID Connect (101 Session)

Tuesday 2B
Convener: Mike Jones
Notes-taker(s): Mike Jones

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link sent from Mike Jones:

The presentation can be viewed at https://self-issued.info/?p=2074, which is a stable link

Authorization with SSI: How Do We Do AuthZ with Credentials?

Tuesday 2D
Convener: Jacob Siebach
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Difference between Access, Authentication, Authorization
How do we really do authorization with credentials?

Authentication and Identity
A lot of authentication does not have to do with identity eg. student getting a discount at a bookstore
-> you are authenticating with identity. identity as set of attributes
identifiable attributes
Authentication = Provenance
indirection (prove your identity, then use that to prove you are what you claim to be) causing problems -> directly prove claims with verifiable credentials

Verifiable Credentials can bypass Authentication to get Authorization
Also be able to delegate someone to act one one's behalf (with VC)

- Replay needs to be protected
    - can't stop replay without authentication
- If there's delegation, you can delegate someone to buy someone under 20 to buy beer
    - -> responsibility tracking comes together

Technical artifacts make sense when it follows patterns of contract and sub-contract
problem with Attribute-based access control: you cannot know what kind of access you are delegating

Dima Postnikov: Don't you authenticate to get a credential (1) as well as potentially to authenticate to retrieve the credential for presentation (2). As well as authenticate to delegate (3) if required.
There are multiple points authorisation happens too: when credential is issued (1) and when credential is used (2)

Benedikt Olek: You need to authenticate, otherwise other people can you VCs (e.g. Verifiers you shared the VCs with in the past)
You can only skip authentication when you have other (e.g. non-SSI-protocol) means of authentication and a secure communication channel

There shouldn't be an authorization token. They can be stolen. Authorization system should not give you a token
What is replacing a token? -> in the bookstore example, the bookstore calls the AS to check if discount is available -> How is it proved?
"confused deputy vulnerability/problem"
Service Chaining problem cannot be solved by authentication approach, needed an authorization approach

you have to have preexisting relationships with the RS, it prevents a lot of ad hoc collaboration
"13+2 problem": there were 400 attributes used in the Air Force, they could get a consensus on what the attribute meant for only 13+2 attributes

on SSI:

- SSI is supposed to unify offline/online experiences. How we do it offline should also work online.
- SSI enables you to choose which attribute will be attached to which DID (= selective disclosure)

micro-credentials
what is the decentralized mechanism that provides authorization?
authorization depends on the service provider

capability-based security
ocaps
a system that actually is working
two things are critical:
attenuated delegation
chaining

If every object knows the access policy for everything, you can work around it, but if you cross organization borders, it breaks.

(OCAPs talk was given at the last IIW)

Proposal at Kantara: naked VC is almost useless, need to tie it to a certain (context?). made a proposal in the healthcare domain.
https://kantarainitiative.org/confluence/display/WT/Draft+Recommendations

good thing about VC: you can provide a subset of the credential

identity: need an out-of-band mechanism to track down someone's identity to do responsibility tracing

if you give somebody's DID, that's a big deal, but you can delegate part of your VC

Q: are we sacrificing decentralization by solving authz/authn?
-> no. there are certain authorizations that is not tied to an centralized authority

Delegation chain, just like creating an intermediate certificate chain

VC and SSI only come in when deciding whether to give it to someone. that doesn't have to be in the certificate

Each delegator makes a decision based on whatever the delegator wants. don't need global agreements.
we are delegating authorizations, not the VCs themselves
If you try to block delegations, it will result in a more insecure system, people will start sharing credentials themselves. People used to share login credentials!

ZKPs FOR JSON-LD

Tuesday 2E
Convener: Tobias Looker
Notes-taker(s): Orie Steele

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slack channel: https://iiw.slack.com/archives/C012NAPF19T
Draft Spec: https://mattrglobal.github.io/jsonld-signatures-bbs-spec/

Draft spec repo: https://github.com/mattrglobal/jsonld-signatures-bbs-spec

BBS+ signature implementations: https://github.com/mattrglobal/node-bbs-signatures

https://github.com/andrewwhitehead/ursa-bbs-py

JSON-LD signature suite to use with VC-JS: https://github.com/mattrglobal/jsonld-signatures-bbs

Regarding credential schema definitions in the vc data model: https://w3c.github.io/vc-data-model/#data-schemas

Proof formats in the VC Data Model: https://w3c.github.io/vc-data-model/#proof-formats

The paper for "provable security": https://eprint.iacr.org/2016/663.pdf

A raw dump of the Zoom Chat follows

Mattr Global - Tobias Looker - ZKPs using BBS+ Signatures
https://mattrglobal.github.io/jsonld-signatures-bbs-spec/
https://github.com/mattrglobal/node-bbs-signatures
From CipherQueen to Everyone: (11:00 AM) Am going to eat lunch, will be on mute.
From Tobias Looker to Everyone: (11:03 AM) https://mattrglobal.github.io/jsonld-signatures-bbs-spec/https://github.com/mattrglobal/node-bbs-signatures
From Orie Steele to Everyone: (11:04 AM) Slack channel for this session is?
From Nader Helmy to Everyone: (11:04 AM)I can make one
From John Hopkins to Everyone: (11:04 AM) fullscreen presentation please
From timcappalli to Everyone: (11:04 AM) https://iiw.slack.com/archives/C012NAPF19T
From Me to Everyone: (11:05 AM) How do I get an account in the iiw slack?
From timcappalli to Everyone: (11:05 AM) https://join.slack.com/t/iiw/shared_invite/zt-e08ieit0-7~iZLzYJBIuaD6CG55YH7w
From John Callahan to Everyone: (11:05 AM) just click the link and it will walk u thru
From Me to Everyone: (11:05 AM) Merci!
From Kaliya to Everyone: (11:06 AM) https://join.slack.com/t/iiw/shared_invite/zt-e08ieit0-7~iZLzYJBIuaD6CG55YH7w
From Rouven Heck to Everyone: (11:06 AM)@John - yet another Mr Login :)
From Brent Zundel to Everyone: (11:06 AM)#zkp in the iiw slack
From David Waite to Everyone: (11:06 AM)Let me know if the slides can be shared as well
From Me to Everyone: (11:06 AM)@rouven .. seriously ..
From Carl Youngblood to Everyone: (11:06 AM)Would also like a link to the slides

From Me to Everyone: (11:06 AM)Just offer proof of IIW attendeeship :)
From Dmitri Zagidulin to Everyone: (11:06 AM)ouch :)
From Orie Steele to Everyone: (11:07 AM)https://iiw.slack.com/archives/C012NAPF19T^ slack channel
From Me to Everyone: (11:09 AM)Would actually be straightforward with vc-authn-oidc that we demoed last IIW :) … but anyways .. really looking forward to this talk
From CipherQueen to Everyone: (11:16 AM)Hi. Am attending the ZKProof workshop. As part of the NIST submission, one goal is provably secure. Is provably secure one of your goals?
From malwhere to Everyone: (11:16 AM)for the signature?The signature is provably secure
From Andrew Whitehead to Everyone: (11:17 AM)I've got an early python wrapper here as well - no documentation and the API will likely change: https://github.com/andrewwhitehead/ursa-bbs-py
From Orie Steele to Everyone: (11:17 AM)https://w3c.github.io/vc-data-model/#proof-formats
From Nathan George to Everyone: (11:20 AM)The credential definition was done in Indy as an efficiency thing, it lets systems cache more of what they use all the time. Can you comment on why inlining that seems like a better idea with BBS+?
From Orie Steele to Everyone: (11:21 AM)Because now you can use ZKPs with any system, not just coupled to a specific ledger.
From Stephen Curran to Everyone: (11:21 AM)I don't think that changes with this. Now you cache the contexts for the schemas of interest. The benefits outweigh - variable length schema and no ledger tie in.What Orie said :-)
From Nathan George to Everyone: (11:21 AM)You always could have those objects source anywhere from a crypto standpoint
From Stephen Curran to Everyone: (11:21 AM)Yup...can still be on a ledger.
From Nathan George to Everyone: (11:21 AM)Just wondering why you want them inline instead of reusable chunks
From Orie Steele to Everyone: (11:21 AM)Yes, you can still cache the JSON-LD contexts, its a best practice for stable ones.
From Stephen Curran to Everyone: (11:23 AM)From a dev perspective, CredDefs on the Ledger and in the wallet and having to be in sync has been painful. Dealt with in production, but friction in development.
From Orie Steele to Everyone: (11:23 AM)q+
From Brent Zundel to Everyone: (11:23 AM)what you're losing is the guarantees that having keys and schemas on a ledger provides.
From Charles Cunningham to Everyone: (11:23 AM)can BBS+ do range proofs? or is it purely masking verifiable attributes?
From malwhere to Everyone: (11:23 AM)No it can't do range proofsits just selective disclosure, you typically combine BBS+ with another ZKP mechanism like Bulletproofs
From Stephen Curran to Everyone: (11:24 AM)@brent, I don't think so. Both parties generate the keys from the JSON-LD deterministically.
From malwhere to Everyone: (11:24 AM)or SNARKs
From Brent Zundel to Everyone: (11:24 AM)Ursa has tools for incorporating range proofs with bbs+ signatures
From Nathan George to Everyone: (11:24 AM)Yes, I think its a bit 6 for one half-a-dozen to another
From Nathan George to Everyone: (11:25 AM)I am trying to figure out why they decided to be different as it has big integration consequences
From malwhere to Everyone: (11:25 AM)Cred defs and JSON-LD contexts are the same here
From Nathan George to Everyone: (11:25 AM)Not really, because there isn't any static serialization to JSON-LD
From Kyle Den Hartog to Everyone: (11:25 AM)And that can still be done using JSON-LD if the ledger can map the IRI to a JSON-LD object

From Nathan George to Everyone: (11:25 AM)I'm hoping Tobias shows that it means graph views or flattening are entirely unneeded
From Dmitri Zagidulin to Everyone: (11:26 AM)q+ to point out that the reverse is the case, re JSON-LD canonicalization
From Oliver Terbu to Everyone: (11:27 AM)Isn't the canonicalisation defined by the ld suite?
From Orie Steele to Everyone: (11:27 AM)Yes it is.
From Manu Sporny to Everyone: (11:27 AM)Yeah, I'm confused about the "We couldn't canonicalize JSON-LD" statement.
From Orie Steele to Everyone: (11:27 AM)There is JCS for JSON and N-Quads / RDF Normaliation...
From Juan Caballero to Everyone: (11:29 AM)Dmitri?
From Andrew Whitehead to Everyone: (11:29 AM)I think the normalized form would have to change significantly to support range proofs
From Nathan George to Everyone: (11:31 AM)There are also a lot of type normalization and schema-like thing that this may have a hard time covering compared to the serialization and encoding approaches others have already tried. I am optimistic but there is still a big hairball of functionality to address I'm hoping there is more on that later in the presentation? (Didn't mean to derail Tobias' presentation)
From Dmitri Zagidulin to Everyone: (11:32 AM)q- (manu can probably address my point better)
From Manu Sporny to Everyone: (11:33 AM)wait, Dmitri, what point?
From Nathan George to Everyone: (11:33 AM)Manu++ teach us the JSON-LD ways
From motoko to Everyone: (11:33 AM)where is the BbsBlsSignatureProof2020 type registered? I don't see it in the @context attribute definitions, should the `proof` have an @context?
From Dmitri Zagidulin to Everyone: (11:33 AM)that canonicalization does not mean "more than one way"
From Manu Sporny to Everyone: (11:33 AM)oh, Dmitri - ok
From Orie Steele to Everyone: (11:34 AM) Where is the link to the paper?
From malwhere to Everyone: (11:34 AM)https://eprint.iacr.org/2016/663.pdf
From Kyle Den Hartog to Everyone: (11:34 AM)@motoko we've got a spec that will be added to the CCG for the ld proofs registries
From malwhere to Everyone: (11:34 AM) There you go Orie
From Kyle Den Hartog to Everyone: (11:34 AM)Not sure if it's in there already or if there's a few small things that need to be done to move it into there
From Tobias Looker to Everyone: (11:35 AM)Yes @motoko correct there is an extended context
From Me to Everyone: (11:35 AM)Agree ++1 awesome … we already working on support @andrewwhite has a python wrapper for the Ursa libraries
From Wip to Everyone: (11:35 AM)So this is just a node wrapper os ursa?
From Orie Steele to Everyone: (11:35 AM)Can we get the python link added to the session notes?
From Me to Everyone: (11:35 AM)Clare .. link is in slack and here https://eprint.iacr.org/2016/663.pdf
From malwhere to Everyone: (11:35 AM)I believe andrew already linked it
From malwhere to Everyone: (11:36 AM)@Andrewwhitehead can you link to your python code for folks
From Andrew Whitehead to Everyone: (11:36 AM)I'll add it to the notesOkay, somebody beat me to it
From Nathan George to Everyone: (11:36 AM)Brent Zundel is the guy to follow up with. They did a lot of work on static serialization and data type normalization for cryptographic verifiability. We just want to make sure that part matches up.
From Kyle Den Hartog to Everyone: (11:37 AM)Linked the Python code in the notes
From Nathan George to Everyone: (11:39 AM)So as long as the derived proofs match the upstream credential it flows through
From John Callahan to Everyone: (11:40 AM)Ruby implementation: https://github.com/johncallahan/ruby-jsonld-signatures
From malwhere to Everyone: (11:40 AM)does the ruby implementation have BBS+?

From John Callahan to Everyone: (11:40 AM)no
From malwhere to Everyone: (11:41 AM)okay, its not hard now, Andrewwhitehead wrote the python one really quickly
From Nader Helmy to Everyone: (11:41 AM)Here's the python wrapper mentioned https://github.com/andrewwhitehead/ursa-bbs-py
From Orie Steele to Everyone: (11:41 AM)Looks like it only has Ed25519 and RSA… but if there was a portable binary of the Ursa lib for ruby… it wouldn't be hard to add support
From John Callahan to Everyone: (11:41 AM)it's a native implementation but I'd really like to see if we could have a benchmark set of ground truth for canonicalization (and back again) for interop
From malwhere to Everyone: (11:41 AM)Ursa has bBS+ Ursa has lots of signatures Orie
From johnnyfromcanada to Everyone: (11:42 AM)I am a novice regarding ZKP. Is there ZKP for "normal" JSON? What is the delta between basic (?) ZKP, ZKP for JSON, and ZKP for JSON-LD?
From Nathan George to Everyone: (11:42 AM)Another question: how do you prevent maliciously minimal disclosure. A common schema helps you know to ask for the right attributes to prevent you from being misled. I think, as John mentioned, we can find another way to address that, just another loose end to chase down.
From malwhere to Everyone: (11:42 AM)the NodeJS wrapper that Tobias is referring is wrapping Ursa's BBS+
From Orie Steele to Everyone: (11:42 AM)Yep, my point was Ursa needs binding for ruby / go / java / python / node … then its all the same game :)
From Juan Caballero to Everyone: (11:42 AM)i wanna hear more about domain proofs if there's time
From Micah McG to Everyone: (11:42 AM)Nodejs/typescript project mentioned: https://github.com/mattrglobal/node-bbs-signatures
From Charles Cunningham to Everyone: (11:42 AM)the problem with "normal JSON" is serialising the data in order to hash/sign in an always-reproducible way
From Orie Steele to Everyone: (11:43 AM)https://tools.ietf.org/id/draft-rundgren-json-canonicalization-scheme-00.html
From Charles Cunningham to Everyone: (11:43 AM)JSON-LD provides a deterministic mapping of JSON(+ context) to RDF
From Orie Steele to Everyone: (11:43 AM)And with JSON-LD 1.1 it also supports @json literals using JCS
From Kyle Den Hartog to Everyone: (11:43 AM)Nathan, schemas can still be made common through the use of anchoring a schema to IPLD for example. We didn't see the need to keep the chronological ordering that a ledger provides for schemas.
From Nathan George to Everyone: (11:44 AM)+1 for Stephen, small bite-sized standards let cool new things integrate and take over more quickly. I'm excited for where this can take us.
From Manu Sporny to Everyone: (11:44 AM)This is *awesome*! :)
From Orie Steele to Everyone: (11:44 AM)Yes :)
From Joel Thorstensson to Everyone: (11:44 AM)@Kyle well if you want to have the ability to update and version schemas it might be useful to have chronological ordering :)
From Charles Cunningham to Everyone: (11:44 AM)this is very awesome yeah gonna see how fast I can use this XD
From Nathan George to Everyone: (11:45 AM)We have been working on variable schema credentials and signature improvements for a LONG TIME. Thanks to Mike and Brent and others that worked behind the scenes on the crypto that this builds on.
From Kyle Den Hartog to Everyone: (11:46 AM)Yes, huge thanks to Mike, Brent, and the Sovrin and Ursa communities who have been driving this forward behind the scenes
From Juan Caballero to Everyone: (11:46 AM)+1
From Stephen Curran to Everyone: (11:46 AM)+1

From Charles Cunningham to Everyone: (11:46 AM)+1
From Nader Helmy to Everyone: (11:46 AM)+`
From Kyle Den Hartog to Everyone: (11:46 AM)+1
From Orie Steele to Everyone: (11:46 AM)+1
From Manu Sporny to Everyone: (11:46 AM)+`1
From Oliver Terbu to Everyone: (11:46 AM)Awesome work!
From Nathan George to Everyone: (11:46 AM)Jack++
From Manu Sporny to Everyone: (11:46 AM)q+
From Dmitri Zagidulin to Everyone: (11:46 AM)+1
From Tobias Looker to Everyone: (11:47 AM)+1 so much prior art to recognize!
From Me to Everyone: (11:47 AM)Real kudos to Tobias and team … I am very impressed with the willingness to stare a hard problem down and make a really interesting contribution to the technology .. we are looking forward to collaborating and seeing where this can take us
From Manu Sporny to Everyone: (11:47 AM)https://json-ld.github.io/normalization/tests/index.html
From Nathan George to Everyone: (11:47 AM)John++ Tobias' team has done some real heavy lifting here.
From Micah McG to Everyone: (11:48 AM)🎉👌👏
From Nathan George to Everyone: (11:48 AM)Getting this stuff to come together could have great consequences for semantic concepts for decentralized web schtuff
From John Callahan to Everyone: (11:48 AM)Nathan++
From Me to Everyone: (11:49 AM)This is the https://en.wikipedia.org/wiki/The_Structure_of_Scientific_Revolutions building on the work of others :)
From malwhere to Everyone: (11:49 AM)that's what I'm working on
From Nathan George to Everyone: (11:49 AM)Ursa builds to wasm, etc already. The blockers are mostly at the ledger resolver and wallet layers
From Brent Zundel to Everyone: (11:49 AM)speaking for Ursa: we accept PRs
From Juan Caballero to Everyone: (11:49 AM)flex: emoji
From Me to Everyone: (11:49 AM)++ to PRs :)
From malwhere to Everyone: (11:49 AM)WASM, Go, Java is what I'm working on
From rileyhughes to Everyone: (11:50 AM)😂
From Kyle Den Hartog to Everyone: (11:50 AM)++++++11111 Brent
From Charles Cunningham to Everyone: (11:50 AM)who wants to write a JSON-LD normaliser in rust?
From Andres Olave to Everyone: (11:50 AM)Congrats to all involved
From John Callahan to Everyone: (11:50 AM)a Rust impl would be great
From Nathan George to Everyone: (11:50 AM)_wants_ to or can be cajoled into it?
From Dmitri Zagidulin to Everyone: (11:50 AM)@Charles - depends on your budget :) (re normalizer in rust)
From Charles Cunningham to Everyone: (11:50 AM)XD
From Manu Sporny to Everyone: (11:51 AM)no, seriously, organizations need to start funding this stuff. :)
From Kyle Den Hartog to Everyone: (11:51 AM)Rust doesn't have the greatest JSON-LD implementation so far. There's a half baked implementation, but it could use some love too.
From Charles Cunningham to Everyone: (11:51 AM)I'd like to tbh because having as much as possible in a warm bundle would be awesome
From Manu Sporny to Everyone: (11:51 AM)haha, love the snail onto a turtle reference.
From Charles Cunningham to Everyone: (11:51 AM)yeah I saw that impl but its abandoned :(
From John Callahan to Everyone: (11:51 AM)I'm not volunteering for this, but how about a DSL using LLVM that could compile into different native language impls instead of a language-by-language approach. Just an idea...

From Nathan George to Everyone: (11:53 AM)Jack: Seen that multiple times, it isn't pleasant. That is why I support Rust, it gets you most of the way to that without having to deal with the DSL.
From John Callahan to Everyone: (11:53 AM)You are probably right, Nathan. It would be complex
From Nathan George to Everyone: (11:53 AM)Find David Huseby in a hallway track, he will have you convinced.
From John Callahan to Everyone: (11:54 AM):-)I know Dave
From Manu Sporny to Everyone: (11:54 AM)+1 to CCG... we might be able to get it into the LD Security WG if it's in good shape.
From Nathan George to Everyone: (11:54 AM)Then you should already believe ;)
From Juan Caballero to Everyone: (11:54 AM)domain proofs?
From Dominic Wörner to Everyone: (11:54 AM)Could yo
From Nathan George to Everyone: (11:55 AM)Manu++ the idea that any-old-data gets selective disclosure provability seems exciting in a "be careful what you wish for" sort of way
From Manu Sporny to Everyone: (11:55 AM)yep
From Dominic Wörner to Everyone: (11:55 AM)Could you say something about the advantages comparing to selective disclosure with signing a merkle tree of claims
From Manu Sporny to Everyone: (11:55 AM)it's the corner cases that are worrying :) -- but we have something to latch onto now :)
From malwhere to Everyone: (11:55 AM)flexibility
From Nathan George to Everyone: (11:55 AM)Its much more efficient from a signature standpoint as well
From malwhere to Everyone: (11:56 AM)^^ @Dominicmerkle proofs are large
From malwhere to Everyone: (11:56 AM)BBS+ is very efficient100 attributes in a BBS+ only yields a 3.3Kb proofan that's if you hide every attributeit goes down as you reveal attributes
From Nathan George to Everyone: (11:57 AM)You don't want to have to define the disclosures that are possible or not possible up front, you want to be able to mix and match at presentation time, its harder to do that with merkle signatures
From John Callahan to Everyone: (11:57 AM)Awesome session… gotta 3pm EDT meeting now. BYE!
From Dominic Wörner to Everyone: (11:57 AM)+1
From Orie Steele to Everyone: (11:58 AM)Yes, Mattr is f***ing crushing it :)
From Rouven Heck to Everyone: (11:58 AM)+! Orie :)
From Juan Caballero to Everyone: (11:58 AM)+1
From Manu Sporny to Everyone: (11:58 AM)+1
From Xavier Vila to Everyone: (11:58 AM)+1
From Charles Cunningham to Everyone: (11:58 AM)+1yeah Mattr with JWM as well, amazing
From Juan Caballero to Everyone: (11:59 AM)great paper
awesome thanks
From Stephen Curran to Everyone: (12:05 PM)+1 to session on Indy and BBS+ to figure out what type of path we might want to follow.
From malwhere to Everyone: (12:05 PM)+1
From Brent Zundel to Everyone: (12:05 PM)incorporating bbs+ ld-signatures into Aries/Indy would be a session I'd be very interested in as well
From Juan Caballero to Everyone: (12:05 PM)+1
From mario Bonito to Everyone: (12:06 PM)+1
From Charles Cunningham to Everyone: (12:06 PM)+1
From Andrew Whitehead to Everyone: (12:08 PM)Maybe a technical session on range proofs & the JSON-LD approach
From Micah McG to Everyone: (12:08 PM)bbs+ ld-signatures => indy +1

From Juan Caballero to Everyone: (12:08 PM)I was saying Booo-urns! I was +1ing bbs+ ld-signatures => indy/ARIES, fwiw :D
From Drummond Reed to Everyone: (12:09 PM)Schemas should be able to have DIDs.
From Dmitri Zagidulin to Everyone: (12:09 PM)q for @Kyle - schemas don't need to be chronologically ordered, but do they need to be (sem) versioned?
From Rouven Heck to Everyone: (12:09 PM)+1 Kyle - ledger agnostic
From Nathan George to Everyone: (12:09 PM)Careful with that generalization, ordering on those objects have some benefits to protect against broken entropy problems, but generally I agree.
From Charles Cunningham to Everyone: (12:09 PM)their versioned editions should remain immutable (like all versioning ideally), so a CAS seems fine right?
From Kyle Den Hartog to Everyone: (12:09 PM)Potentially and with the use of IPLD the CAH should change by doing that meaning a new IRI should be produced I believe
From Nathan George to Everyone: (12:10 PM)The bigger issues to address are around trust for data subsets without a complete data definition And how immutability affects that trust
From Nathan George to Everyone: (12:11 PM)You need to be careful to preserve independence between the issuer and verifier (including data access or DoS concerns)
From Andrew Whitehead to Everyone: (12:11 PM)I'd prefer a DID URL to a DID ;)
From Kyle Den Hartog to Everyone: (12:11 PM)Yup, and I believe immutability is valuable, but not necessarily the chronological ordering which is why I was thinking IPLD seems like a natural fit for this.
From Andrew Whitehead to Everyone: (12:12 PM)(or DRI)
From Drummond Reed to Everyone: (12:12 PM)Why would you prefer a DID URL to a DID if the DID took you directly to the immutable object?
From Rouven Heck to Everyone: (12:12 PM)yeah, immutability + context addressing
From Drummond Reed to Everyone: (12:12 PM)+1 to the immutability
From Orie Steele to Everyone: (12:12 PM)I prefer to use a URI… which might be content addressed… but might not be.
From Charles Cunningham to Everyone: (12:12 PM)yeah IPLD seems ideal, the DID approach it seems would also be immutable but brings in a variety of DID methods which are not really necessary I think
From Dominic Wörner to Everyone: (12:13 PM)Is a schema really the same as a ld context? The schema could tell what me what is required in a credential. The context tells me what attributes could be expected
From Drummond Reed to Everyone: (12:13 PM)"trust framework" = "governance framework"
From Joel Thorstensson to Everyone: (12:13 PM)What we do with Ceramic is creating updatable documents on IPLD which allows for versioned schemas :)
From Drummond Reed to Everyone: (12:13 PM)Cool!
From Charles Cunningham to Everyone: (12:13 PM)^^ similar to like Tupelo?
e.g. deltas on a piece of data as IPLD fragments?
From Andrew Whitehead to Everyone: (12:14 PM)@Drummond maybe it's old fashioned but I like when a DID resolves to a DID doc, not a schema
From Joel Thorstensson to Everyone: (12:14 PM)Similar to Tupelo, but anchored on blockchains :)
From Nader Helmy to Everyone: (12:14 PM)ceramic network https://github.com/ceramicnetwork/specs
From Charles Cunningham to Everyone: (12:14 PM)very nice
From Dmitri Zagidulin to Everyone: (12:14 PM)@Dominic - re the difference between a schema and a context — so, there is SOME overlap, in the venn diagrams between them? But like you said, their purpose is somewhat separate.
From Dmitri Zagidulin to Everyone: (12:15 PM)@Dominic a @context is more of a 'schema migration map'
From Drummond Reed to Everyone: (12:15 PM)@Andrew, the specific proposal is for the immutable object you are identifying to be IN the DID document you get back.

From Dmitri Zagidulin to Everyone: (12:15 PM)or like.. definition migration.
From Manu Sporny to Everyone: (12:15 PM)q+ to suggest we should change the spec!!!:)
From Charles Cunningham to Everyone: (12:15 PM)oooooohhhh ceramic === 3boxall is clear now
From Joel Thorstensson to Everyone: (12:15 PM):-)
Will have a session on how Ceramic works in session 4
From Drummond Reed to Everyone: (12:16 PM)Brent and Ken Ebert came up with a very elegant proposal for doing just that for any immutable object you can render in a DID representing.
From Nathan George to Everyone: (12:16 PM)I like the idea of normalizing those into JSON-LD type language so they can be inline or referenced, then we get more awesomeness
From Drummond Reed to Everyone: (12:17 PM)Drummond just fainted :-)
From Nathan George to Everyone: (12:17 PM)Inlining has disclosure consequences, so yeah...
From Orie Steele to Everyone: (12:17 PM)Let the battle begin
From Nathan George to Everyone: (12:17 PM)It was Manu that said it, that means he will lead the effort right? ;)
From David Waite to Everyone: (12:18 PM)+1
From Manu Sporny to Everyone: (12:18 PM)haha, definitely not. :)
From Orie Steele to Everyone: (12:18 PM)We got this.
From Manu Sporny to Everyone: (12:18 PM)Parallel == more efficiency gains.
From johnnyfromcanada to Everyone: (12:18 PM)Thanks!
From Dmitri Zagidulin to Everyone: (12:18 PM)lol
From Manu Sporny to Everyone: (12:18 PM)https://github.com/msporny/dnaclone instructions there ^
From Me to Everyone: (12:18 PM)Thanks all!!!
From Brent Zundel to Everyone: (12:18 PM)perfect!
From Me to Everyone: (12:19 PM)I captured the chatFor the notes I expect

KERI (A) Key Event Receipt Infrastructure: A ledger agnostic framework for decentralized identity.

Tuesday 2F
Convener: Sam Smith
Notes-taker(s): Sam Smith

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

KERI unifies many DID methods types.
Link to notes (slide deck) and white paper, provided by Sam Smith:

Notes/Slide Deck:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI2_Overview_AB_IIW_2020.pdf

White Paper:
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI_WP_2.x.web.pdf

Verifiable Credentials for Trade Items

Tuesday 2G
Convener: Paul Dietrich, Gena Morgan, & Phil Archer (GS1)
Notes-taker(s): Phil Archer

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link provided by Phil Archer to verifiable credentials Slides:
https://docs.google.com/presentation/d/1Vlt--R5ju2c79vNUvtmNGQK_s4Qnhgx8/edit#

Session is about how we can apply verifiable credentials to 'trade items' - products in stores, shipments, etc

PD (Paul Dietrich) gives brief overview of GS1.
... Want to look at how this emerging tech can impact our members.
... Slide 8 shows the kind of things that consumers want to know about a product
... facts come from different sources now - don't always want to hear it from the brand
... provenance is always important for products, especially food.
... Slide 9 shows more detail
... Paul asks the group how they see this issue - 'what do you see?'
... Who is able to make claims about a product? or to present a credential?

Mikhael: Pleased that GS1 is here. You guys are basically a global monopoly - I sell on Amazon. You're often under the radar - good to see you.
... One crucial piece of info is "what platform has this product been verified on" Amazon approves products, as do others. That's a potential SEO score. Good. Trust scale can increase.

PD: Some way that retailers can endorse brands.

Mikhael - yes, like Amazon has 'Amazon Choice'

Gena - we are federated, we're not one organisation as such, but as a federation, we do ensure uniqueness across the world.
... Not our first IIW - we're trying to see how this tech can help.

Siva - great initiative on the trade items. Do you also see claims and assertions on the traders themselves? trustworthiness of the buyer and seller?

PD - Yes, for sure we'll see that. We'll see a lot of assertions made between the trading partners.
... we see use cases for on-boarding on trade partners. It currently takes many forms, often paper-based. VCs have the potential to make that more streamlined.
Keith - VCs for retailers to access my stock level info. Employees can have access to that.

Karyl - my co. works on DIDs and VCs. We have some customers and partners in the food distribution space. Also expanded to PPE in Covid crisis. Authenticating the vendor is a real issue.

Paul Jackson - who is the holder in this model? Where are the VCs going to be held? And how found?

PD - may get to wallets through the brand, or through registries. It depends where you are in the supply chain. I see wallets being important. But registries too.

Heather V - based on my research... when you talk about the ID of a product on a supply chain, it's not the same as a person (scribe missed a bit)
... Early upstream, nothing has a barcode yet. So tracking that is hard.
... Asset passports are a poss way forward. An object that will stay the same and change ownership is one thing. Digital Twins are another. Pre-barcode there is a lot of data that needs to be associated with it. A wallet is a non-physical ID representation that data can be associated with. You need the data collected associated with the object accessible in a digital space. The data needs to have fine-grained access rules.

PD - really good insight (scribe apologises for missing some of it).
... Trade items don't have privacy issues.

Heather - my report is at https://bit.ly/GSCreport

Vic Cooper - when you buy an item, there's a whole chain of connections that are really powerful.
... If I buy, it's added to my list of things I own, I should be able to use that connection to get support. getting all that different info could start with scanning a barcode. Those connections could create those customer experiences

PD - now is a great time to be exploring that. GS1 is working on creating those links (GS1 Digital Link)

Gena - plugs the demo tomorrow.

Vic - how do you go from a barcode to detailed info. Barcodes are at class level. Not serialized.

Gena - explains more granular IDs, 2D barcodes etc.

PD - there are certain classes of products, like bottled water, that are not serialized. Others - more valuable items - do. Serializing costs money.
Paul Jackson - do you see any governments requiring serialization? Things like batch numbers etc.

Gena - talks about pharma now does requires serialization.
... It's also about cost, as Paul said, but lot level can be important for food recalls.
... We often focus on batch-level info. Mentions the Romain Lettuce example. It could be the basis of targeted recalls. Lot level ID is certainly something that govs and industry are focused on.

PD - back to slides (slide 10)
... we think VCs will be important.
... assertions usually made by an organization. We're not seeing a lot of cases where the trade items are making assertions (I'm a strawberry and I got too hot today). The content of the claims we see are generally very broad. The vocabulary around that is going to be quite large too.

PD - talks about the W3C VC spec. It says that URIs should, ideally, be resolvable.
... We've seen examples of claims using DID-based subjects, others that use domain names as subjects.
... For trade items, we think it makes sense to use Digital Link URIs. It's a resolvable URI (HTTP). That might then resolve into a set of links.

Guillaume - you said that the DL can be a VC subject. Does the DL contain claims?

PD - the DL is an identifier, it is a URI. It maps a physical label, like a UPC, into a URL. You can map between the GS1 identifier and the URI and vice versa.
... That translation can happen easily enough (see code in GitHub https://github.com/gs1/)

Haiku notes:
Trust products
Through the supply chain
Track and trade
With GS1 barcodes

[I like that, thank you!]

PD - plugs tomorrow's demo and session on resolvers.
PD - talks through slide 12
PD - talks about GS1 Digital Link a little more, Yes, it does support query strings, but best to use just paths.

Melanie - seeks clarification that id.gs1.org is not the only resolver.

PhilA - emphasizes that there can be any number of resolvers, each is sovereign - see tomorrow.

PD - Talks about the Web vocabulary for describing products.
... gives an example of a term from the GS1 web Voc (https://gs1.org/voc)
... If you're making claims about products, I recommend that you use our schema.org extension to do this rather than invent your own (if it includes it). reach out to us if there's something missing.

[Discussion of the GS1 Web voc. Not originally designed for VCs (it's older) but this is an important use and part of its growing importance at GS1]

Paul Jackson - is it widely used?

[PhilA - talks about mapping between GDSN and the Web voc)

PD - shows slide 14 - an example VC.
... Making use of the GS1 Digital Link URI means that you're using the IDs already used throughout supply chains.
... It's resolvable (through a resolver)
[Scribe missed a bit, sorry]
Drummond asked a question about provenance of information
Gena - chain of custody info is always important. That can be linked back to understanding that the person who had custody is themselves verified.
Gena - things like what are the minimal set of credentials for a supplier? That's a decision point for the future.
... My understanding is that the governance stack will be important here, maybe the top 2 levels.
Drummond - that's a terrific use case. And you work in so many supply chains. Having them fit within a governance framework and the Trust over IP Foundation is designed to support exactly that kind of thing.
PD - goes back to the VC example. When would you use a DID? We have a GLN to identify a partner? What makes sense in a global supply chain?

Drummond - this is so prototypical. I first met the GS1 team about 2.5 years ago and was so pleased to see you.

== End of session ==
Chatlog:
From Guillaume to Everyone: 07:00 PM Hello!
From Gena Morgan to Everyone: 07:01 PM howdy
From Me to Everyone: 07:02 PM Slides are at https://docs.google.com/presentation/d/1Vlt--R5ju2c79vNUvtmNGQK_s4Qnhgx8/edit#slide=id.p1
From Drummond Reed to Everyone: 07:09 PM I first met the GS1 team at IIW about 2.5 years ago. They have been a pioneer in figuring out how DIDs and verifiable credentials will work with the global supply chain.
From Nicky Hickman to Everyone: 07:13 PM Does the credential associated with the Thing (product) not follow it's route through the supply chain
From Me to Everyone: 07:15 PM Not necessarily, Nicky. Supply vchains are enormously complex
From Drummond Reed to Everyone: 07:16 PM I believe a classic pattern we'll see in supply chains is credential registries, where the holder is designed to be a directory available either publicly or to the members of the supply chain who need access to it.
From Nicky Hickman to Everyone: 07:16 PM Does the VC not follow the liabilities expressed in INCOTERMS for example?
From Heather Vescent to Everyone: 07:18 PM Tracking and digital identity on the supply chain: https://bit.ly/GSCreport
From Me to Everyone: 07:31 PM And we have open source code for this https://github.com/gs1/
From mitfik to Everyone: 07:33 PM +1
From Gena Morgan to Everyone: 07:35 PM important to understand that the domain could also be the brand example.com/gtin/614141123452
From Nicky Hickman to Everyone: 07:37 PM Could this help with after market care e.g. product recall e.g. exploding fridges, faulty cars.... that's a great use case Have you explored how these resolvers might link with data use in cargo communities & freight forwarding communities eg in a container port system
From Jeffrey Hallett to Everyone: 07:38 PM Are QR Codes equally applicable in this discussion?
From Me to Everyone: 07:38 PM Jeffery - yes. Nicky - maybe we should meet in a garden afterwards?
From Alex Rosen to Everyone: 07:40 PM Are there restrictions on use of things like the vocabulary or is that all open?
From Gena Morgan to Everyone: 07:40 PM It is open
From Me to Everyone: 07:46 PM https://gs1.org/voc

COVID Apps: What Could Possibly Go Wrong?

Tuesday 2I
Convener: Phil Wolff
Notes-taker(s): Phil Wolff

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Risks and Threats:

- Surveillance

    - Government national security, internal security services coopt public health data. See Palantir.
    - Doxing with immune/sickness status can hurt the individual, the family, workplace, community.
- Project risks (breaking scope, schedule, budget, quality)
    - Pushing too fast; making bad choices.
    - Poor coordination (duplication, contentious initiatives)
    - Semantics for passport/EHR data are changing rapidly, vary widely
    - Expedience trumping better architecture, public policyIntegrating with systems that are not aligned to privacy values.
    - Incomplete solutions
    - Poor job setting expectations with healthcare organizations.
- Bringing technical solutions to relational/relationship problems
- Commoditization of identity vice keeping it transactional
- Too tightly coupling identity with medical data
- Human behavior
    - Heisenberg effect? Can passports with credentialed data alter their behavior in good ways? Bad ways?
    - Perception of immunity passports (content) can alter behavior, social norms. https://en.wikipedia.org/wiki/Gattaca
- Technical risks
    - Bluetooth false positives at a very high rate?
    - Missed opportunity: Not building on existing infrastructure, like immunology records provided by clinics to parents for their kids to schools.
    - Excluding humanities professionals from design and oversight. Social scientists, for example.
    - Not modeling caregivers, familial relationships, proxies and other people who need legal or practical use of data.

- Excludes billions of people without the latest devices or connectivity.

- Contact tracing can produce panopticon if privacy architecture is broken
    - https://www.apple.com/covid19/contacttracing/
    - https://github.com/mit-ll/BluetoothProximity
    - http://web.mit.edu/webcast/pact/s20/
    - https://www.sicpa.com/news/covid-19-immunity-passport-secured-blockchain-enable-deconfinement

- Living wills and durable powers of attorney not available conveniently/digitally
- Does this framework account for humans who don't care about the harm they cause others?
- Not designing first for highest impacted populations
- Not designing for the offline

Action:

- Code of Ethics for vetting design and architecture. Potentially Trust Over IP (ToIP)

- Best practices for building apps with sensitive data
- Social Contouring, to meld humanities with other
- Guardrails for bad actions and audits to catch them
- Get the Tempo right:
    - Stop admiring the problem, fix it now, people are dying
    - Go slow to go fast

Apps list:

- https://appassay.org/ (focused on analyzing which apps implement which features using which approach -- e.g. anonymous/pseudonymous/… because all have very different privacy etc ramifications)
- https://www.apple.com/covid19/contacttracing - Apple / Google contact tracing
- https://www.google.com/covid19/ - Apple / Google contact tracing
- TraceTogether: Singapore Government Technology Agency (GovTech) and the Ministry of Health (MOH) https://www.tracetogether.gov.sg/
- Polish Govt app to force people to stay in quarantine: https://futurism.com/the-byte/poland-app-patients-quarantine?
- MIT Safe Path app: http://safepaths.mit.edu/? Private Kit: Safe Paths; Privacy-by-Design Covid19 Solutions using GPS+Bluetooth for Citizens and Public Health Officials
    - http://news.mit.edu/2020/safe-paths-privacy-first-approach-contact-tracing-0410
- Covid-19 self assessment tool: https://www.humandx.org/
- Open Health app https://www.openhealth.cc/ Compiled great resources for #covid19 at https://www.openhealth.cc/ including tracking testing facilities and a symptom tracker app.
- https://github.com/DP-3T/documents/ Decentralized Privacy-Preserving Proximity Tracing
- Bluetooth Pooling: https://marcdavis.me/wp-content/uploads/Publications/2005_ProceedingsUbiComp2005_BluetoothPoolingEnrichCoPresenceInfo.pdf
- CommCare for COVID-19 https://www.dimagi.com/
    - Some of the template apps are, per list here:
        - "Contact Tracing: WHO First Few X (FFX) Cases"
        - "Port of Entry Surveillance"
        - "Facility Readiness and Supply Chain Tracking"
        - "Lab Test Tracking" (announced)
        - "Health Worker Training & Monitoring" (announced)
- https://github.com/mit-ll/BluetoothProximity
- https://www.sicpa.com/news/covid-19-immunity-passport-secured-blockchain-enable-deconfinement
- WHO on Contact Tracing @ https://www.who.int/csr/resources/publications/ebola/contact-tracing/en/
- https://coviid.me - Contact tracing for Africa doesn't require a cell phone at all.
- www.hieofone.com thanks https://github.com/HIEofOne/Trustee-Immunity-Passport

KERI (B) Key Event Receipt Infrastructure: A ledger agnostic framework for decentralized identity.

Tuesday 3A
Convener: Sam Smith
Notes-taker(s): Sam Smith

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

KERI unifies many DID methods types. Continuation from KERI (A).
Link to notes (slide deck) and white paper, provided by Sam Smith:

Notes/Slide Deck:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI2_Overview_AB_IIW_2020.pdf

White Paper:
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI_WP_2.x.web.pdf

Introduction to UMA - User Managed Access (101 Session)

Tuesday 3B
Convener: George Fletcher
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Links to the slide deck & notes:

https://kantarainitiative.org/confluence/download/attachments/17760302/2019-04-30%20IIW%20UMA%20101.pdf?api=v2

https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-federated-authz-2.0.html

https://kantarainitiative.org/confluence/display/uma/Home

https://iiw.idcommons.net/Use_%E2%80%93_Managed_Access_(UMA)_%E2%80%93_101_Session

Malware Attacks Against SSI: How SSI may be the perfect honeypot if you're not careful.

Tuesday 3C
Convener: Michael Lodder
Notes-taker(s): Kyle Den Hartog

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to slides: https://docs.google.com/presentation/d/15rK2DfRgQksgGy_H9q5d_mweNC-jJdmqvkMcuoyoZ7E/edit?usp=sharing

Provisional threat model about Indy from @stephen Curran https://docs.google.com/document/d/1M1-Xi99-pkgDnFiYmoc12b3eMgkyBC_HqYZMrTrCkCI/edit

Aries RFC about credential fraud: https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0207-credential-fraud-threat-model

Link to paper by Heather Vescent and Bob Blakley:
https://www.researchgate.net/publication/330542765_Shifting_Paradigms_Using_Strategic_Foresight_to_Plan_for_Security_Evolution

Link to DID/VC IoT threat model: https://link.springer.com/chapter/10.1007/978-3-030-39047-1_16

Identity in DXOS Collaboratively Editing Document In Decentralized Application with Groups and Multiple Devices

Tuesday 3D
Convener: Kaliya Young & David Boreham (Wireline)
Notes-taker(s): Kyle Den Hartog

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Alan Karp: We built a peer to peer file sharing tool called SCoopFS (the F is silent)
https://dl.acm.org/doi/pdf/10.1145/1753846.1753966?download=true.

One thing we learned was that people don't want to see those crazy URLs. There is also a tech report with more detail at https://www.hpl.hp.com/techreports/2009/HPL-2009-53.pdf.

Party is the name for the eventually consistent regulated data type.
When inviting a device to a user. When inviting a new person to the par
Doesn't need to be a URL. What is being transmitted is the identifiers.
CRDT editor.
Questions: How can people leave the party? How to do chained revocation?

Evernym AMA

Tuesday 3E
Convener: Richard Esplin
Notes-taker(s): Drummond Reed

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Introductions: Where are you from, and why are you interested in Identity.

- Privacy "making sure our kids aren't monitored everywhere"
- Trusted computing and trust issues in computing
- Bringing people together
- Having a way to truly prove who you are while retaining control
- Interesting technically (and increasing interesting politically)
    - Removing control from gov't
- Lots of efficiencies to be gained by fast verification
- Identification of the entities in a supply chain
- Telecommunications (peer wise communication) using SSI/DIDComm
- Governance and how it fits in identity infrastructure

Evernym use cases:

- https://www.memberpass.com/ - The digital credential being developed by CULedger
    - Give customers surity of knowing who the person they are talking to online is who they say they are
- Transferring medical personnel with VCs, went from days to minutes to transfer
- Prove doctors are not sick the day before
- Alberta Credentials Ecosystem (ACE)—https://www.aceprogram.ca/

Question about what our technical focus areas are. Richard's answer:

- We are very happy with the work we've done on the Hyperledger Indy/Ursa/Aries stack in terms of core DID and VC functionality
- We are very excited about new technical functionality like Rich Schemas
- Moving from the abstract/theory to actually doing it is very exciting
- Much of our focus right now is on the rest of the business problems, tooling, and governance needed to deliver a "whole product" to customers

Verity and LibVCX?

- Evernym started with code that looks like hyperledger and aries
- The core of it was a library calle LibVCX. Got a lot of mileage, but was hard to keep revising to bring it current with Aries interop specs.
- The work on interop has revealed a lot about the specs and where the gaps on interop really are
- The Verity product was a rewrite, starting anew, designed to take advantage of all the learnings. Verity will use Indy and the Aries libraries but builds on top of those components.
    - Will not be put back into hyperledger

What do you open source vs keeping closed?

- Open sourcing is very time consuming
    - Have to get alignment through the org

- Accelerated adoption that comes from openness Vs. commercial viability
- Controlling your business to make money
- Take into account how "easy" something is, if it's easy then you should probably just open it
- Write down and stick to principles for when to open source
    - Publish these principles for contributors
- Will have another session dedicated to this topic.

Shift from Federated IDs to SSI changed everything, and it is much better.

- Short term is an integration play: SSI credential issuance is about how someone gets their identity. Traditional IAM systems pick up once the identity is granted, and integrates throughout the enterprise.
- Long term: SSI is a paradigm shift. Enterprises have a hard time buying something that is new, but we are at the tipping point where enterprises can by a native SSI solution.

Where the identity industry is going, especially regarding KYC and AML.

- South African banks are experimenting with KYC (get the national ID into the bank), but staying away from AML (it's opinionated has more liability).
- Eventually there will be primary SSI credentials, but the industry can bootstrap with secondary credentials: proof that a primary credential (physical) was presented..
    - When ingesting an identity document, there are a lot of edge cases that makes it hard to process.
- Over time, there will be a "supply chain" of credentials. Issuers who check credentials, and provide new credentials for a specific purpose within a different trust model.
- Goal is to achieve a "web-like" adoption model. We publish our data so others can link to it, and then we can link to their data . . .
- CULedger's Memberpass originally thought "KYC / AML is the problem we should solve". But currently that is the banker's job. It is a big problem, and technology is a small part of it. Someone has to accept the liability of the credential. So focus currently is:
    - Making things inside the credit union easier (authenticate customers).
    - Prove to a 3rd party that the person is an actual human.

https://www.r3.com/videos/building-global-payment-networks-for-credit-unions-corda-settler-and-self-sovereign-identity/

Related to adoption, do we have efforts in the works to make SSI a built-in browser standard so that for example consumers can have a built-in DID wallet in the browser?

Child Safety Online: SSI, VCs, Governance, Guardianship, GDPR

Tuesday 3F
Convener: Johnny Hermann
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

SSI, VCs, governance, guardianship, GDPR

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slack: https://iiw.slack.com/archives/C01291AMSK1

Problem Statement (Initial)
Anyone interacting online, in particular children (and their guardians), should be able to trust with high certainty that rigorous verification (to an acceptable transparent degree) has been assessed on other people (or entities) they are interacting with, while still complying with data protection regulations regarding personally identifiable information (PII).

How to:

- Verify claims made by users interacting on social media and games, starting with *age-range brackets* ("child", "teen", "adult", etc).
- Build or leverage a non-profit to establish governance model, legal compliance, technical solution, etc.
- Bootstrap network effect to get end-user buy-in and uptake.
- Structure guardianship relationship over DIDs and VCs, in particular between parents and children.
- Ensuring compliance with data protection regulations, including GDPR, CCPA, Pan-Canadian Trust Framework (PCTF), etc.

Conversation Notes
UK Law (rejected) - Required age-verification for sites online
Potential social failure for required verification of age online.

Guardianship

- Facebook Kids - Has controls, but verify as guardian via own Facebook account
- No proof I was actually the guardian.

Volunteer Ottawa - Vetting volunteers
OAuth
OpenID Connect - Identity Assurance Specification (but no DB behind it)
https://openid.net/2019/11/14/openid-connect-for-identity-assurance/
Give people a reason to sign up.

Covid:

- driving online use
- different cultures
- different problems (contact tracing, immunity passports)

- School online - awareness of children online, exposure to “internet”. School as data provider?
- Can we leverage awareness / momentum?

Schools have a register of children ages / brackets. But can of worms regarding legality, liability, etc.

Volunteer Manitoba
Insurance & liability issues
No governmental solution
Vetting volunteers for work with children, seniors, etc.

Vulnerable Sector Check (subset of Criminal Record Check)
2-on-1 system, 911 (emergency), 311 (city), 211 (community)

Demand-side increasing:
- Covid
- UK Age-Appropriate Design Code (passed Parliament, under impl review)
    - All websites (unlike COPPA in US)
- NGO - Child protection space

Narrow scope to gain traction
Limit trial to MVP, on say one gaming platform, one game - ratchet up from there

Connections / Contacts:
- Neil Thomson - neil.thomson@queryvision.com
- Phil Archer (GS1 but, for this, phil@philarcher.org)
- Randy Warshaw, rwarshaw@yahoo.com
- Moira Patternson

Minors do not necessarily have real-world IDs, let alone tech (like phones / digital wallets).

Tech:
- Truu
- Evernym

Project in Zambia with high school kids. They are getting a certificate of completion of the course materials they pass in filmmaking. Verification of credentials in countries depends on legacy systems that will vary. SSI is supposed to be user-centric. Why is it always assumed (it seems) that the government has to issue identity attributes?

VC & Open Badge Linkage

Tuesday 3G
Convener: Gabe Cohen (Workday)
Notes-taker(s): Orie Steele, Nikhil Wadwa

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Open Badges - https://www.imsglobal.org/sites/default/files/Badges/OBv2p0Final/index.html
VC Data Model - https://w3c.github.io/vc-data-model/
Spec to be hosted here - https://github.com/workdaycredentials/specifications
Slides here -- https://docs.google.com/presentation/d/1XJjyt04BaCtSLE1_KMa4ysOgh3vsDeK48d-jEPheKP8/edit?usp=sharing

* IMS Global is the standards body behind badges
* Badgr and Credly have platforms for hosting badges
* Pretty picture with JSON data
* Millions of badges in the world today
* Used at Companies and heavily in the education space
* Workday implemented badges according to the Open Badges spec

* We've represented the image and the data that backs a badge in the evidence field

* There's a notion of a badge class
* Metadata about a badge, image, and who issued it

* This data is hosted on a website

* The credentialing space W3C and DIF, etc.
* VCs are much less mature than the badging specification and are more security oriented

* Today you can issue badges to emails, phone numbers, and URLs
* We are introducing DIDs for issuers and recipients

Today badges can be issued to

- Emails
- Phone numbers
- URLs

Workday implemented badges based on OpenBadge specification
Open Badges support JSON-LD,

Can be used to represent many things, including Amazon Web Services Solutions Architect
A Badge Class describes metadata about the credential and issuer.

Badges are meant to be public, so privacy concerns are low.
Badges are more informal than VCs, still verifiable

Verifiable credentials are supported in workday mobile app

How can Badges be VCs?

Plan to add DID support to OpenBadges
Badges are less serious than traditional VCs, still badges are verifiable

Issuer and Holder can be the same, and be a DID.

Plan to merge VCs and badges to use best of both worlds and drive more adoption
Badge and Credential are linked. Badge is public, Credential has sensitive details, and goes to the holder.
The spec defines how badges and credentials are linked.
New changes to spec:

- The evidence section allows you to issue/ verify the challenges
- The BadgeClass contains the endorsement
- Nothing has changed in the credential

* Comparison of Badges and VCs
* Badges are discoverable and sharable with lower trust “fun”

* We would like to bridge them together by using the same identifier between the badge and VC
* We can extend the badge representation to hold the full set of claims
* All badges are VC backed

* Extension represents claim data
* Make use of the holder’s DID Doc
* Expose a service endpoint to interact with the holds to run a proof request for the VC

* Is a challenge is for authenticity of the badge? - Orie Steele
* Trust is based in the hosting of a badge
* The VC provides a better trust mechanism

* Extension that brings in claim data into the open badge
* And a link to challenge the VC if needed

* Endorsement linking them in the existing badge class

A VC could carry a number of badges - VCs could be likened to containers

Education industry has responded positively to the container model

The credential service can facilitate selective disclosure.

- E.g. job experience can be published publicly, and can be challenged for salary range
- users can treat the badge as a presentation layer around the VC - and attributes of the VC can be selectively disclosed by the user

Verifiable Credential Service is a kind of “inbox” that will forward requests to a user mobile device.
IMS Global has a group tackling autonomy of skills

Adding DIDs to badges allows students to carry their achievements with them - and the ability to combine them with VCs is important as well

DIDCOM working group at DID still hasn't got to credential exchange

Having a DID present in a badge raises correlation aspects - we are exploring a few different models related to that - this is also an ask by the IMS folks

Credentials could be used to establish reputation - badges could also be received anonymously

Presentation of ones identity is typically used for trust access - more privacy based secure thing would be instead of establishing identity - establish proof of permission to access

Badges and VCs should move towards allowing the user to share whatever they want

Placing selective disclosure in user hands is important - e.g. piano player badge / selectively show or hide experience

Work will take place in Aries wg around cred exchange/mobile in coming months

* You can add a service to your DID Document to present an endpoint for challenging for the VC

* Is this a Workday proprietary service or part of the ID Hub? - Orie
* This could be an endpoint to an agent that can respond to requests
* Will forward the request to their wallet

* You mentioned that there was a 1-1 linkage, but badges. A VC can hold more information than a badge. This reminds me of a container. Once they standardized on the containers they could be transported anywhere. Are VCs like containers that can carry any data type? - Timothy Ruff

* This specification is not published yet.

* Open Badges are more well known than VCs. The industry is more matured in the OB area.

* RWoT embedded a badge inside of a VC.

* Are you using the badge as a presentation layer of the VC?
* Is the badge signed? - Orie

* No, the badge trust is oriented in the hosting domain.

* The VC has done discoverability. You want it in a public space with a limited amount of data.

* Is there anybody from Learning Machine or Highland working on this? They seem to be in the same space.
* We've talked to Kim Duffy (coauthor of RWoT paper).
* This was presented to Kim's W3C working group.

* VCs have concrete use cases. Badges tend to be used for more silly purposes as well as things like Skills. This makes bringing them together more difficult.

* Orie - always look for the badges attached to a Github repo. Look at testing badges and others to judge the maturity of the project.

* The way that we do TLS might have to shift from having a client that can do proof requests. - Tim

* Transmute has a GitHub DID method. We like GitHub actions. One of the things that we looked at was using the portable web wallet and checking that into a repo and then checking in the public key into the repo and have it sign commits with that key. Turn on only accept commits from certain issuers. You can generate VC pieces to automatically update the badge.

* Are you guys working with the ILR wallet spec?
* We are aware of what's happening there. As far as our contributions, we are working with them in their CLRs.

* In the stacked credential content/scope, you have there VCs with skills and then based on an aggregation of skills, you can earn something. I think that this is what credentials engine is doing. The linkage is the standardization. - Matthew Hailstone

* IMS Global has a group focusing on accreditation (autonomy of skills). CASE competencies and academic standards exchange.

* Most of the BC gov case has to do with licenses. You might have a badge you were licensed. I haven't seen anything with a community holder in that system.
- Sam Curren

* With VCs the user controls where the VC is held. Are you saying that the Open Badge provides visibility and the VC does not?
* Badges have a "backpack" that is similar to a wallet, but Is hosted.

* The DIDComm group has yet to get to credential exchange. If you have an endpoint, you can send a message encrypted with a key. The verifier asks what they are willing to prove, and the holder can accept. This is coming, but isn't there yet. One of the downsides is that it makes the credential correctable. In the case of a badge issued to a DID. There could be one persona, or it could be that each badge is issued to a unique DID.
- Sam Curren

* The proof of control over a DID is an ask from the IMS group.

* You present a challenge that needs to be signed with the DID. Generally called DID Auth. One of the things that the VCs offers the badge world, you can have anonymous badges. Maybe this turns badges into a form of reputation. Being able to present the silly things as a form of reputation is interesting.

* For resource access we tend to prove who they are vs do they have permission. I can prove who I am and then they can look up my permissions. Or the permissions can be baked into the VC.

* Having a wallet that can hold both public and private data could be huge.

* I like that Badges could be a public presentation of a Credential. - Sam Curren

* It feels like Badges are institution centric. This allows a more user centric approach. Allowing me to receive badges that I can choose selectively to display. - Sam Curren

* Selective disclosure would be very valuable. If I move to a new town and spent a lot of time in the PTA, I might not want to expose that if I don't want to get sucked back into the PTA.

* IIW presentation on selective disclosure that might be interesting.
-Tobias Looker

Vectors of Authoritarianism

Tuesday 3H
Convener: John Wunderlich
Notes-taker(s): John Wunderlich

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Authoritarians want to know:
- Where you are?
- What you are doing?
- Who you are meeting?
- What are you thinking?
- How can we manipulate your behavior?

All of this is related to identity, so how do we identify identity solutions and policies that will fail towards digital autonomy instead of authoritarianism

The Zoom Chat:
From Jeff Orgel to Everyone: (03:32 PM)Authoritarianism - What are the vectors?
From Me to Everyone: (03:34 PM)How to build a Digital identity System that fails to digital autonomy and not authoritarian Issues of control. Who encrypts, who controls?
From Jeff Orgel to Everyone: (03:36 PM)How can enabling a globally intrusive tool not be too intrusive and fails to digital autonomy? Iss this SSI & DIDs doing there thing?! ...doing "their" thing?
From Lawrence Liu to Everyone: (03:37 PM)Plus there is also the other party called "HACKERS" that will take over the data or system
From Marc Davis to Everyone: (03:37 PM)BLTS= Business, Legal, Technical, Social
From Me to Everyone: (03:39 PM)How do you create a social commons Responsible people don't need rules
From Jeff Orgel to Everyone: (03:40 PM)Culture shifts optics on what is funny or not. Will it have the same reshaping of our opinion authoritative invasiveness?
From Marc Davis to Everyone: (03:41 PM)One of the challenges with authoritarian systems is that when the "Legal" vector is no longer usable, what do you do? What happens when the rule of law is not honored by authoritarians?
From Jeff Orgel to Everyone: (03:43 PM)Isn't there orthogonal balance.

From Me to Everyone: (03:44 PM)Every solution space will have a cost. How to evaluate?Surveillance and predation go together.OK with things for a short period of time or a particular context.
From Marc Davis to Everyone: (03:49 PM)Two design vectors:
From Me to Everyone: (03:49 PM)Game theoretic dynamics of disclosure in different contexts
From Marc Davis to Everyone: (03:49 PM)1) Permanence of digital records
From Me to Everyone: (03:49 PM)Controls need to be at the point of collection.Contact Tracing therefore needs to be voluntary.
From Dan DuBeau to Everyone: (03:51 PM)he challenge, I think, is around transparency and accountability. Is it reasonable to allow governments to gather information in support of their charter so long as they are held accountable for breaking the rules? If they overstep authority, the most important thing is to know that it happened. I feel the problem starts here. Most of the time, we don't even know it's happened.
From Marc Davis to Everyone: (03:52 PM)2) Dangers and game theoretic dynamics of levels of identity (anonymous, pseudonymous, real, etc.) in identity disclosure when cost of disclosure could be one's life
From Marc Davis to Everyone: (03:54 PM)Where is best focus point for control: point of collection vs. point of use?
From Jeff Orgel to Everyone: (03:54 PM)When the target of surveillance is resident in an individual (virus) the hunt occurs in the realm of the individual. That realm is well seeded by digital connectivity and footprints at easier picking than analog detective work.
From Marc Davis to Everyone: (03:55 PM)Chilling effect of surveillance is integral to discussion of point of collection awareness and control
From Me to Everyone: (03:59 PM)Transparency and Governance are important factors.How do you build a Digital identity system that allows a person to use their digital identity to dissent against the state?
From Marc Davis to Everyone: (04:00 PM)Need to build systems that support "illegal" activity under an authoritarian government, so individuals can organize and act against the government
From Jeff Orgel to Everyone: (04:01 PM)How do you design something that allows people to push back vs your authoritarian government and still feel safe? - JW
From Me to Everyone: (04:01 PM)Distinguish between identity systems and identification systems?
From Marc Davis to Everyone: (04:01 PM)But how do you build systems that support this positive "illegal" activity, but still combat truly negative "criminal" activity?
From dsearls to Everyone: (04:02 PM)I just showed up, so I don't have anything to say.
From Me to Everyone: (04:03 PM)How to build fail-safes into systems.
From Marc Davis to Everyone: (04:08 PM)Encryption in the hands of individuals has the potential to provide some defense against the intrusion of authoritarian governments into individuals' personal data and identity.
From Marc Davis to Everyone: (04:09 PM)Question of who holds the keys to the encrypted data is a major control point in systems.
From Jeff Orgel to Everyone: (04:10 PM)Governenace is as much a part of the check list as well - Johannes
From dsearls to Everyone: (04:11 PM)JW: SGTF: Social Graph Transfer Protocol.
From Marc Davis to Everyone: (04:11 PM)Problem of "governance" of systems under authoritarian governments is that the "governance" can be a mechanism of authoritarian control and/or untrustworthy.
From dsearls to Everyone: (04:11 PM)I need to run out. Drat.
From Will Abramson to Everyone: (04:11 PM)
https://www.w3.org/TR/activitypub/https://indieweb.org/
From Me to Everyone: (04:15 PM)What if the governance is malignant? Maybe the BLTS framework doesn't work in a kakistocracyOne of the identifiable vectors is arbitrary governance.
From Jeff Orgel to Everyone: (04:17 PM)Cell towers withstand violence as a totem to "common good".
From Brian Behlendorf to Everyone: (04:18 PM)Kakitastrophe is a disaster caused by governance by the

worst people.
From dsearls to Everyone: (04:18 PM)Back.
From Brian Behlendorf to Everyone: (04:18 PM)Here in the US we just call that "Tuesday"
From Jeff Orgel to Everyone: (04:18 PM)Inflexibility and binary sorting as a vector?
From Me to Everyone: (04:19 PM)Another vector might be binary or simplistic categorization of people or groups.
From Jacob Siebach to Everyone: (04:20 PM)What is the question about poles?
From Me to Everyone: (04:24 PM)Othering is a vector of authoritarianism
From Lawrence Liu to Everyone: (04:24 PM)China is not authoritarian
From PhilWolff to Everyone: (04:24 PM)#OaaS (Othering as a Service)
From Me to Everyone: (04:27 PM)Excellent book: The 5,000 year leap
From Marc Davis to Everyone: (04:27 PM)Another vector of authoritarianism is the destruction of shared epistemic frameworks based on rationality or truth and the ability to shape discourse and what counts as a fact as needed by the authoritarian power (cf. Orwell's 1984).
From PhilWolff to Everyone: (04:29 PM)Treated Equally Under the UX,
From dsearls to Everyone: (04:30 PM)A useful book here is George Lakoff's Moral Politics: How Liberals and Conservatives Think: https://www.amazon.com/Moral-Politics-Liberals-Conservatives-Think/dp/0226467716
From Jacob Siebach to Everyone: (04:31 PM)Read "The Law" by Fredric Bastiat.
From Marc Davis to Everyone: (04:31 PM)Ditto on George Lakoff!
From PhilWolff to Everyone: (04:32 PM)Authoritarianism creeps in when marginalized populations are not included in the design of its laws, systems, institutions.
From Me to Everyone: (04:33 PM)Maybe one of the indicia of a move to authoritarianism is if any one of the "Four Freedoms" https://en.wikipedia.org/wiki/Four_Freedoms
From dsearls to Everyone: (04:37 PM)By the way, the founders were not of one mind on religion. They tipped their collective hats to God, but were clear about separation of church and state, of freedom of religion, and, as Jefferson put it, "that our civil rights have no dependence on religious opinions."
From Marc Davis to Everyone: (04:37 PM)In an authoritarian system, the "law" cannot be relied on to be fair or a framework for opposition to state power.
From Jacob Siebach to Everyone: (04:37 PM)Incorrect: they were very FOR the worship of God in government.Franklin was the one that said Congress should always start with prayer.
From Me to Everyone: (04:38 PM)Do Not Rely on Governance if you want to be authorian proof.
From Jacob Siebach to Everyone: (04:38 PM)Jefferson's letter about "church and state" was written to tell someone that the government would NOT stop their right to worship.
From dsearls to Everyone: (04:39 PM)Can we agree, Jacob, that they were not of one mind about a particular religion, but were at least of one mind about the freedom to have or not have one, personally?
From Jacob Siebach to Everyone: (04:40 PM)Oh, absolutely!
From dsearls to Everyone: (04:40 PM)There is no normal intelligence.
From Marc Davis to Everyone: (04:40 PM)In an authoritarian context we cannot assume that other people or organizations are trustworthy.
From dsearls to Everyone: (04:40 PM)Sorry to be so disagreeable. :-)
From Jacob Siebach to Everyone: (04:40 PM)Heh.
From Jacob Siebach to Everyone: (04:41 PM)The nice thing about IIW is that we can have discussions without secret police taking us all away.
From Me to Everyone: (04:41 PM)+1 JacobIf the system depends on educated or trained users, it's a potential vector
From dsearls to Everyone: (04:43 PM)Before this thing is over I want to hear Justin play one or more of all those guitars.

From Jacob Siebach to Everyone: (04:43 PM)And then Jeff can put it on that record behind him.
From Me to Everyone: (04:43 PM)Trust but verify doesn't work. Have to start with a non-trusted relationship assumption.
From Marc Davis to Everyone: (04:44 PM)Thank you John!
From AriDiMatteo to Everyone: (04:44 PM)Thank you!

COVID Daze/Days – The HumanOS & New Relationships with Connected Systems & Services

Tuesday 4A
Convener: Jeff Orgel
Notes-taker(s): Scott Mace & Jeff Orgel

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

1. **Notes from Scott Mace:**

What do you think people will give up in terms of expectations, wants, hopes, in regards to this change? Anyone having to help someone under tension? I believe a lot of things we believe are digital harms right now. i.e. my daughter jumped on a Lime scooter even though she was supposed to be 18. There is a thing called duty of care. A lot of changes in IT? Iain you're doing a cool thing with intent casting.

Iain Henderson: I tend not to worry too much about privacy. It's stopping bad things from happening. vs. empowering the individual. The human OS has a natural immune system that rejects BS. People know there's a catch.

Jeff: Real IT reflects your reality. Played by brain science software systems. If hard in real world, you'll have a harder time on the internet. Real ITdo, aikido is fundamentally defensive. The web is much like that. Learn to move with and through currents. Understand human nature. Security is not convenient. What do you mean by offensive?

Iain: Firemen have a lot of kit. I build stuff. Need to digitize your filing mechanisms.

Jeff: I find passwords on desktop, not protected.

Iain: You have to build capabilities of your own. Empower yourself.

Jeff: Mate up the best of the human computer with systems, with intention.

Scott: Skeptical that humans want to work at this empowerment.

Jeff: There's been an impact. We now have a huge slowdown. The world has come to a stop. As a digital anthropologist, who has watched people hit the brakes hard, there's a huge amount of slowdown. The only time on planet Earth we're all worrying about the same thing.

Scott: Some are in more of a privilege. Slowing down isn't good for lots of people at all. Hope they find resilience, as a nation together. Hopefully there will be a lot of relearning.

Jeff: Terrible to send your kid off to fight that. It comes at quite a price.

Iain: There's research by a friend of mine (see link in chat) on organizations and their information capabilities, less than 1% will be masters, the vast majority will be between rubbish and average. as a community, we need to get our minds around that. We won't get 50% of population to do a data store or intent casting, but 1% of a big number is a big number.
Jeff: The same percentage of people who would learn a martial art. A lot of people like watching martial arts movie. A lot of the tooling I'm referring to is in the head. Funked up by people running ahead of their own sensibilities. POTS line was root, native, through the soil. It's like The Matrix.

Phil Wolff: Who's our topic?

Jeff: The human operating system affected by these technologies; we delegated a lot of judgement to trust in those systems, and that's been beat up. Things changed so much, people are having to do so much over the wire that it's become a social and business respirator. If someone pulls it out of a toilet, you're going to take it. We will have a 15-30% jump in workers not going back to the office. What was your session?

Phil: What could go wrong with all the COVID apps.

Jeff: What could go right or wrong?

Phil: I hate optimism. I find it unnerving. Murphy rules. But there is some utopian opportunity. A time for really big undertakings. Why not North America putting people to work planting a billion trees.

Eric Welton: I like the idea of the CCC. But this represents a unique opportunity for credentialing and identity tech. I was in Adrian's talk about onboarding. I have a window of opportunity with really large companies. What they're looking at, right now we have to do things right now. How do they restructure the lunchroom in the cafeteria. They're looking for evidence at control points. The far ground is Adrian's trustee. Right now, keeping people at home. Right now, get the ceremony of digital credentials in place. Ignore the details of who has the best wallet. I need a pass from I don't care where, even to go to work, if they test me, document that and store it on a phone I carry. So you don't have to worry about an issuer. It's in a semi-public space. It's controlled by the company that operates the factory. Once that's out there, will be much easier to improve toward SSI than jumping to SSI from a dead standstill.

Jeff: A fascinating springboard.

Iain: Which wallet would you start with?

Eric: One company operates 38,000 office buildings around the world. They have turnstiles and badging in place at buildings already. How do we tap that? Not so much a wallet as attaching a credential to that existing infrastructure. Shift from having the security people take the burden to "bring your own data" thing. Dropbox almost would work. Not sure that wallets, especially the ones that touch a blockchain, are kind of off limits. Brings up a statement that says you were tested at Walmart, light verification. The SSI wallets we have right now are a little too heavy.

Iain: Chance Apple will go in that direction.

Eric: I don't have any experience with the existing wallets.

Phil: Is Google Pay considered a wallet?

Iain: It must be.

Eric: Can we put payloads in wallet and flash out a QR code?

Jeff: How will you carry that credential, or there's been discussion about a digital passport. Many people don't have a cell phone. Related to zero knowledge proof. Holographic picture.

Iain: Just the idea of a digital wallet. Apple wallet [lists contents]. If I try to buy a digital wallet, where do you start?

Jeff: Does it belong on a phone?

Iain: Will Abramson knows.

Will Abramson: NHS doctors all have mobile phones. Onboarding process is a lot easier than the general population, who maybe don't all have phones.

Phil: Start with TikTok.

Dr. Saeme: If you think only about a travel document as a clearance, the next-generation e passport will be reading and writing. Can add vaccination and health. It will be controlled. Responsibility of the government. You will have a health visa.

Phil: The passport is just the government's wallet they're lending to you.

Jeff: Can you put minimum viable data on that to a very thin need to know? Why not?

Dr. Saeme: More than 10 years ago, I created a multipurpose smart card.

Jeff: One of the categories in the Digital Harms Dictionary is overcollection of data.

Eric: Tokyo Olympics has the concept of plastic armband. COVID is our dry run. Not unreasonable to say, within this context, here's this Bluetooth tracer, we want to link data safely back to something. That can be moved to the outside, let inside into hyper-surveilled commons, to contact hey you were in the concession line with someone who was incredibly toxic. Go to the hospital now. Move the gating to the edge. Encrypted data on how to contact you. Will see balancing around this. None of these one magic credential stuff. A lot of special purpose solutions.

Dr. Saeme: A fine line between use of technology and surveillance. You have to choose whether to go to China or not.

Eric: A brave new world of reservations.

Jeff: A cycle of social groundhogging.

Phil: Mobile transformed societies. We've been through big changes before.

Jeff: Now we only have connectivity, not connectivity. How will people adjust to this new relationship? It's like we drank too much. Really sick and having to come out of it.

Dr. Saeme: Learn from our errors. Everyone would like to go to the old way when we find a vaccine. Believe me, this will not be the last epidemic with climate change and disparities and poverty. I think solidarity, self-control, control of masses, instead of by one entity. We have a common enemy.

Shireen Mitchell: That hasn't changed. I don't agree with any of this. Not from the communities I come from. We have people marching who think we're the ones who are going to die. It's not the same thing. It looks like it but when I talk about the most marginalized. There are plenty of neighbors who still want us dead.

Jeff: So many different communities.

Shireen: Old stuff, the technology doesn't change it, it amplifies it.

Jeff: We will see new breadth. I'm a political scientist. I've never seen the world all concerned about the same thing. It's not us that's after each other. It's global because of the movement of it all.
********** ********** ********** **********

2. <u>Notes from Jeff Orgel:</u>

Heartening and challenging talk about a fierce topic. There is much hope of cultures and communities being elevated somewhat together as this is the first time since the dinosaurs got smacked that the same thing rocked the whole planet at the same time – and the threat we are protecting each other from is not ourselves – the Alien's Are Coming Bonding Effect.

Considering the new era of dependency on technologies, how might people's values regarding privacy, personal, social and business connectivity be impacted?

New considerations:
I/T as a respirator
Will the slowdown in daily pace give new optics in terms of time to consider what we have entrusted or given away to technologies., and if so what would each of us realize and/or change?

Even if the COVID situation leaves time for concern and maybe even panic, is the change in pace likely to instill greater self awareness of the role systems have been playing for us?

Will to Live: when will the grandparents on borrowed time see their great grandchildren again, or get homemade cookie from them

Is the idea of carrying a digital passport related to vaccination history best managed in a single dedicated tool fully committed to that one validation space preferred over phone based, multi-system wallets or such. How data minimum can they be. How data minimum should they be?

ZOOM SESSION CHAT THREAD:
From Iain Henderson to Everyone: 04:19 PM

https://www.amazon.com/Information-Masters-Secrets-Customer-Race/dp/0471988014
From Eric Welton (Korsimoro) to Everyone: 04:42 PM howdy - yeah - i've had some other challenges today that have kept me in and out of IIW
From Me to Eric Welton (Korsimoro) : (Privately) 04:45 PM Good to have you here Eric!
From Scott Mace to Everyone: 04:50 PM I remember how strange it was to travel in Eastern Europe in the early 1990s and when I checked into hotels, the clerk took my U.S. photo ID and held it from that evening until I left the next morning. Not something I had ever experienced before!
From Scott Mace to Everyone: 04:57 PM Dropping off, bye all
From Me to Everyone: 05:04 PM I have a motto: A mistake is almost always worth the price as long as it doesn't happen again. We are paying quite a price on this and hope we learn a LOT!
From shancasey to Everyone: 05:13 PM Shireen mentioned this in an earlier session - when the people most impacted are centered then the opportunities for expansive recovery can happen.

Introduction to SSI & Decentralized Identity (101 Session)

Tuesday 4B
Convener: Karyl Fowler & Juan Caballero
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presenters' deck:
https://docs.google.com/presentation/d/129rEI4sHrEGufw5AyihEbnysCBbHlSFk/edit#slide=id.p1

Zoom Session Video Link (Provided by Karyl Fowler):
https://youtu.be/mBa-lN5PnKI

Zoom chat:
From Karyl to Everyone: 10:56 PM
https://docs.google.com/presentation/d/129rEI4sHrEGufw5AyihEbnysCBbHlSFk/edit#slide=id.p1
From Vittorio Bertocci to Everyone: 11:00 PM +1 on slack]
From Derick Grey to Everyone: 11:01 PM I'm not on slack, how do I get an invite?
From Vittorio Bertocci to Everyone: 11:01 PM
https://join.slack.com/t/iiw/shared_invite/zt-e08ieit0-7~iZLzYJBIuaD6CG55YH7w
From Ramnath Krishnamurthi to Everyone: 11:01 PM yes i am not on slack either
From Vittorio Bertocci to Everyone: 11:01 PM See above for the invite ^
From nembal to Everyone: 11:01 PM want to record?
From Stew Whitman to Everyone: 11:02 PM Slack channel https://iiw.slack.com/archives/C0132P23EL9
From Tushar Phondge to Everyone: 11:02 PMWill this session be recorded? Great!
From timcappalli to Everyone: 11:03 PM I don't think it's recording. There's usually a little overlay
From Stephen Curran to Everyone: 11:04 PM There is no host, so no way to record.
From Me to Everyone: 11:05 PM https://iiw.slack.com/archives/C0132P23EL9
From Stephen Curran to Everyone: 11:16 PM Hmmm...Hotmail. One of these things is not like the others :-)
From Vittorio Bertocci to Everyone: 11:18 PM Obligatory "OAuth is not an identity protocol" :P

From Me to Everyone: 11:20 PM ^ Take it up with Heather :D
From Vittorio Bertocci to Everyone: 11:20 PM Nevermind ;)
From Kayode Ezike to Everyone: 11:28 PM @KarynHarrison to address your question, I recall the notion of Rubrics broached at RWoT 9: https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/topics-and-advance-readings/rubrics.md
From KathrynHarrison to Everyone: 11:28 PM Ooh thank you!!
From Me to Everyone: 11:30 PM yup! I believe there's a newer version of that rubric in the w3c did core spec appendicesand an even newer version that's not public yet still being peer-reviewed in a google docbut like I said, it really only rates DID:Methods by the degree of decentralization achieves at different layers of the protocol, infrastructure, and IPa strong ideological commitment to decentralization (and open standards procedure generally) make the issue of "certification" (i.e., these X methods are approved by this public institution) a very tricky one...
From Ramnath Krishnamurthi to Everyone: 11:31 PM will you be sharing this presentation?
From Karyl to Everyone: 11:33 PM Presenters' deck:
https://docs.google.com/presentation/d/129rEI4sHrEGufw5AyihEbnysCBbHlSFk/edit#slide=id.p1
From Stephen Curran to Everyone: 11:34 PM For VCs, the blockchain/ledger allows the verifier to prove the presented data without going back to the issuer.
From Grace Rachmany to Everyone: 11:38 PM As far as I know, most of the programs with refugees are not using SSI in a significant way, but are using centralized databases, but please correct me if I'm wrong.
From Stephen Curran to Everyone: 11:38 PM Pretty sure that's right, Grace.
From Darrell to Everyone: 11:39 PM Grace - agreed. However iRespond is using SSI in a refugee camp in Thailand.
From Me to Everyone: 11:45 PM Two specialists to talk to about these things are Balázs Nemethi (Taqanu) and Dakota Gruener (ID2020)
(both are here at IIW this year and keep tabs on all the refugee programs)
From Darrell to Everyone: 11:45 PM @Juan agreed - ID2020 is supporting iRespond.
From Me to Everyone: 11:46 PM Also I believe someone from Kiva is here
From Darrell to Everyone: 11:46 PMSeveral are - Matt Davie is. Nathan George was just hired on by Kiva as well.
From Me to Everyone: 11:49 PM oh wait Balázs is here-- in this zoom! hehe
From Hadeel Elbitar to Everyone: 11:53 PM For someone who is hearing about this for the first time, what's the main take away you want us to have? :)
From Tushar Phondge to Everyone: 11:56 PM I heard that SSI can solve "Password Problems". How can I find more on that? I have read about DID-AUTH is that something used to address Authentication and Password problem?
From Me to Everyone: 11:57 PM ^ Indeed, there is a DIDAuth working group in DIF!
From Grace Rachmany to Everyone: 11:57 PM For now, what I've seen is it's making the problem worse with private keys that can't be recovered if the participant loses their keys
From Me to Everyone: 11:57 PM there are many authentication demos in the demo hour-- check out Oliver Terbu's demo of the new Ethereum Wallet Connect system, and eSatus' Indy wallet
From Derick Grey to Everyone: 11:58 PM If I want to start on a new company that could integrate with SSI platforms, how do I make sure I am following credential standards and collaborate without also losing my IP to larger players?
From Tushar Phondge to Everyone: 11:58 PM Great! Thanks
From Me to Everyone: 11:58 PM Derick - join DIF :D
From Derick Grey to Everyone: 11:58 PMDigital Identify Foundation is what I'm assuming DIF means? :)
From Me to Everyone: 11:58 PM yesh
From Dee Platero to Everyone: 11:59 PM @Juan, Thanks for sharing!
From Derick Grey to Everyone: 12:00 AM Thank you Juan!

From Me to Everyone: 12:03 AMThis goes all the way to the top!
The whole C-Level needs to change!
From Ramnath Krishnamurthi to Everyone: 12:03 AMi second Juan's comment on the C level mentality
From Darrell to Everyone: 12:05 AM@Juan - lemme know how well that works! :-D
Dinner time - later folks - keep being awesome
From Me to Everyone: 12:05 AM Thanks! --> Domilabs.io
From Dee Platero to Everyone: 12:05 AM Bye Darrell! Thanks for your comments
From Me to Everyone: 12:05 AM btw for people curious about creditworthiness self-verification
From Stew Whitman to Everyone: 12:06 AMG2G, Thanks all, see you tomorrow.
From Me to Everyone: 12:07 AM"Superfriends" we used to call it Encrypted Data Vault (EDV)
also crucial to medical record reform (Adrian Gropper's Trustee/HIE-of-one project)

Your Experience with Exercising Your Rights (e.g. downloading your data) Under CCPA or GDPR

Tuesday 4C
Convener: Johannes Ernst
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Attendees:
Wendell Baker
Pete
Keith Kowal
Kaitlin Asrow
Terry Hayes
Jacob Siebach
mahod mah
Johannes Ernst
Doc Searls

Johannes presented his experiences with exercising data download rights from various companies: e.g. Google, Facebook, Walgreens, PG&E etc. Some observations:

- Some are PDF, or HTML, many of them (unreadable, to the consumer) JSON or CSV
- Process to get through the download is complicated
- Major platforms (like Google, Apple) were fast (hours); many others took 45 days, and some asked for 45 day extensions
- Identity verification of downloader is difficult; failed to prove my identity in a few cases
- Google privacy settings respected: no location data in my download
- Everybody made up their own formats
- Some standard formats (eg .mbox for e-mail, .ics for contacts)
- "Rate limits": may only download data x times in y period (e.g. once a quarter)

Two types of data: data retained for service use (available for transparency reasons), data that the consumer cares about retaining (mail, photos…). Both referred to above.
Possibly also portability to other services, but so far not possible (proprietary formats)

Related materials:

- https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

Zoom Chat copy-paste (edited for brevity)

14:33:30 From Jacob Siebach : https://www.theverge.com/2018/12/20/18150531/amazon-alexa-voice-recordings-wrong-user-gdpr-privacy-ai
From mahod mah : they can deliver cars from texas.. and it's tax free
From mahod mah : but then you still reregister in CAFrom mahod mah : and pay some..
From mahod mah : it's weird From mahod mah : some people also keep cars registered in other states, in CA to avoid the sales tax on new car
From dsearls : Getting bad ads is just bad use of profile selections by advertisers of their robots.
From dsearls : OR their robots. From dsearls : I'm late to this. Are we talking here about how to get more personalized advertising, or something else?
From Jacob Siebach : We're discussing GDPR/CCPA.
From Kaitlin Asrow : how the rights to download/access data are valuable or not
From Jacob Siebach : Companies have your data, and what is the extent that they have, and how often are they wrong.
From mahod mah : Doc: we got a demonstration at beginning of what the data looks like when you ask for it under CCPAFrom mahod mah : and are discussing what it means to give people access to their data
From dsearls : OK.
From Terry Hayes : And that you can't really use it anywhere
From mahod mah : yes From mahod mah : I give info that is 2 addresses back, and 20y old
From mahod mah : but disguise it a bit: i figure they know me, but why know me now?
From dsearls : to me the CCPA is about getting back data horses that have left your barn. Alas, not about encouraging development of ways to keep the horses in the barn. Also, you are a mere "consumer," with no recognition that you can produce anything, including better terms by which you do business.
From Jacob Siebach : I did bring that up a moment ago, just before you came, Doc. :)
From Kaitlin Asrow : though CCPA is the largest expansion of the definition of "consumer" across all US data laws
From dsearls : Good. Thanks. Meanwhile the GDPR regards you as a mere "data subject": a pinball in the machines of controllers and processors.
From Kaitlin Asrow : agreed, I think there are looking for new terms that are not already baked with legal precedent
From dsearls : It is good to have Wendell here to explain the ad systems' side of this stuff.
From Kaitlin Asrow : for example, the term "person" is used in US law to refer to a business in some cases
From Jacob Siebach : @doc Agreed.
From mahod mah : ha
From Terry Hayes : Of course!
From dsearls : I think this is what Wendell is talking about:https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
From Johannes Ernst (Indie Computing) : https://indieweb.org/site-deaths
From dsearls : Nothing disappears as totally as bits. If you're "saving" something that way, you're making a choice that likely won't leave a trace, or a fossil, or ash, dust or anything. It's just gone from here to gone.
From dsearls : See https://www.bing.com/search?q=google+graveyard
From dsearls : https://killedbygoogle.com/

From dsearls : I think the GDPR and the CCPA are red herrings for developers, and for users as well. Very distracting, away from work that needs to be done. From dsearls : I actually don't want to change our relationship with anything through the mechanisms of existing laws. it's the wrong approach.
From dsearls : I came over from another session on SSI wallets. Good invention, once we have ones we can use. I don't think anybody working on those is thinking about the GDPR or the CCPA. They just want to make wallets for verifiable credentials.
15:04:20 From dsearls : I consulted Axciom years ago, and advised them to make all the data they collected on people available to them. When they finally did that (after firing the guy who hired me), I was amazed at how totally wrong much of it was. Maybe most of it. Age, residence, phone numbers, licenses held, number of kids, cars, places I shop, loyalty memberships... amazingly wrong. Their system invited me to correct the data, and for yuks I tried correcting a small subset. None of the changes stuck. When I checked again, it was just as wrong.

DIF UNIVERSAL RESOLVER & UNIVERSAL REGISTRAR

Tuesday 4D
Convener: Markus Sabadello
Notes-taker(s): Melanie Nuce

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Links from Markus Sabadello:
https://uniresolver.io/
https://uniregistrar.io/

Notes from Melanie Nuce:

- DIDs are an important link in the SSI community
- Decentralized identifiers are not controlled by a central authority
- DID resolution: very specific technical function that a lot of other things depend on; process of obtaining a DID document for a given DID, which contains metadata about the subject - what is needed in order to interact with or connect to the owner of a DID; to obtain verifiable credentials
    - Public keys
    - Service endpoints
    - Other information as defined in the DID specification from W3C
- DID does not depend on a single technical infrastructure; there are multiple DID methods; an informal list is available on W3C site: https://w3c-ccg.github.io/did-method-registry/
- Each DID method has information about how it is defined and how it can be resolved
- DIF Universal Resolver project (https://github.com/decentralized-identity/universal-resolver) is to build an implementation that supports as many different DID methods as possible; utilizes drivers that are contributed by the communities that are building their own DID methods
    - There are other “universal resolver” projects; DIF is just one
    - https://uniresolver.io is a well-known deployment of the DIF universal resolver

        - It is centralized, which is not preferred for a technology that intends to be decentralized
        - It is experimental and is provided to allow for people to develop and test
        - There are downsides related to trust and security due to centralization
- Originally, there was zero interoperability between different DID methods; implementations were individual silos
- Each driver that implements a DID method is a Docker image held in a Docker container
- Given that Docker containers are heavyweight, the universal resolver is only suited to be run as a hosted service
    - Cannot be run as a DApp or an iOS app
    - Javascript-type resolvers are more suitable for mobile devices
- Various resolver architecture illustrations can be found at https://w3c-ccg.github.io/did-resolution/#resolver-architectures
- DID Document metadata proposal - in discussion
    - https://github.com/w3c/did-core/issues/65#issuecomment-597030882
- Danube Tech (Markus' company) is involved in the Silicon Valley Innovation Program (SVIP), with funding and partnership from the US Department of Homeland Security; working on blockchain security technology. Not directly focused on DIDs, but there is a relationship/dependency
    - Interoperability is one of the key requirements of projects involved in SVIP
- DIF Universal Registrar: a tool for creating, updating and deactivating DIDs. Currently supports only four different DID methods
    - It is organized similarly as the DIF universal resolver in that it intends to support multiple DID methods
    - It's experimental and should generally be used for testing/developing utilizing supported DID methods
    - Given that you don't want a central service managing all the keys for DIDs, what kind of API do we want to setup for the registrar (question from Dimitri Zagidulin)
        - Pair the registrar with Web KMS?
- Create, resolve, update, and deactivate (CRUD) are not protocols, they are different for each DID method; they are abstract functions with inputs and outputs defined by the various DID methods

A deactivated DID will not return a DID document - it may return a special flag or some metadata; but a common response has not yet been fully decided

The State of SSI (gathering & sharing lists, big news, etc)

Tuesday 4E
Convener: Timothy Ruff (DTV)
Notes-taker(s): Sarah Allen

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Acceleration of decision-making because of pandemic
One Example: Evernym, NHS, UK

- doctor shortage in the UK, doctors need to move to diff facility when there's a spike in cases, half-day per doctor to provide credentials when going to a new institution
- pilot with 100 doctors last year now accelerated to roll out 10k then target 1m NHS workers
- Manreet Nijjar (Dr. Manny): https://ssimeetup.org/self-sovereign-identity-healthcare-dr-manreet-nijjar-webinar-21/

Tim has at least 6 others.

Recent work for SalesForce

- Review of VC acceptance by large organisations, academia and standards bodies
- Pointed at this document https://docs.google.com/document/d/1gBKx47cgxsUnTMLxqg6Poswp4-led3x51unUY42fKUU/edit#heading=h.casje1yh789

- https://blogs.harvard.edu/doc/2012/10/22/lets-talk-wallets-at-iiw/
- https://w3c-ccg.github.io/did-method-registry

Kaliya recommended GoodTech.wiki - as a community resource for sharing information about these 'lists' .
Doesn't cover the ledgers or standards
Pam Dingle also working on a list of standards

Learner Wallet - draft spec

DID Methods https://w3c-ccg.github.io/did-method-registry/
Tim shared the link to the spreadsheets for contributions
https://docs.google.com/a/digitaltrust.vc/spreadsheets/d/1egn-ZXVSD_LMPpJVZdD12d_VvLMIPpYrFJdLmOOlqNE/edit?usp=sharing
Reviewed all pages including the consortia, different types of factors to measure & track
Discussion re those who claim to be SSI or Distributed Identity but are not - 'self-sovereign imposters'
Discussion re imposters will be found out if you can't leave - customers are learning
SSI Credential for companies who claim to run or sell SSI systems / solutions, verified by known / respected consultancies (e.g., KPMG). Orgs can then use the Credential in marketing.
Could even go "meta", where companies themselves have SSI wallet containing SSI Certification VC, which can be revoked. (Dogfooding!)

Haiku:
Momentum, Adoption
SSI markets
Listing, cresting a wave

A Verifiable Public Document Graph To Facilitate SSI

Tuesday 4F
Convener: Joel Thorstensson
Notes-taker(s): Joel Thorstensson

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

During this session we gave an overview and discussed Ceramic, which is an implementation of a "verifiable public document graph". We talked about how it can be used to create DIDs as well as any type of documents that are owned by DIDs. During the discussion we also touched on how Ceramic can be used as a general metadata infrastructure that connects different blockchain systems by allowing users to link multiple blockchain addresses to one unified DID.

More information about how Ceramic works can be found here: https://github.com/ceramicnetwork/specs

Dance Party

Tuesday 4G
Convener: Grace Rachmany
Notes-taker(s): Phil Wolff

Tags for the session - technology discussed/ideas considered:
#afrocuban #danceparty

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

We danced under Chatham House Rules.

DIDComm WG Progress Update

Tuesday 4H
Convener: Sam Curren
Notes-taker(s): Sam Curren

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Origins
Early work within Hyperledger Aries
Discussions at IIW 29

WG Setup
Established DIF Working Group
Finished Legal Charter including scope of work
Surveyed for and chose meeting time
Finished review of the principles contained in the Operational Charter
IPR Signatures

Related Work
JWM IETF Draft
ECDH-1PU - Anoncrypt (working on encrypted sender)

Completed Work
Repo Creation (didcomm-messaging)
Source Documents in Repo
Structure for source documents

Current Work
JWM Sender identifiers
0-RTT vs Explicit DID Exchange

Roadmap
Build output running
Key type support
Semantics of Connections / Relationships
Balance between being terse and being complete
Transport Application

Join Us
https://identity.foundation/
(Free Participation in this WG)
Meetings
Monday at Noon US/Pacific
Rolling Agenda:
https://docs.google.com/document/d/1BpTm5SmgfOJcEsXfizO0ZmH1r7imTJDGKudAZtYsm0M/edit#

Co-chairs
Sam Curren (Mattr, formally Sovrin Foundation)
Tobias Looker (Mattr)
Oliver Terbu (Consensys)
(Volunteers Welcome)

Other discussion included Relationship to Aries and various Aries general questions, ledger support, ideas and visions for the impact of DIDComm, etc.

Entity & Object Identifiers: Bringing Assurance & Immutability to a Decentralized Network

Tuesday 4I
Convener: Paul Knowles (The Human Colossus Foundation)
Notes-taker(s): Paul Knowles

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

A digital network must contain assured *data entry* and immutable *data capture* elements in order to maintain integrity. *Data entry* can be referred to as the "male" (or *yang*-) side of a decentralized network model due to the requirement of a signing key in order to establish that inputted data has come from an assured source. Conversely, *data capture* can be referred to as the "female" (or *yin*-) side of the model due to the provision of immutable fields in order to capture and store inputted data. The following component model indicates the *yin-yang* synergy of a balanced network with everything in the northern hemisphere representing the male side of the model and everything south of the equator representing the female side.

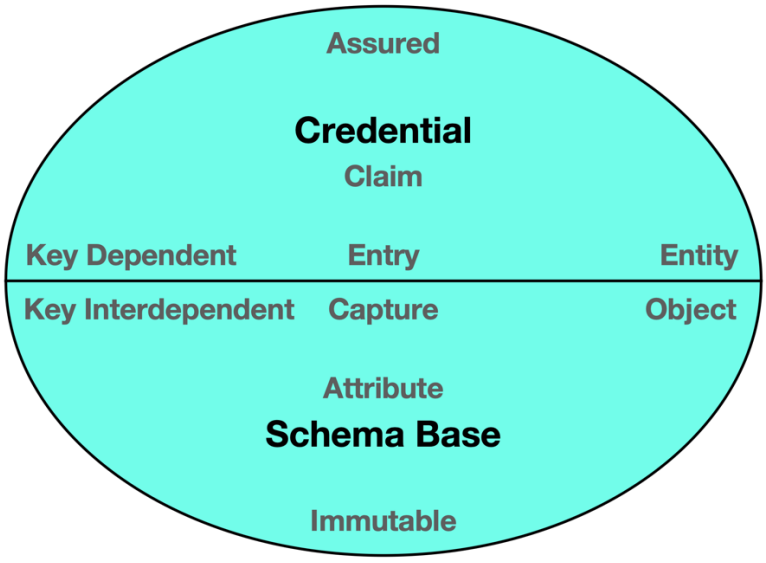


Figure 1. A component diagram showing male and female counterparts in a balanced network model.

In figure 1, elements, components and characteristics in the top half of the model fall into the "Credential" space, the *data entry* domain, while those in the bottom half fall into the "Schema" space, the *data capture* domain.

The characteristics of the identifier types required for *data entry* and *data capture* differ. In the case of *data entry*, assured entry elements are identified by *entity identifiers*, a type of identifier that is governed by an entity who controls the signing key. In the case of *data capture*, on the other hand, immutable capture elements are identified by *object identifiers*, a type of identifier that contains a hash of the content of an object. The following hash grid table describes the different identifier states.

State	Key Dependent	Key Interdependent
Assured	Entity identifiers	Object identifiers that include reference to an entity identifier
Immutable	Entity identifiers that include reference to an object identifier *(This state cannot exist)*	Object identifiers *(No entity identifier referenced)*

Figure 2. A hash grid table describing the different states of entity and object identifiers.

To help dissect the characteristics of the identifier hash grid table described in figure 2, the meanings of the associated characteristics need to be defined.

Key Dependent vs *Key Interdependent*

Key Dependent:
The identifier is governed by an entity and therefore a signing key is required.

Key Interdependent:
The identifier can either be governed by an entity (whereby a signing key is required) or not governed (no keys required).

Assured vs *Immutable*

Assured:
The identifier is governed by an entity and therefore a signing key is required to establish assurance.

Immutable:
The identifier contains a hash of the content of an object which cannot be changed. If an object identifier is governed, the controller of the signing key has control over the content contained within an associated identity document and, as such, it can no longer be deemed immutable.

To scale this back to the *Credential* and *Schema* domains in the network component diagram shown in figure 1, this essentially means that all elements within the male side of the model should be signed by a signature key as proof of governance to establish assurance. All elements within the female side of the model, on the other hand, should contain a hash of content to establish immutability.

As a summary statement, **entity identifiers** bring assurance and **object identifiers** bring immutability to a decentralized network.
Note: The Human Colossus Foundation will be introducing key components of a Decentralized Data Economy (DDE) through a series of blog posts over the course of 2020.

Closing / Open Gifting / Opening

IEEE Special Issue on Resilience & Recovery – The Role of Identity?

Tuesday 5A
Convener: John Callahan
Notes-taker(s): John Callahan

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The moderator is a guest editor for this special issue of IEEE IT Professional magazine (see CFP below) December 2020 issue on Communications Resilience & Recovery. What does identity have to do with resilience & recovery? We will discuss in this informal session. YOU MUST BRING A BEVERAGE OF YOUR CHOICE SINCE THIS IS A HAPPY HOUR EVENT (PDT)! NO ADMISSION WITHOUT A BEVERAGE VISIBLE IN THE ZOOM CHAT! No exceptions! :-)

==========IT PRO CALL FOR PAPERS==========
https://www.computer.org/digital-library/magazines/it/call-for-papers-special-issue-on-communications-recovery-and-resilience

Resiliency and recovery are timely topics in telecommunications. As societies rely on communication networks for critical services at an increasing rate, and technologies evolve based on the assumption of reliable services supported by reliable networks, extremely high reliability is necessary. Networks must therefore provide higher amounts of service at higher quality, all while being resilient and recovering swiftly. Cost constraints, new attack vectors, and network disasters all have to be addressed with resiliency and recovery mechanisms. This special issue of *IT Professional* seeks to provide readers with an overview of current issues and advances in network resiliency and recovery. We seek high-quality contributions from industry, government, business, and academia that present recent developments in communication resiliency, showcase successfully deployed solutions, or discuss challenging issues that deserve further study. Topics of interest include, but are not limited to, the following:

- Network infrastructure
- Interoperability
- Planning and engineering
- Resiliency protocols
- Proactive maintenance
- Prognostic monitoring
- Emerging solutions and technologies
- Applications and use cases
- Optimal practices
- Security management
- Cloud systems recovery and DR
- Ad hoc communications
- Disaster communications
- Business continuity planning

Submission guidelines
All manuscripts must be submitted to ScholarOne Manuscripts by the deadline to be considered for publication. Submissions are subject to peer review on both technical merit and relevance to *IT Pro*'s readership. Articles should be understandable by a broad audience of computer science and engineering professionals, avoiding a focus on theory, mathematics, jargon, and abstract concepts. Only submissions that describe previously unpublished, original, state-of-the-art research and that are not currently under review by a conference or journal will be considered. Extended versions of conference papers must be at least 30 percent different from the original conference works. Feature articles should be no longer than 4,200 words and have no more than 20 references (with tables and figures counting as 300 words each). For author guidelines, including sample articles, see https://www.computer.org/publications/author-resources/peer-review/magazines.

Questions?
Please direct any correspondence before submission to the guest editors at it6-2020@computer.org.

- Tim Weil (SecurityFeeds LLC)
- Jason Rupe (Cable Labs)
- John Callahan (Veridiumid)
- Bhuvan Unhelkar (University of South Florida)

==========END CFP ============
I found this document via a Google search:
https://obamawhitehouse.archives.gov/files/documents/cyber/The%20Information%20Card%20Foundation%20-%20IDENTITY%20AND%20RESILIENCE.pdf

but not much else on "identity and resilience" even though it seems a critical topic. Let's explore the topic while enjoying our favorite Happy Hour beverage!

Other notes:

- CIKR: https://www.dhs.gov/blog/2009/11/19/cikr
- First responder data caps
- First responder identity: https://www.secours.io/
- IEEE Communications Standards special edition on Decentralized Identity https://www.comsoc.org/publications/magazines/ieee-communications-standards-magazine
- Major challenges:
    - offline proving
    - network partition and reconciliation
- Faster satellite communications through Amazon Kuiper Systems, SpaceX Starlink

Building UI's for Decentralized Tech

Tuesday 6A
Convener: Christian Hildebrand
Notes-taker(s): Christian Hildebrand

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Two links shared from Christian Hildebrand for the UI working group:

1. https://docs.google.com/document/d/1-aOlsj91RXcECiWnaJ1YQr3z42CZOtmKiz5pP6z0qrQ/edit

2. https://join.slack.com/t/diduxworkspace/shared_invite/zt-dxi5f6t1-J9aixWCPSsmEH4ZTW_ngRA

Day 2 Wednesday April 29 / Sessions 6 - 14

Decentralized Data Economy (DDE) Unconference – Europe. Initiative to Bootstrap Unconference Format For Component Like TDA, PBS, MSP, SSI, VC etc

Tuesday 7A
Convener: Robert Mitwicki
Notes-taker(s): Robert Mitwicki

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The main idea is to facilitate an event where we can zoom out a bit on all the components which are created in SSI, blockchain, regulatory bodies, semantic data and see how all that together fits.
The Human Colossus Foundation would love to bootstrap first even this year. Gather people from different sectors and focus on a high level picture of the next generation of the internet. How components work together and they should, what are challenges, how to overcome them.
We discussed as well as the follow up of the previous session how important is user interfaces in user centric approach.

We considered options to spin that off under dedicated tracks events like MyData or IIW.
We mentioned great events which covering different aspects of that space like RWoT, MyData, IIW.
We mentioned about propagating IIW in Europe seems that the tracks in different time zones are not filling up same way as others we would love to fix that.

How Can We Make Digital Identity A Sticky Topic?

Tuesday 8A
Convener: Marta Geater Piekarska
Notes-taker(s): Neil, Jeffrey, Sankarshan

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Marta - director for ecosystems for hyperledger; how can DLTs improve non-traditional use cases? Supply chain and social impact are of interest.
Why aren't there more people interested in SSI? The tech world loves it. Everywhere else??

Is SSI ready to offer a solution? Is the technology ready? Is it ready to be delivered on a global scale? The technology works and is continually improving. It is an iterative, constantly developing process. The problem is that the governments and civil society are not yet ready.

Sovrin ZKP - JSON-LD dichotomy may have been bridged yesterday at IIW. US govt has been working on supporting actually interoperable standards for years. But the dichotomy chills adoption - since lack of interoperability is still on the horizon when a dichotomy is not solved.

Identity is not the problem. It is the data behind the identity and flows of data between parties creating and relying upon the data that are where the adoption must take place.

Mentioned the TRUU story - how does a pandemic create the opportunity to circumvent the regulatory structures for approving a medical professional's CV vs immediate health care need to drop proofs of medical CV. ((Truu is built on Evernym and their stack doesn't interoperate with anyone...cause they built ahead of the market))

Austria - overall situation is like everywhere - govt has heard about SSI, pandemic drives contact/tracking/privacy set of questions; using hackathons to come up with possible solutions and to raise awareness of society of SSI solutions; nothing that is real or anywhere near ready to scale

Sri Lanka - Govt interests in SSI seem to be limited.

Europe - EU cross- border ID would be ideal use case for interoperable ID (SSI), but so far that is not happening; the issue may be that there is no trust in how the data would be handled if it to be combined as individuals cross borders.

Known traveler digital ID - project implemented by Accenture and MSFT - govts of Canada / netherlands - hyperledger INDY - create digital ID which tracks your digital footprint from the moment you start searching for your flight to the very end of your journey. Could eliminate the need to travel with a passport? Instead of submitting the credentials in the paper form is substituted with electronic/digital so there is no loss in privacy

Identity and SSI is not about having control over your passport. With SSI there is no need to aggregate the data - the cryptographical proof is sufficient. Airlines could use the DIDs to take specific actions.

The world we have now - requires real information. The need to convince conservative institutions about these new technologies which meet the current regulatory requirements is the hurdle that is required to be crossed.

A number of organizations are reluctant to hold or aggregate the data. Organizations which are trying to move away from that responsibility may be interested in SSI. Any audit of necessary information to the regulatory body can be done easily with the data flows. SSI enables not having data but access to the data.

What about businesses/individuals adopting SSI for use cases which are helpful for them? The entry point through the government is the easiest way to expedite mass adoption.

[from chat log]

Who/what institution have the power to drive adoption and what are their needs/pain points - does SSI solve them? This is a hard challenge - it literally is a 3 sided maret that all needs new adoption

[from chat log]
DIDs with limited lifetime advertising a limited subset of information might be a way to handle the use case of travel. Special one-off use cases can be served through this method. Even contact tracing (cf. work undertaken by Google and Apple)

Skills is one use case where the adoption of identity/SSI could have a scope. There is a smaller need for a large ecosystem to be created for it to take off. People should be able to issue skills credentials without accreditation and find them acceptable.

Ottawa - on boarding volunteers requires manual intervention that might be helped with verifying the credentials in a digital manner.

[Killer Use Case Discussions]

Use cases which address the topic of revenue or of reducing costs might be more important towards improving quick adoption of SSI. Probably bottom-line impact is the most obvious impact (operational efficiency). When discussing with prospects - do not discount the complete economic disaster that is from COVID-19 etc. Organizations would want to look at their costs to plan and outlast the shutdown. Potential significant cost savings → new opportunities might be the driving change

How can you get value without vendor onboarding or KYC - SSI can be used to create the credentials which can be shared/exchanged. This unlocks the value and potential in the adoption of SSI. Governance framework. Who is going to take the first step (first mover?) How can this be used in a low tech solution (usage pattern of smartphones across Africa).

Virtual resume (a couple of demos have happened) - “are you who you say having the qualifications”.

Maybe the big problem is that we are trying to tackle human identity - taking a complicated problem and applying a new technology. Is it possible that digital identity for pets/animals could be the first step to adoption? Doing iterations to test and then move to human identity.

Can one of the companies at IIW do DID/VC based login? BC Gov did that a year ago.

Digital Life Hub for everybody on the planet (secure storage, management, contacts, calendars, wallets, skills, personal credentials etc)

Digital wallet containing digital immunity to help improve the travel industry operations

Highlights from the Zoom Chat thread:

I think the question is - WHO (what institutions) have the power to drive adoption an what are their needs / pain points - does SSI solve them.This is a hard challenge it is literally a three sided market that all needs new adoption.

"onboarding" and "smoothness" can be faster and easier implemented using centralized solutions. You can see that through different ditial identities created by govsintreste of people in identity management not but privacy yes and the anwarnace is increasing
connect facebook deos nice job with onboarding :)

another note - think we are very focused on building with cutting edge technology but applying old world mentalities. think we should maybe look at alternatives and completely new approaches ;)

Group Identity – Open Discussion

Tuesday 8D
Convener: Will Abramson
Notes-taker(s): Will Abramson

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This session posed two questions:
How do we model the identity of groups and our relationships to these groups and within these groups?
How the tools we are all building help us do this?

Link to notes provided by Will Abramson:
https://docs.google.com/document/d/1ENWEMiEB4xa-RbEwwlavw-iF72wkxVKqgKWT_uVMsQs/edit?usp=sharing

Patient Choice Using Distributed Identifiers

Tuesday 8E
Convener: Tom Jones
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presentation is on this page http://tomjones.us/Home/Solutions

The methods for providing users with strong assurance eg X.509 have not had acceptable UX
NSTIC → IDEF

The discussion is about enabling great Level 2 experience (when user makes an assertion they need validation; identity assurance needs proof of identity proofing; authentication assurance needs proof of protection of user secrets; cover nearly 1:1 claims about the user; 3rd party claims can extend to comparisons of different co-pay choices; any of these can be bound to other user contexts at other HIPAA entities)

At registration the new patient needs (driver's license; health insurance card; payment card; health history)
The information received can be validated by some existing technique and methods
Patient Registration with Distributed Attributes - standard
Precondition :

In this use case the patient has a smartphone; has the capability to load an app (which controls the identity and release of information). It is optionally possible to consider that the phone holds the healthcare information for the patient

PCP gives the user the location or, URL so that the app can be loaded on the phone - could be a QR code

User loads app on their phone → establishes an identifier on their own (self issued identifier) → user binds the identifier to medical records at the PCP/Hospital → phone binds the identifier to claims of authentication assurance

The app is a "certified app" and the phone is capable of securing the user's secrets.

User can use these claims in a new context with any other HIPAA covered entity. User agent could download user data in FHIR format. User agent could verify the trustworthiness of any provider. User could upload user FHIR data to any certified web site. The goal is that the FHIR data never leaves the context of HIPAA

If the device is "shared" - given to another user with the screen unlocked; the new user (not the one who created the profile) is likely to have access to the app and detail. Unless the app requires secondary authentication for data/functionality within the application container
Guardianship role capability can be added to the flow which is driven by the app.
Minimal user data needed

Closing / Opening & Agenda Creation

Domains of Identity: Book Coming Out - Overview & Help Me Figure Out How to Sell More/Share it Widely

Session: 9A
Convener: Kaliya Young
Notes-taker(s): Kaliya Young

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

SESSION ENDED Early :) contact me if you want to connect about this kaliya@identitywoman.net

Sharing about **Domains of Identity Book**

IDPro Group

What is success and how many books I have sold
A million books?
Who is going to buy the books.
Best channels
Best Target audience.

IAPP

Webinars - for folks to learn about the work.
Good way to promote.
Virtual Book Tour -

Good for decision makers.

The think that keeps jumping out of me.
    Devolves into access and authorization.
    used to the design pattern of Centralized IAM systems.
To do the work to get the attention to sell the books.
Channel sales. If I have to sell a million widgets. If I have 10 channels and they each do 100,000.
Sometimes that can off load part of the daunting task.
What would have to be true to be comfortable with number X.

Awareness is not linked to "sales" low awareness
Effective Targeting.

Those who are deep into the practice.
CISO
ISO
RightsCon

Kayode had read it a year ago.
The Domains of Identity - define the channels.
Business, Gov, How to market to the different groups.

Kim Hamilton's work with the EDU task force.
Segment audience and develop selling point.
Finding the channel to reach them.

Consultant - who help you sell a book.
What is the benefit of the book?
Will any part of the proceeds go to a charity.
Aligning myself with a cause.

KERI (C) KACE Agreement Algorithm Recovery

Session 9B
Convener: Sam Smith
Notes-taker(s): Sam Smith

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This was the third in the three-part KERI session deep dive:
Session 2F: KERI (A); Session 3A: KERI (B), Session 9B: KERI (C)

Links to notes (slide deck) and white paper, provided by Sam Smith:

Notes/Slide Deck:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI2_Overview_AB_IIW_2020.pdf

White Paper:
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI_WP_2.x.web.pdf

Principles of User Sovereignty

Session: 9C
Convener: David Husseby
Notes-taker(s): Grace McCants

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

David Husseby
Where we are now:

- FB/ Google: Use the system and adhere to the rules, this is one extreme of the system.
- Surveillance capitalism, set up such that people are rewarded enough to not revolt.
- At urging of Sam Smith, DH started to wonder: what is the other end of the spectrum.

Link to session slide deck presentation, provided by Dave Huseby:
https://docs.google.com/presentation/d/1V1t6m217EFN8xOw5Zb6Mwr3LBp96O5JFID543io_XME/edit?usp=sharing

Chat Thread:
From Adrian Doerk to Everyone: 05:52 PM
What is surveillance capitalism? A video by me: https://www.youtube.com/watch?v=t_aNHKait1o

History, David

- User sovereignty as a term has been use since 2011, first person public speaking was Mitchell Baker, head of Mozilla.
- Similar ideas, Declaration of Independence of Cyberspace used similar terminology. Our jurisdiction is different.
- In 1996, Technologists like ourselves were asserting user sovereignty and were worried about government incursion.
- In 2011, MB statement is about violation of user privacy. It went from government to corporation as the concern.
- In 2020 it's around the hand-in-glove cooperation between corporation and government, so you can see FB saying that they will disallow anti-lockdown organization posts. FUrthering the power of corporation and governments

From Heather Vescent to Everyone: 05:57 PM Question: Which government are you referring to? US gov or foreign Govs (who do information operations)?

- DH: It could be anybody who's job is to direct policy.
- Timothy Ruff: It could be any entity that could jail you or coerce you with guns
- It could be your own government

J Searles: The Utopia of Rules, Dave Gravers

Heather: Had my own thoughts about how the role of government has shifted dramatically in last 3 months based on my research on espionage. I had no idea of this prior to my research. One of hte most radical

ideas I came up with was, I learned I support government surveillance more than corporate surveillance. The governments have the guns but the corporate surveillance doesn't have responsibility.

Chris: I would agree. There is no sense of principles that dictates
Doc Searles: Depends on what government you are talking about. Reason we are less disturb about private kind is because they just want to spy on us to sell us shit, but there is a lot they could do that we aren't aware of

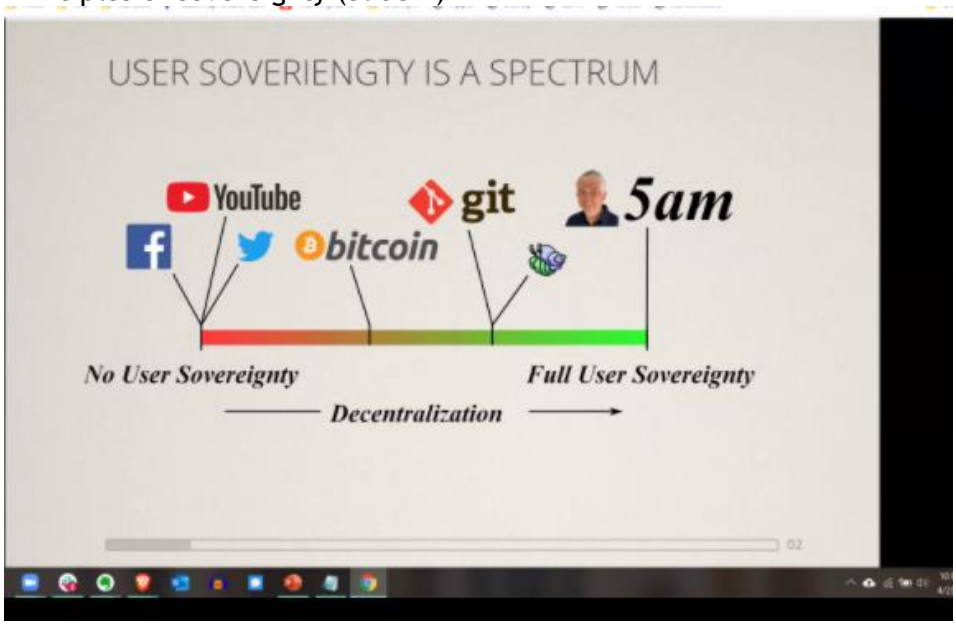
Heather: Info gathered by private sectors has been used by foreign governments. You could argue that FB and Twitter are weapons used against various countries.
Chris Buchanan: In US under supreme court rulings, Data collected by private companies that the government can buy is not considered surveillance and not subject to the same rules as government laws. So you're giving it to the government without any oversight.

Heather: That was the problem with PRISM, because governments found a way to get the data without abiding by the laws

Jeff: Governments are ideally formulated by their communities. Business can aggregate that information in a space where they operate on their own and use force. There is a lot going on that it government agnostic. Deep tech is scary

Aaaaaand… going back on track as the slide set begins to operate.

Principles of sovereignty (Slide 1)



5AM is the project David is working on, offering a new term of decentralization. People use distributed and decentralized interchangeably although people will say that decentralization is about power and rights. I'm suggesting that decentralization is the direction in which user sovereignty increases.
From Phil Windley to Everyone: 06:08 PM
Sam is the mascot for full user sovereignty
https://www.windley.com/archives/2015/01/re-imagining_decentralized_and_distributed.shtml

The Six Principles

This is for the most extreme end of the system.

- Absolute privacy by default. System knows absolutely nothing about the user. For example, a blind relayer might not need to know anything.
- Absolute anonymity and zero correlation by default (TOR level IP masking). Privacy to maintain leverage over a system that seeks to monetize their interactions. Primary tool against using data against someone is anonymity. Full control over what they share with other users.
- What, not who. Principle about designing authorization of system to be around what you are and what you can prove about yourself. Skipping identification and going straight to authorization. Identification today we use as the means to authorization and that is not necessarily a requirement. Would it be possible to build a payment system where content creators could collect fees from content viewers in a system which knows nothing either about the identity of the creator of the subscribers. If you look at the AML and KYC systems, these are all about law enforcement.. The biggest hurdle is biggest payments systems ban this. In theory, it is technologically possible. Someone could show they are a legitimate company with ability to collect money, and subscribers could provide KYC authorization without identity information.

Next 3 are the ones we usually discuss here.

- All data and operation are governed by open and standard protocols and formats. Today IMAP for email follows this. This works because there is a standard data protocol and format. This gives a tool to verify full user sovereign systems. This is how certification is done at the Linux foundation.
- Strong encryption by default to enforce data control. This is about the user knowing who is using what, where data is and the ability to delete.
- Informed consent. Any time we violate any of the other principles for legal or regulatory reasons, the system must get informed consent of the users, with the understanding that anyone can withdraw consent. Timothy says any decision making, and David says we don't know why AI makes decisions. Any balanced terms of use between user and system.

CHAT:

From dsearls to Everyone: 06:15 PMopen standard protocols and formats assure not only portability but what economists call *substitutability*. this is also what Dave is talking about here.
From Timothy Ruff to Everyone: 06:16 PM Doc, chime in please
From dsearls to Everyone: 06:16 PM Phil wrote about this in 2014, here: https://www.windley.com/archives/2014/03/substitutability_is_an_indispensable_property_for_the_internet_of_things.shtml
From Timothy Ruff to Everyone: 06:16 PM Doc, we learned a lot of this from you, we'd be honored to have you chime in I realize this is standing on the shoulders of giants.

Timothy Ruff: Doc sees that there's a lot of top-down versus bottom up. What's the benefit for individuals. If you do not simultaneously address what are the rights of the organizations, and why would they change all their systems, then it's not going to go anywhere. We need to have balance here. Not say this is a user revolt. We want a balance of power. We want more than we have so each one of these principles about what is the benefit for the organizations.

From KathrynHarrison to Everyone: 06:17 PM What % of the general population would actively advocate/ ask for these principles? I agree with them but think it's a small audience today.
From dsearls to Everyone: 06:18 PM I'm more wide than tall. Like a turtle. :-)
From David Huseby to Everyone: 06:18 PM+1 Doc
From KathrynHarrison to Everyone: 06:18 PMAlso question is incentives
From David Huseby to Everyone: 06:18 PMrightI have a little on that too
From KathrynHarrison to Everyone: 06:18 PMFree data and information has been crack for the General population for the last 20 years
From David Huseby to Everyone: 06:18 PMPII is toxic waste
From JeffO-StL to Everyone: 06:19 PMRe-evolution, not Revolt

From JeffO-StL to Everyone: 06:19 PM Revolution
From Kaitlin Asrow to Everyone: 06:19 PM data pollution
From Me to Everyone: 06:19 PM What's wrong with a user revolt? Organizations are not living beings. They are created by us.
From Gabe Cohen to Everyone: 06:19 PM Substitutability = easier to bring new users to your platform
From dsearls to Everyone: 06:19 PM Relevant: https://www.gapingvoidart.com/gallery/dinosaur/

From johnnyfromcanada to Everyone: 06:19 PM We are anchoring the negotiation with society!
From JeffO-StL to Everyone: 06:20 PM fat fingered last) Re-Evolution (of systems and values) is evolved Revolution maybe...
From Marc Davis to Everyone: 06:21 PM "Informed consent" is highly problematic in practice. Most TOS and Privacy Policies are "contracts of adhesion" (asymmetric power enforced without any alternative choice). What I see missing here is a clear articulation of what rights each party actually has or should have. If you want true user sovereignty, the rights and legal and regulatory frameworks need to be clear in empowering the self-sovereign person. I can point you to my talks on Digital Feudalism and Digital Enlightenment from 2010 on.

Doc: We assume that we are the ones consenting to their terms, but it should be able to go both ways. We wouldn't be talking about this at all if a simple request of do not track in a browser had been obeyed 10 years ago, but it wasn't'.

David: In that world we could negotiate our own terms. In my next talk about fundamental problems of distributed systems, if you don't adhere to these 6 principles, you subject the system to corporate capture. It opens the door for a company to provide a centralized solution.

From Marc Davis to Everyone: 06:21 PM "Informed consent" is highly problematic in practice. Most TOS and Privacy Policies are "contracts of adhesion" (asymmetric power enforced without any alternative choice). What I see missing here is a clear articulation of what rights each party actually has or should have. If you want true user sovereignty, the rights and legal and regulatory frameworks need to be clear in empowering the self-sovereign person. I can point you to my talks on Digital Feudalism and Digital Enlightenment from 2010 on.
From David Huseby to Everyone: 06:21 PMright
From Timothy Ruff to Everyone: 06:21 PM
Grace: user revolt has the same problem as what we saw on Thor: Ragnarok: if you plan a revolution, you'd better pass out enough fliers! Seriously, it's hard to get enough users to care enough to execute a successful revolt. In the end it's best to do it together, with the best interests of orgs considered, too.

From Dennis Landi to Everyone: 06:22 PMGot it. thanks
From Chris Buchanan to Everyone: 06:22 PMDoc, one of the interesting things about having bilateral privacy policy is the potential to match users with services.
From Benedikt Olek to Everyone: 06:22 PMI think user sovereignty comes also with a lot of responsibilities. In SSI, you might need to properly handle your secrets (priv. Key). If somebody gives you a perfect anonymity tool (like SuperTor), you still can accidentally doxx yourself and so on
From Me to Everyone: 06:23 PMThe new CAL Open Source license is relevant to this talk. I can elaborate. | https://medium.com/holochain/understanding-the-cryptographic-autonomy-license-172ac920966d

David: Preview of problems in distributed systems (missed the main points), but because the problems of distributed systems caused GitHub to be bought by microsoft and they have 30% of the Opensource project and host the top 100 opensourece projects. And evne the projects that DLF hosts are still on Github. The communities should use the best tool but there are people who are nervous about Microsoft owning Github. We are seeing streamlining of Github with AZP and now were' seeing Windowssubsystems by Linux. They're looking out for their business. By not providing fully decentralized systems, Git opened itself up to capture. I'll go into that deeper in the next session.

From dsearls to Everyone: 06:24 PMAgree, Chris. The question is how that gets framed up. If it's always up to the service, you have as many policies as there are services.

From KathrynHarrison to Everyone: 06:27 PM Means quality of decentralized service has to be 10x traditional systems if it is going to get adoption. Most people are pragmatic.
From dsearls to Everyone: 06:27 PM We're up to 77 people here. Might be a record for a breakout. 78
From johnnyfromcanada to Everyone: 06:27 PM In Timothy's state-of-the-art session yesterday, we raised the notion of "SSI Certification" and/or "SSI Declaration" that companies should align and commit to. Seems to me that these principles (or similar) could be a foundation for such. Also such a certification would need to be tiered / levels (CMM), just as these 6 principles are likely unattainable fully (aside from some exceptions).
From Timothy Ruff to Everyone: 06:28 PM True. SSI took the time to verify doctors in the UK from half a day to a few seconds. That's easily 10X.

From Principle to Practice. What would it look like

- User would have full control
- User is fully anonymous and private by default

Joyce told me this story, I go to this coffee shop every day, and I have for years, and they offer 20% off for first time customers. what about me? I've been keeping you in business for years!
The reality is like this, a lot of systems work like that. But we could show up as first time customers every time.

Joyce: to add to that, what would happen if as soon as we walk into a mall, every shop knew we were looking for a pair of black shorts. What negotiating power would we have? We could not possibly get the best deal if they all knew that. We want our ability to hide that information about ourselves to be built into the system.
DAvid: By anonymous it means I am not radiating any information that you can gather that would allow you to correlate me across time and space.

Doc: If we are outside our regular social circles, we are nameless. A nonymous, not nameful. We should have that as a default online and then add in nonomous, or credential as required or as we choose.

From Me to Everyone: 06:30 PM
You're obviously going to the wrong café. My health food shop gave me a discount after I'd been coming for 3 months.
From Wendell Baker to Everyone: 06:30 PMWhat about that bar where everyone knows your name?
From Cam Geer to Everyone: 06:30 PMDave that is the first state - we are looking at — window shopping
From Wendell Baker to Everyone: 06:30 PMjust trollin ya :-)
From David Huseby to Everyone: 06:30 PMyup
From Kaitlin Asrow to Everyone: 06:31 PM
whoever holds more information is able to capture more surplus from the transaction
From dsearls to Everyone: 06:31 PMDave's talking about what our natural state of anonymity is in the physical world, as a default outside the circles where we are known.
From Jeffrey Aresty to Everyone: 06:31 PM IBO feels the need for a Declaration of Rights which establishes a framework for adoption - we would appreciate your comments
From Timothy Ruff to Everyone: 06:31 PM The 10X requirement Kathryn's referring to comes from "The Change Factor," which posits that users require a 10X improvement before they'll overcome the switching costs of making a change. There's a whole book and other stuff about it.
From Jon Lewis to Everyone: 06:31 PM I think the analogy of the mall is flawed. If all of the merchants knew that we were looking for black shorts... we would ultimately get a getter deal. The merchants would compete for the business and our ability to leverage a competitive market would increase.
From KathrynHarrison to Everyone: 06:32 PM I think we need to look more to models for how we operate in analog world...
From Jon Lewis to Everyone: 06:32 PM We want them to know what we are looking for.
From Cam Geer to Everyone: 06:32 PM The person / user chooses whether to have a relationship with the business / service. Otherwise default state is anonamous

From Cam Geer to Everyone: 06:32 PM The person / user chooses whether to have a relationship with the business / service. Otherwise default state is anonamous
+1 Kathryn — this is the primary discovery action of the Me2B Alliance
From dsearls to Everyone: 06:33 PM Right, Cam.
From Me to Everyone: 06:33 PM @dee, I am happy to discuss the CAL license here or set a session about that.

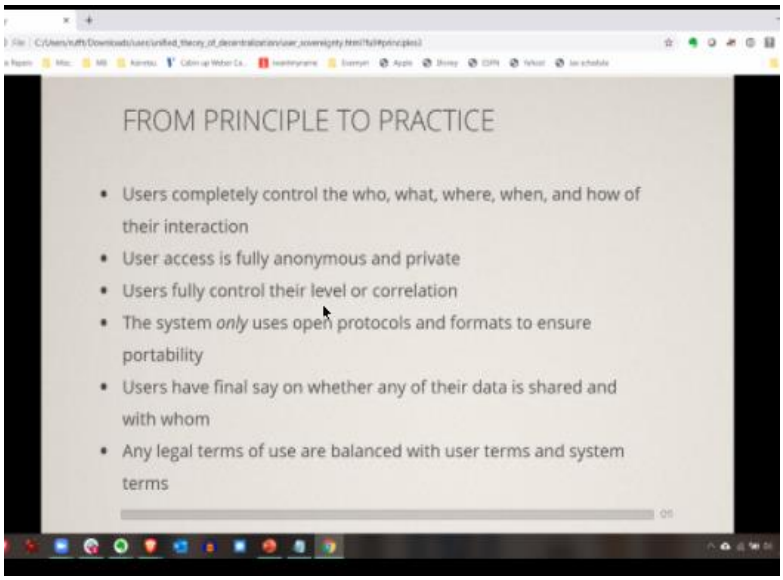
Chris: It takes a willful decision on the side of the platform to ignore that data.
From Jsearls to Everyone: 06:34 PM I've been saying this is "natural anonymity" I'm known as a person, but nothing more until I want to reveal more.
From George Fletcher to Everyone: 06:34 PM not named doesn't mean not correlated. As humans we are global correlateable identifiers unless we go to extreme lengths
From dsearls to Everyone: 06:34 PM I think what Dave's talking about is each person as her own platform. Not about what service platforms (apple, google, et. al) are doing.
From johnnyfromcanada to Everyone: 06:34 PM This extreme is likely asymptotic in practice.
Phil: You are nameless but not anonymous. I have a sophisticated system -- I don't lose track of you as you walk past me on the street
Jeffrey archer posted a document.
From Cam Geer to Everyone: 06:34 PM yes…that is what the Me2B Alliance certification is driving toward. It is just the assertion
From johnnyfromcanada to Everyone: 06:35 PM Forgetfulness is a key part of GDPR (and others).

From JeffO-StL to Everyone: 06:35 PM @PhilW: The Human as a sensor package is a great topic of discussion.! I did a session at IIW..
From Juan Caballero to Everyone: 06:36 PM Is this the things OSP made for HoloChain ? https://medium.com/h-o-l-o/why-we-need-a-new-open-source-license-c8faf8a8dadd
From Cam Geer to Everyone: 06:36 PM +1 Grace
From Kaliya Identity Woman to Everyone: 06:37 PM The ioFoundation is working on something like this a universal declaration of digital rights starting with - https://www.theiofoundation.org/
From Cam Geer to Everyone: 06:37 PM And open source is even moving into base silicon https://riscv.org/
From dsearls to Everyone: 06:37 PM Forgetfulness dates from Brandeis & Warren's treatise on privacy as "the right to be let alone." (let=left)

Marc Davis: A lot of work was done on digital feudalism versus digital enlightenment, I can point to that. Relative to that, the talk seems to assume a kind of techno-determinism, that alternative technology will push the stack in the right direction. When you talk about the balance of user terms and legal terms. To have user sovereignty requires not only technology but also law, and regulation, it has to include rights, legal, and regulatory frameworks. not just through technology. The point about informed consent goes right to that. Informed consent tends not to work in practice.

DAvid: These are just principles.

Doc: We already have laws that are screwing things up. GDPR assumes we are nothing more than data subject. In the absence of tech, state of California decided we are just consumers and our rights are nothing more than our ability to ask for our data back. If we firm up everything in terms of the laws, we get locked up in the tech. We could start tech first and then have the laws follow the norms.



David: I'm a crypt anarchist but I'm also willing to put on a suit and talk to people in power. But I am also willing to do this first. We should always be willing to have the conversation, but I think this is a foundation for where we should start principles wise and as we design new systems.

My last slide of my last talk is about why Web 1 and Web 2 are centralized and why most of what's coming out of Web 3 will also be centralized.
I don't think we should ask permission.

Jefferey: Laws are not going to come from sovereign states. The International legal system is broken. Anybody in civil society can make a bunch of statements about how it should be. We need to state our position. Nothing you are saying is illegal in any country.

Chris Buchanan: This is a community project and I would like to participate in something like that and my corporation would like to be part of that. My company is involved in that. It's hard to draw the connections with current reality when talking about biometrics surveillance systems. We want to lay it out and say "This is the perfect". Then we can ask what policies are in the way of the perfect, and what are the incentives for people to move and what is the overall global strategy in how to prioritize our own efforts in the SSI community to move this forward to move this forward in away tha tisn't behemoth resistant in every area. My experience with government is that they are for some of this. Having explicit consent is huge and it would solve some of the problems with technical surveillance. I think there's interest within places that you would normally think of adversarial. Getting together with the group of folks who can speak to what the perfect is, and bringing in some naysayers and people who would say, well that won't work because. Let's start refining that. That's how you reach strategy. This deserves a serious amount of brainpower. It is the most important thing. We didn't have stoplights before we had cars.

From David Huseby to Everyone: 06:44 PM +1
From Timothy Ruff to Everyone: 06:44 PM We're out of time... :-/
From Line Kofoed to Everyone: 06:44 PM +1
From Me to Everyone: 06:44 PM How do we provide you feedback
From Juan Caballero to Everyone: 06:45 PM yeah where's this go Chris! Doing God's work
From David Huseby to Everyone: 06:45 PM let's meet in a garden room later this afternoon to talk about where this goes
From JeffO-StL to Everyone: 06:45 PM I would like to be available for such an effort (WG) as well.
From dsearls to Everyone: 06:45 PM There are groups working on some of this: http://me2b.us, http://customercommons.org, http://projectvrm.org
From David Huseby to Everyone: 06:45 PM or that ^^^
From Juan Caballero to Everyone: 06:45 PM ^ yes
From Marc Davis to Everyone: 06:45 PM The question is not only what laws are on the books, but what rights and agreements we want various parties to have in a world based on "self sovereignty"—i.e., look to contract law—the agreements individuals and organizations make with each other and that articulate their respective "rights and duties"—this is different from transnational, federal, or state legislation, but much more about the agreements parties make with each other.
From johnnyfromcanada to Everyone: 06:46 PM These principles can also be another simple way to help people to understand SSI in general (after telling them about wallets. :-))
From Timothy Ruff to Everyone: 06:46 PM Haha Johnny!
From Kaitlin Asrow to Everyone: 06:46 PM I am concerned that the volume of contracts necessary to deal with every digital interaction is not tenable
From johnnyfromcanada to Everyone: 06:47 PM In fact, everyone's wallet should contain these on an e-laminated card.
From Kaitlin Asrow to Everyone: 06:47 PM individuals cannot negotiate contracts at scale
From Juan Caballero to Everyone: 06:47 PM ^ the three groups Dsearls mentioned all work on that as a substantial focus
From Heather Vescent to Everyone: 06:47 PM My concern is that there are not people in the room with power to make this a reality.
From Juan Caballero to Everyone: 06:48 PM @Johnnyfromcanada, here's my attempt at that: http://www.caballerojuan.com/blog/ssi/the-next-big-thing-is-you/

From Kaliya Identity Woman to Everyone: 06:48 PM Before you talk - breath, figure out what you want to say, say it and then stop…and wait
From dsearls to Everyone: 06:48 PM Hope folks saw Jeff Aresty's shared document earlier.
From Jsearls to Everyone: 06:48 PM @heather, this speaker is saying that his corp is speaking to govt
From Kaliya Identity Woman to Everyone: 06:48 PM don't feel like you need to fill the space - we can't see each other and don't have the natural body language.
From Timothy Ruff to Everyone: 06:48 PM @Heather... not directly, but indirectly we can do a great deal. I have some ideas, and Chris is talking about what he/Mitre can do, and there's gonna be way more...
From Me to Everyone: 06:48 PM I would be interested in that working group too!
From Marc Davis to Everyone: 06:49 PM A key intervention is a small set of standardized contracts that reflect "self-sovereignty"—expressed in simple, brief, language that a non-lawyer can understand and actually consent to—to standardize and make more efficient and transparent the rights and duties each party has.
From johnnyfromcanada to Everyone: 06:49 PM Many domains head this direction of core principles. E.g., software engineering developed a "kernel". Agile now has an "essence" (heart).
From Cam Geer to Everyone: 06:49 PM@ Kaitlin — that's why the agreement direction needs to be flipped. Put users in control with a "bill of rights" they control and the business / govt / services agree to abide by them or the person / user doesn't use their offering
From Heather Vescent to Everyone: 06:49 PM Also I'm not sure how much of this future I actually want. Goal of my project is to build a fully sovereign github and Jira replacement.
From Kaitlin Asrow to Everyone: 06:50 PM @Cam, agree 100%
From Timothy Ruff to Everyone: 06:50 PM To each her own! For me, I want greater user sovereignty, freedom to take my data and relationships from platform to platform as I choose.
From Me to Everyone: 06:50 PM A bunch of people are working on developing a Git replacement on Holochain, you should get in touch with them.
From dsearls to Everyone: 06:50 PM I think we need one invention that mothers a necessity for everything Dave's talking about here. These principles should guide the development, for example, of digital wallets of credentials. Once corporate and government entities share and respond to the use fo these credentials, we may have the first traction required to internet investors and support by foundations and well-off individuals. In the absence of that tech, we're where we've been.

SCIM Working Group Re-ignition

Tuesday 9D
Convener: Darran Rolls
Notes-taker(s): Matt Domsch

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Attendees:
Darran Rolls, Matt Domsch, Pamela Dingle, Jonathan Wright, Tushar Phondge, Satish Joshi, Inderjeet Kaur Khanuja, Tim Cappalli, Jacob Siebach, Jn taylor, Jason Downs, Josh Verbarg (State Farm), Dmitri Zagidulin, Joseba Lekube, Raider Horbe, Maryam Shahid, Neil Thompson, Erich Fortuni, Juan Caballero, Phil Archer, Lawrence Liu

What is SCIM?
https://tools.ietf.org/html/rfc764
http://www.simplecloud.info

Tim: Glad to see so many implementations
Josh: pushing SCIM with all of their application vendors
Neil: To state farm: data access, or data transfer? Josh: simple store of users, separate stores of attributes and policies.
Darran: provenance of attributes? We're making late-bound use of these attributes without recording from whence they came.
Dmitri: use Verifiable Credentials for attributes
Neil: groups, and groups of groups, were necessary for the BI industry to qualify for authentication and authorization
Satish: RBAC isn't sufficient. You get group explosion. Need fine-grained attributes, but even ABAC doesn't satisfy all the large enterprise needs.
Dmitri: Secure Data Storage Group (W3C and DIF) is a good place for conversation re SCIM + SSI. Focus on encrypted data storage, focusing on user profiles and user accounts. Needs profile export and transfer between applications. Session 13 today.
The same tech allows both pseudonymous and public/corporate identities. Regulated, trusted authorities and registries is suited to adding a trusted stamp of approval. Internal HR can also provide trusted stamps of approval.
KYC runs across enterprises. SSI separates verification of identity from identity, and re-couples them only when needed.
Neil: What/who is the root of trust? Like a non-governmental but trusted org that may be rooted in government.

BC - tackled the easier problem (which is a great starting point!).
Obstacles to SSI:

- Technical: Key management & Wallets. Interesting tech here, but still raw.
- Social: who will the certification authorities be? This is solved in enterprises by HR, but not across enterprises.

FastFed is using the SCIM schema as the lingua franca of establishing federations.

Group Chat:
From Jacob Siebach to Everyone: 10:48 AM Please explain what "SCIM" is.
From Me to Everyone: 10:49 AM http://www.simplecloud.info/
From Juan Caballero to Everyone: 10:50 AM @Jacob: https://tools.ietf.org/html/rfc7642
From Jacob Siebach to Everyone: 10:50 AM Thank you both. :)
From Neil Thomson to Everyone: 10:53 AM link to presentation?
From Juan Caballero to Everyone: 11:00 AM full disclosure, i'm a tourist, no need to tailor the presentation to me :D
From Rainer Hörbe to Everyone: 11:01 AM re the HR extension: it would be nice to consider not only the joiner/mover/loaver processes, but the transfer as well (new record in authoritatiove source, but account + entitlements are kept) - I found this quite frequently in workforce IAM
From Juan Caballero to Everyone: 11:09 AM ^ sounds pretty SSI? +1 thanks all! I learned a lot and am going to go "butterfly" around other sessions. Keep up the good work!
From timcappalli to Everyone: 11:17 AM Can I grab 2 minutes at the end? (Not SSI related)
From Dmitri Zagidulin to Everyone: 11:24 AM sure thing!

From Satish Joshi to Everyone: 11:24 AM Dmitri, can I get details of the organizational identity POC work you mentioned?
From Dmitri Zagidulin to Everyone: 11:28 AM I'm having trouble locating an actual website for the POC, but here's some press releases mentioning it: https://www.prnewswire.com/news-releases/digital-bazaar-and-gs1-us-collaborate-on-a-new-proof-of-concept-exploring-the-intersection-of-organizational-identity-and-blockchain-technology-300923178.html
From Satish Joshi to Everyone: 11:28 AM Thanks
From Dmitri Zagidulin to Everyone: 11:29 AM and https://www.ledgerinsights.com/digital-bazaar-gs1-digital-identities-for-supply-chain/
From Lawrence Liu to Everyone: 11:34 AM @dimitri there is a 3rd part of obstacle that is legacy processes of enterprise needs to be changed Like my bank (HSBC) they have a photocopy of my ID on file. But each time I file of a new service even I can prove myself by login credentials they still want me to upload another photocopy of my ID I believe it is the same as insurances companies
From Dmitri Zagidulin to Everyone: 11:41 AM @Lawrence ohhh excellent point
https://identity.foundation/working-groups/securedatastorage.html
^ this is the Secure Data Storage Working Group I mentioned earlier
From Jan Taylor to Everyone: 11:42 AM @Lawrence my state's drivers license bureau takes a photo every visit to update your photo even when renewing, updating address, endorsements, etc.
Can't remember where I was going with that though.
From Josh Verbarg (State Farm) to Everyone: 11:45 AM Michael Jones mentioned it in the OpenID Connect session... I started taking a closer look to understand it. and keep it going when the certs expire...
From Lawrence Liu to Everyone: 11:45 AM @jan I'm HK our driver license has no photo or address like North America. ID has photo but no address. It is renewed may every 10 years when there is a country wide call for renewal. Typically u will have 1st ID before 12 yrs old then changed at 18th yr old and after than it depends on when u loose your ID or country call for a revision
From Me to Everyone: 11:45 AM https://openid.net/wg/fastfed/
From Lawrence Liu to Everyone: 11:46 AM So y does my same bank and branch still need the photo id when it is already on file
From Me to Everyone: 11:46 AM https://www.sailpoint.com/blog/fast-federation-onboarding-applications-to-your-identity-provider/?elqct=website&elqchannel=organicdirect
From Jan Taylor to Everyone: 11:46 AM @Lawrence wow, now that makes sense. It's the same ID every policy.
From Me to Everyone: 11:46 AM https://www.sailpoint.com/blog/sailpoints-fast-federation-fastfed-sdk-released/?elqct=website&elqchannel=organicdirect
From Lawrence Liu to Everyone: 11:46 AM If they do not change legacy processes DID and SSI will not take on
From Jan Taylor to Everyone: 11:47 AM Right
Thanks Everyone!

Patient Choice Using Distributed Identifiers

Tuesday 9E
Convener: Tom Jones
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presentation is on this page http://tomjones.us/Home/Solutions

The methods for providing users with strong assurance eg X.509 have not had acceptable UX
NSTIC → IDEF

The discussion is about enabling great Level 2 experience (when user makes an assertion they need validation; identity assurance needs proof of identity proofing; authentication assurance needs proof of protection of user secrets; cover nearly 1:1 claims about the user; 3rd party claims can extend to comparisons of different co-pay choices; any of these can be bound to other user contexts at other HIPAA entities)

At registration the new patient needs (driver's license; health insurance card; payment card; health history)
The information received can be validated by some existing technique and methods
Patient Registration with Distributed Attributes - standard
Precondition :

In this use case the patient has a smartphone; has the capability to load an app (which controls the identity and release of information). It is optionally possible to consider that the phone holds the healthcare information for the patient

PCP gives the user the location or, URL so that the app can be loaded on the phone - could be a QR code

User loads app on their phone → establishes an identifier on their own (self issued identifier) → user binds the identifier to medical records at the PCP/Hospital → phone binds the identifier to claims of authentication assurance

The app is a "certified app" and the phone is capable of securing the user's secrets.

User can use these claims in a new context with any other HIPAA covered entity. User agent could download user data in FHIR format. User agent could verify the trustworthiness of any provider. User could upload user FHIR data to any certified web site. The goal is that the FHIR data never leaves the context of HIPAA

If the device is "shared" - given to another user with the screen unlocked; the new user (not the one who created the profile) is likely to have access to the app and detail. Unless the app requires secondary authentication for data/functionality within the application container
Guardianship role capability can be added to the flow which is driven by the app.
Minimal user data needed

DID WG Q&A

Session: 9F
Convener: Brent Zundel
Notes-taker(s): Brent Zundel

Tags for the session - technology discussed/ideas considered:
DID, W3C, standardization

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Primary discussion involved questions about the progress of the DID WG, i.e., what are we currently working on, what are the key discussions, what is the scope of the work, etc.

Rough summary of answers given: We are working to define DIDs, related documents, and guidelines for DID Method specifications. We are talking about metadata and where it belongs, DID resolution contracts, and DID URL parameters.

If there is something you want the DID WG to talk about, or if there is something that needs to be added to/removed from the spec, please raise issues on our repositories: https://www.w3.org/2019/did-wg/

Saved Zoom Chat:

09:57:03 From Chris Lee : Catch you guys later!
10:28:02 From Dan Burnett : webex stole my mic
10:28:12 From Dan Burnett : and won' give it back
10:28:45 From Dan Burnett : what i was going to say is that "A DID identifies a DID Subject, and a DID Subject is the Subject of the DID" :)
10:29:04 From Dan Burnett : trying to rejoin
10:29:04 From Will Abramson : hahah
10:30:18 From Dan Burnett : Read
10:30:23 From Dan Burnett : Create, Read, Update, Delete
10:30:37 From Dan Burnett : maybe now resolve :)
10:31:11 From Dan Burnett : Mic still not available to Zoom. My preceding WebEx call definitely didn't release it :(
10:31:50 From Dan Burnett : until the mic resource lock expires
10:32:21 From Dan Burnett : DID methods
10:34:29 From Will Abramson : Possibly this- https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/draft-documents/decentralized-did-rubric.md still a WIP
10:36:14 From Dan Burnett : The rubric will be published as a non-standards-track (informative) document by the W3C DID Working Group
10:36:26 From Will Abramson : cool

The Future of Indy, Aries & Ursa

Session: 9G
Convener: Richard Esplin
Notes-taker(s): Keng Suzuki

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Discussion topics:

- Background on the projects
- Current work items
- Open questions about the future

- purpose: for new contributors
- https://github.com/hyperledger
  - ursa related repo: ursa-rfcs, ursa-docs, ursa-python
  - indy related repo: indy-hipe(like rpc), indy-node(identity role on top of plenum), indy-lenum(consensus alg), indy-sdk(library makes easier to talk ledgers)
  - aries related repo: aries-rfc, aries-framework-[go|dotnet|, aries-acapy-plugin-toolbox, aries-protocol-test-suite
- bestway to track status:
  - https://wiki.hyperledger.org/display/indy/Indy+Contributors+Meeting
  - https://wiki.hyperledger.org/display/IWG/Identity+WG+Implementers+Call
- current work stream in here
  - indy-vdr
  - indy-credx: key storage
  - use more github issues
  - cicd (from jenkins to github actions)
  - rich schema (about verifiable credential)
  - privacy preserving revocation
- Communication place
  - chat: https://chat.hyperledger.org/home
  - create LFID: https://wiki.hyperledger.org/display/CA/setting+up+an+LFID
- indy networks
  - sovrin: public ledger
  - bedrock: steward model
  - consensus

- there is an independent Aries implementation, ACA-Pico, being written by students in Pico Labs as an open source project at https://github.com/Picolab/aries-cloudagent-pico

Sidetree Protocol / Element DID & Friends

Session: 9H
Convener: Orie Steele
Notes-taker(s): Orie Steele

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Orie shared these links:
https://github.com/decentralized-identity/sidetree
https://github.com/decentralized-identity/element
https://www.youtube.com/watch?v=XBSP1lkhjVo

^ This last video shows how Transmute has built https://element-did.com/ with the sidetree protocol.

We discussed the structure of the protocol.

Carl Youngblood (AWS) asked a lot of great questions about how to replace the ledger part, or the storage part.
Jayce (Bloom) asked questions about sidetree and did core compliance.

We talked about sidetree spec v0 and v1, and the timeline for finishing it (we don't know yet).

We talked about JSON Patch and JSON Schema based patches.

Orie revealed Transmute will not support JSON Schema based patches in Element V1, since they are not necessary if you support ietf-json-patch.

Kyle from Mattr asked questions about why ietf-json-patch is important.

We discussed that it allows the did controller to update their did document, including adding support for experimental features or new key types like GPG and BBS.

Troy from Secure Key explained how they use Sidetree with Hyper Ledger Fabric.

Secure Key uses sidetree for things other than did documents.

Transmute uses Sidetree to store hashlinks to Encrypted Data Vaults / Secure Data Stores as a way of scalably commiting to specific versions of credentials.

Sidetree spec v1 has a lot of breaking changes.

The DIF Sidetree WG is working to finish spec v1 and implementers are tackling these changes independently of each other.

Microsoft won't support IETF JSON Patch, Secure will support both IETF JSON Patch and the JSON Schemas, Transmute will only support IETF JSON Patch.

Understanding MyData Operators

Session: 9I
Convener: Iain Henderson
Notes-taker(s): Nicky Hickman

Tags for the session - technology discussed/ideas considered:

#MyData #Personaldata #empowerment

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

White Paper published today https://mydata.org/operators/

- Move from 'protection' (e.g. GDPR) to empowerment, actionable rights rather than protective rights
- MyData is a 'movement' ~ 200 organisations, 1000 people, distributed org model via local hubs, annual conference, more focused than IIW but some fellow travellers

MyData Operators - acknowledge that most people can't manage their own personal data, an Operator is a new category of businesses that empower the individual

- 20/30 'proto-operators'
- MyData offers ecosystem governance, holding operators to account, operator will typically(but not necessarily) have a **fiduciary** relationship (e.g. with a doctor, a lawyer, a government), with the individual. The Operator must work for the individual or be **neutral** (a facilitator), cannot work for an organisation or a platform.
- Reference model is not defining solutions or standards, but instead defining requirements, look to W3C etc to continue to develop standards that promote the primacy of the individual
- Promoting interoperability
- Most significant element is that if an organisation wants to be a MyData Operator, they must be able to be interoperable with other operators, More than Data Portability MyData Operators must demonstrate strategy / roadmap to move towards interoperability

Important work that starts to build potential for a real market.
Power in terms of

- no specification of standards
- no specification of tech
- focus on business requirements and Governance

Adrian Gropper: Now moving towards Standards discussion here @ IIW based on the principle that we already have the tech and the standards

Johannes Ernst: MyData is important and very focused community. Interoperability is important for the market to emerge not essential - e.g. personal computing market, expect Data Operators to go the same way. (discussion as to whether standards should come before or after market adoption) Compelling vision of a new market category called Data Operators - data is not held hostage

Nicky: Classic application of ToIP Stack - starting with business, flow through governance, now time for the tech. Operators exist in Layer 3 (Data Exchange) would great to work with ToIP Foundation to start enabling this market

Adrian: Transactional Authorisation work in WIETF

John W: Build social trust, MyData focuses on building services that people can trust, these are different types of standards in human trust than those standards in technical trust. Will be domains / Vertical standards

Nicky promised to share some slides on Data Value Cycles -and pointed at the important gap that the data operator filled at the heart of the cycle

Adrian: Still need standardisation in things like 'privacy policies' ref from Nicky re Doc's Machine Readable Privacy Terms (IEEE)
John W - tools for managing personal data still not realistic - Operators are needed
Johannes - lots of different potential business models
Iain - More work on showing their model and approach to start working towards interoperability

What does MyData need from us ?

- **Join MyData,** very Euro-centric, under-represented in USA
- Johannes has helped start a MyData Hub in heart of surveillance capitalism (Silicon Valley)

Haiku:
MyData Operators
Interoperating
To Empower Me

CHAT THREAD:
From Me to Everyone: 04:57 PM link to the paper https://mydata.org/operators/
From Kazue Sako to Everyone: 04:58 PM Hi, I am vice-chair of MyData Japan
From John W (JLINC & MyData) to Everyone: 05:08 PM Can you post the link again
From Iain Henderson to Everyone: 05:08 PM https://mydata.org/operators/
From Kazue Sako to Everyone: 05:12 PM Is there a link for your presentation? I missed first 20 minutes or so
From Iain Henderson to Everyone: 05:16 PM I'll post that after the session Kazue thanks
From Kazue Sako to Everyone: 05:16 PM Thanks!
From Juan Caballero to Everyone: 05:23 PM Brussels is pretty cool these days!
From Me to Everyone: 05:25 PM Have you got a link for that you can put in the notes? @ Adrian
From Johannes Ernst (Indie Computing) to Everyone: 05:29 PM I have some audio issues, just me?
From John W (JLINC & MyData) to Everyone: 05:29 PM Adrian; you're mic died
From Me to Everyone: 05:29 PM Surely it depends on what you're trying to standardise
From John W (JLINC & MyData) to Everyone: 05:35 PM Schroedingers Data
From Juan Caballero to Everyone: 05:35 PM thanks all! i'm gonna keep rotating
From Me to Everyone: 05:50 PM
These are the slides I shared https://docs.google.com/presentation/d/1QIL9P7036E4VmsK6Uq--UQ4niTlijsnTWrMrxsYcno8/edit?usp=sharing
From Iain Henderson to Everyone: 05:50 PM Thanks Nicky

GS1's Decentralized Approach to Resolving Identifiers Over HTTPS

Session: 10A
Convener: Phil Archer, Gena Morgan Paul Dietrich, & Melanie Nuce
Notes-taker(s): Gena Morgan & Orie Steele

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slides are at https://docs.google.com/presentation/d/1fLDETcghxxRfac7mDCTGpqktaVnn9bjl/edit#
General principles paper is at https://gs1.github.io/DigitalLinkDocs/principles/

GS1 DIgital Link standard makes the standard product Identifier - the "UPC" code web resolvable. Making it do more than go beep at the check out.

SSI / DIDs "not central point of issuance, no single point of failure"...but we can meet those requirements with persistent identifiers with centralized federation… centralized + delegation can work.

We can resolve identifiers with DNS / HTTPS… and it works today!

Bar codes are 40+ years old… they are trusted and used everywhere… its deeply embedded, its here to stay… we are trying to make those identifiers resolvable / dereferencable.

GS1 operates in lots of sectors / healthcare /automotive / construction and most known for retail.

GS1 is in 114 countries, truly global… GS1 has people in north korea :)

Bar Code -> URL -> URLs

How do we learn more about products in a structured way? _Using URLs!_

Location, Batch, Manufacturer, etc… the vocabulary for products can be embedded in URLS, and some of that information can be extracted without even being online.

What do we mean by "resolve"?

We want to be able to link to multiple types of information.

Any one thing, will have lots of associations… we can link to them all.

We can also query, not just resolve… using linkType parameter.

Can you give me patient information, a video, etc… the resolver will comply if it can.

You can also ask for all the links…

The structure of the JSON response is not standardized yet.

There will likely be a way to provide a signature on it.

Other companies can provide their own resolvers.

All the HTTP / DNS stuff works at the network level… so you don't need to download a whole HTTP page to get all the links.

So what? How does this compare to did resolution?

You can take a bar code, and you can resolve that barcode to a number of things… b2b, b2c, or an e-wallet with credentials.

3rd Party Credentials for Organic, Gluten Free, etc…

Some claims have more weight when they come from a 3rd party, such as a certification body - not the first party brand.

Key points:
- We just use HTTPS… its massively implemented and supported… it works in web browsers.
    - Identifiers can be persistent as well… specs are persistent… web addresses can be persistent if you want them to be.
    - HTTP depends on DNS, but identifiers don't.
    - We can say state our persistence policy, but humans will always be responsible for enforcing the policy.

GS1 doesn't want to be the only resolver.

The GS1 Resolver Code is Apache2 on github, you can run your own… maybe on a cloud other than Azure.

The identifier is separate from the resolver…. the same identifier might resolve to different documents depending on the resolver…. this is a a feature defined in the standard… v2 is coming soon.

How do we make the use of VCs valuable?

How do we say a Product is Gluten Free as stated from a specific organization.

credential identifier is a URL.

credential type "NutritionalClaimCredential"

Example uses a regular HTTPs URLs.

VC Data Model does not require the use of DIDs! for Subjects, Holders or Issuers.

Credential Subject will be a GS1 Identifier.

GS1 uses machine readable vocabulary.

GS1 doesn't need to use DIDs. Even if a verifiable credential (issuer) . COuld use if you wanted commitment to a credential at a moment in time and in a way that is "trustless". Time based feature of this may be what is valuable.

DID controller determines what goes into a DID- so DID doc is augmented with commitment.

Should we use DIDs? How does it make it more (or less) secure than a URL as an identifier with a signature around the data block? Not clear that the complexity of DID resolution provides more security or trust t serving up the linked data from the resolvable product ID..

VC data model does not require came before the DID std. Trust system lies with DNS and domain and operator with HTTPS. (Orie - please help summarize what you just said :-))

DiD resolvers are no more secure than a DNS against attacks. Certain risks in DNS but any new technology still requires trust and the may be subjected to similar attacks

==Zoom Chat log ==
From Infominer to Everyone: 07:40 PM just add 3 letters at the end 'ZKP'
From Infominer to Everyone: 07:49 PM this is great, happy to hear :)
From Eric Welton (Korsimoro) to Everyone: 07:53 PM walmert.com?
From Gena Morgan to Everyone: 07:56 PM so - in summary, the presentation of data from a particular source of that data can be signed (to ensure their identity is trusted) and we have trusted data from whomever the source may be. Is that correct? so we don't need DIDs for serving up supply chain data between trading partners and even consumers
From Me to Everyone: 07:57 PM That's my understanding, yes
From Eric Welton (Korsimoro) to Everyone: 07:58 PM i agree as well - there are some concerns around that -- orie might be able to speak clearly to them. it is not the sort of thing you can take with the same level of assurance as, for example, a public/private key pair are *pairs*
From Jace Hensley to Everyone: 07:58 PM The proofPurpose field of the proof object also tells you how to validate that proof using the resolved document for the keys
From Eric Welton (Korsimoro) to Everyone: 07:59 PM i wondered if you could say "pp.<method>" and then have a pp object in the DID-doc.... but I never worked out if that made sense or horribly broke things... thoughts?
From Jace Hensley to Everyone: 08:03 PM That's kinda what the proofPurpose+verificationMethod fields do right? proofPurpose tells you where to look and verificationMethod tells you what to look for (what key to look for in the DID doc) Saying DID doc but it could be any controller doc

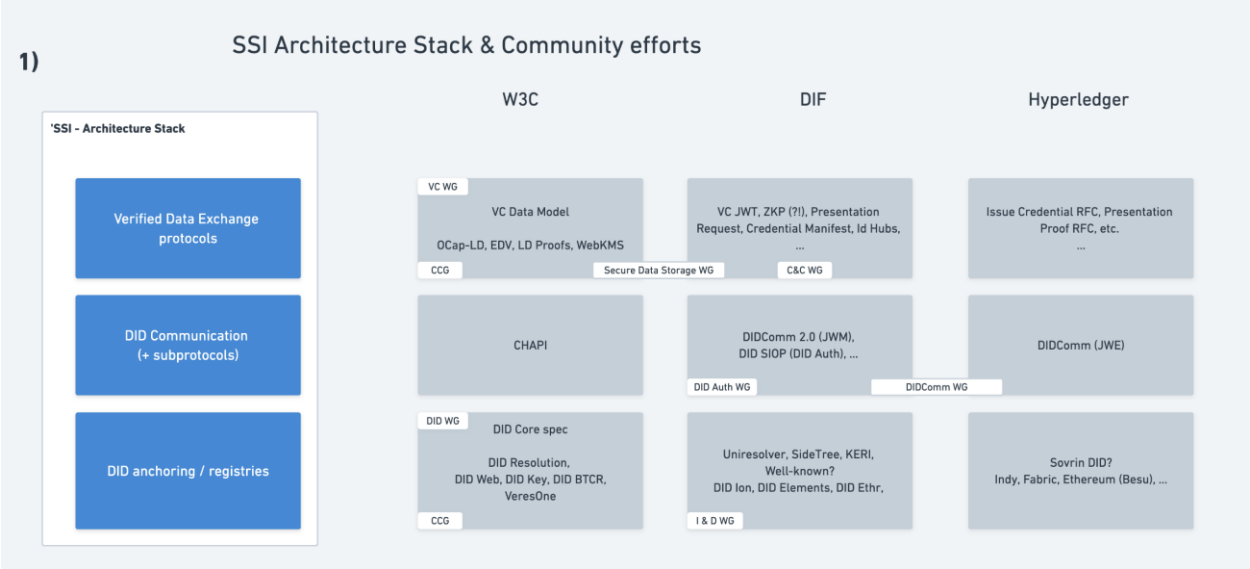
SSI Architecture Stack/Layers & Community Efforts

Session: 10B
Convener: Rouven Heck
Notes-taker(s): Sarah Allen

Tags for the session - technology discussed/ideas considered: #SSI STack

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

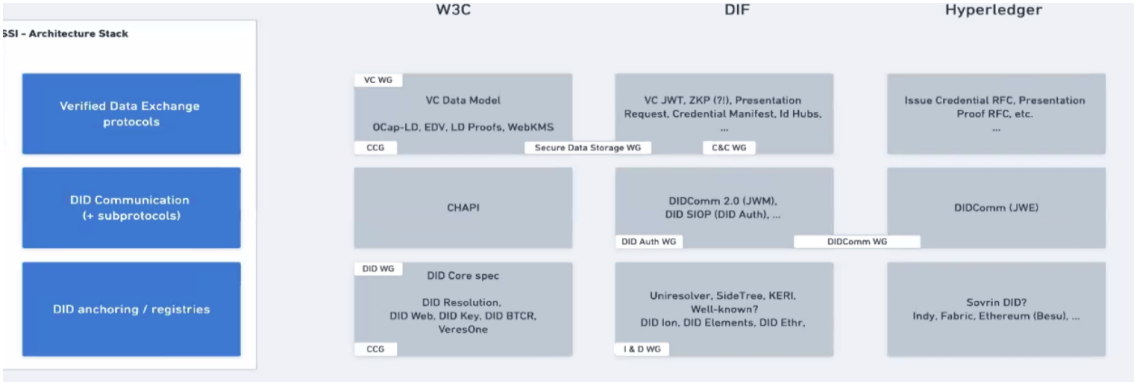
Background: about a year ago, a session about SSI protocol stack, industry has evolved,



We reviewed Figure 1: https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0289-toip-stack/README.md

Layer 3: Data Exchange Protocols: Credential exchange
Layer 2: DID Comm protocol
Layer 1: Public Utilities: Somewhere we anchor DIDs

Many open questions, for example: Where does credential storage live? starting point….



VC Data Model: Verifiable Credential Data Model

CHAPI: Credential handler API

KERI: Key Event Receipt Infrastructure

SIOP?

DIF: Decentralized Identity Foundation

maybe help to agree on the communication between the layers…

“a blockchain is not a blockchain is not a blockchain” — people are calling things blockchains that have neither blocks nor chains,

Trust over IP stack doesn’t include word “blockchain”

We want to abstract Layer 1 ⇒ give it a DID, get back a DID Document

Besides Pub/Private Keys, we need the DID abstraction layer

The schema will have a DID and you will look up the schema referred by the DID

Entity vs Object Identifier

Ideally Layer 3 is also self-contained

Layer 1 ⇒ All about DID resolution
Layer 2 ⇒ All about security and privacy
Layer 3 ⇒ All about credentials

Layer 3: Data Exchange Protocols: Credential exchange
Confused -
Layer 3 - for exchanging credential
different layer to use. Trying to parse it all.

Over DIDComm - verifiable credential exchange - one thing you can do.

Lots of places not need a high trust credential.

Not necessarily

What does trusted data stored and claims mean?

DIDComm is a secure and private communication protocol. Can make any protocol run over this.
DidComm is not a transport protocol.

DIDComm is not about trust, it is about security and privacy. It verifies that communication is from a specific identity, but does not indicate who is behind that identity. Cryptographic trust.

DID provides an assertion of sameness. Meaningless yet globally unique and resolvable.

Layer on what are the attestations of the thing you have just identified.

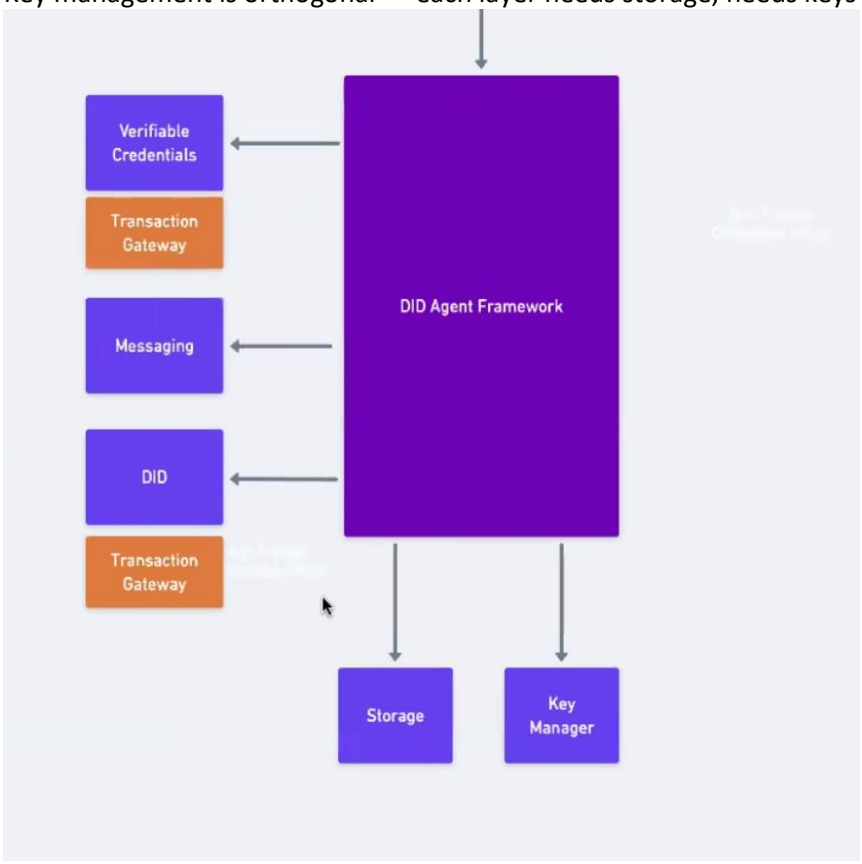
Proving control over a DID does not itself constitute what we typically associate with "authentication"

Goal: Layer 3 things can use any Layer 1 things

CHAPI constitutes the basis of a secure connection the same way DIDComm does, but I would not classify it as "DID Communication"

Layer 1 seems most clear (description slightly revised)

KERI is actually completely at Layer Two
KERI is a DKMI. Seems like Layer 1.
KERI actually a key management infra, more like layer 2?
Key management is orthogonal — each layer needs storage, needs keys



Maybe Keri isn't in the diagram, rather it is a support function

"KERI is a way of life"

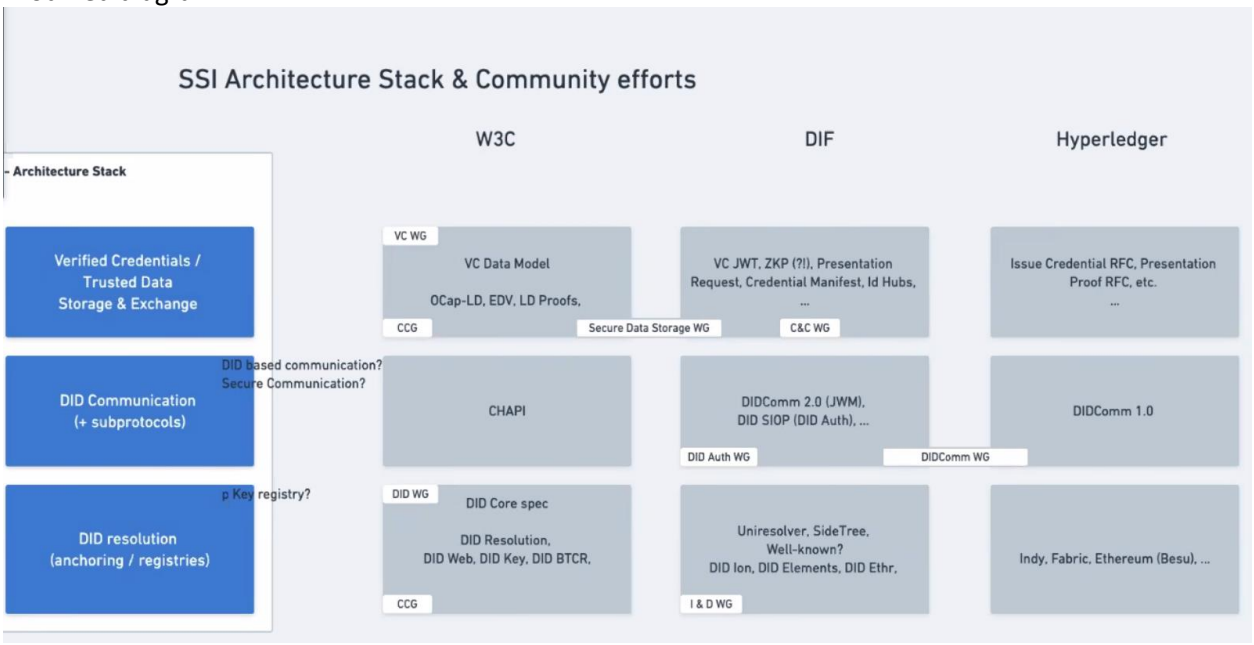
Separate Governance from technical initiatives — e.g. Veres One, Sovrin

This framework supports bottoms-up and top-down governance

People can choose which tech and which governance model

The type of governance needed at each layer is very different.

This diagram is super helpful where having examples in each box help us to understand the category. An example trust framework would be very helpful.
Modified diagram...



CHAT From the Zoom SESSION:
This diagram is in this doc: https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0289-toip-stack/README.md

@Sarah - to be clear, the link I provided was to the first diagram Rouven showed (the ToIP stack). I don't have a link to this one Rouven is showing, but hopefully he does

The link is there but doesn't have public access.
http://www.whimsical.com/U2YsBVLyBKgPt2rt76TFYs

Trust over ip: https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0289-toip-stack From Juan Caballero to Everyone: (11:19 AM)

+1 Anil. Proving control over a DID does not itself constitute what we typically associate with "authentication"

As an application or system software developer, I find this kind of diagram very helpful Also, as a protocol implementer

^ Good feedback!
Also, as a community organizer.

@Sarah Me too, but then, I'm biased after a year of working on the ToIP stack BTW, I'm still on the queue to talk about where storage belongs

Phrased in another way, this three layer stack would be:
- Secure Data
- Secure Connections
- Public Key Registries

From Sarah Allen to Everyone: Aren't we humans?
From Sam Curren to Everyone: speak for yourself Sarah! :)
From Drummond Reed to Everyone: What Anil is explaining is why we now present the Trust over IP stack with the ToIP Governance Stack on the left and the ToIP Technology Stack on the right. Because the needs of a trust community first have to be mapped into their governance policies, and THEN into technology
From Nader Helmy to Everyone: Credential handler API constitutes the basis of a secure connection the same way DIDComm does, but I would not classify it as "DID Communication"
From Drummond Reed to Everyone: KERI is actually completely at Layer Two
From Sam Curren to Everyone: Uh... maybe.
From Nader Helmy to Everyone: KERI is a DKMI. Seems like Layer 1.
From Juan Caballero to Everyone: KERI is a way of life I like this one still no idea where KERI goes
From Drummond Reed to Everyone: (11:45 AM) Yes, I would agree with what Rouven is saying. KERI is key management architecture.
From Brent Zundel to Everyone: (11:47 AM) You may not need storage for DIDcomm, but you would need key management, right?
From Juan Caballero to Everyone: (11:48 AM) should we call it... Secure Data Storage?
From Brent Zundel to Everyone: (11:48 AM) right, just trying to tease out the difference between storage and key management.
From Juan Caballero to Everyone: (11:48 AM) I, for one, would like a zany neologism like Vaulting
From Drummond Reed to Everyone: (11:48 AM) Yeah, I like that, catch term! ;-)
From Me to Everyone: (11:50 AM) it can potentially SOLVE a huge Relying party problem.
From Oliver Terbu to Everyone: (11:51 AM) Isn't it a CCG work item or WG group?
From Brent Zundel to Everyone: (11:52 AM) https://www.w3.org/community/veres-one/
From Juan Caballero to Everyone: (11:52 AM) DID:sov ? Oh that reminds me where is DID:peer governed?
From Sam Curren to Everyone: (11:54 AM) in a repo. :)
From Nader Helmy to Everyone: (11:55 AM) DID Peer is also in the process of moving to DIF if I remember correctly
From Sam Curren to Everyone: (11:55 AM) I believe that's true.
From Bruce Conrad to Everyone: (11:55 AM) In the sense that everyone who uses peer DIDs governs themselves? using code in a repo
From Juan Caballero to Everyone: (11:56 AM) it just struck me as a little cog with big consequences for the stack!
From Sam Curren to Everyone: (11:56 AM) governance is light for did:peer. it mostly relates to the governance of the spec itself, not really usage.
From Drummond Reed to Everyone: (11:56 AM) In the Sovrin Update session coming next, we'll be talking about how governance frameworks fit into the Trust over IP stack

From Juan Caballero to Everyone: (11:56 AM) touché
From Bart Suichies to Everyone: (11:57 AM) I like the distinction between governance on the tech, and governance on the usage of the tech
From Drummond Reed to Everyone: (11:57 AM) @Sam Curren - exactly right wrt the did:peer spec. The governance there is entirely over the spec.@Bart +1
From Nader Helmy to Everyone: (11:57 AM) We should accept it will be exceedingly difficult to get additional governance on chains like Bitcoin
From Drummond Reed to Everyone: (11:57 AM) +1
From Bart Suichies to Everyone: (11:58 AM) you cannot compare governance from tech, and legal governance.. they are separate.. need to exist both.
From Nader Helmy to Everyone: (11:58 AM) Governance is required at some layers, but not all and not in all circumstances
From Drummond Reed to Everyone: (11:58 AM) There can be different governance frameworks (including NO formal governance framework at all) at all four layers
From Juan Caballero to Everyone: (11:58 AM) and the other way around
From Drummond Reed to Everyone: (11:58 AM) Bitcoin has no formal governance framework at Layer OneYes
From Oliver Terbu to Everyone: (11:59 AM) Ethereum can be permissioned as well
From Sam Curren to Everyone: (12:00 PM) Ethereum or ethereum ? (capitalization matters in this case)
From Bart Suichies to Everyone: (12:00 PM) is the question what layer's governance model should be leading? Tech driving governance, or the other way around?
From Juan Caballero to Everyone: (12:01 PM) ^ I'm really not sure what the question is
From Juan Caballero to Everyone: (12:01 PM) it might be helpful for someone to state it
From Bart Suichies to Everyone: (12:01 PM) eg: governance model of layer 4 drives decisions on technology (how things can work, assurances on technology, etc)or: bitcoin as a technology exists, and governance on layer 4 is based on top of potential of technology
From Drummond Reed to Everyone: (12:02 PM) +1 Bart
From Juan Caballero to Everyone: (12:05 PM) heyo we got 10 minutes left, did Rouven have questions?
From Geovane Fedrecheski to Everyone: (12:07 PM) do we have public examples of governance frameworks, with all (or most) of the roles fulfilled?
From Drummond Reed to Everyone: (12:09 PM) @Geovane - there are some at certain levels, but not at all levels yet. For an example of Layer One, see https://sovrin.org/governance-framework/
From Geovane Fedrecheski to Everyone: (12:09 PM) cool, thanks @Drummond!
From Manu Sporny to Everyone: (12:10 PM) Squirrel!!!
From Oliver Terbu to Everyone: (12:10 PM) Alastria
From Drummond Reed to Everyone: (12:10 PM) There are a lot of opinions about Layer Two, but if we are going to see the full benefits of a thin-waist protocol stack, we need ONE protocol on layer 2
From Karyl Fowler to Everyone: (12:10 PM)There you are @manu! we learned about Veres One's community group earlier!
From Brent Zundel to Everyone: (12:10 PM) I think this has been a really good conversation. There are 5 minutes left. Where do we go from here? What are some concrete next steps?
From Oliver Terbu to Everyone: (12:10 PM) Alastria has defined a Trust Framework
From Juan Caballero to Everyone: (12:11 PM) ^ ¡Viva España!
From JC Ebersbach to Everyone: (12:12 PM) @Oliver, do you have a link to the framework?
From Juan Caballero to Everyone: (12:12 PM) https://alastria.io/en/estructura-de-alastria/

Getting Back To Work: End to End Concept Live Prototype Using Hyperledger Aries for Essential Workers

Session: 10C
Convener: John Jordan (BC Gov)
Notes-taker(s): Stephen Curran

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Overview: Welcome to the SafeEntryBC prototype, a conceptual model describing a set of tools that might help us explore ways to help citizens and the economy of BC as we transition from our current state to "the new normal." A successful transition requires that as citizens move around more, they can be as safe as possible. In many places that will mean knowing more about other people with whom they are interacting, particularly service providers that are entering controlled-access facilities. In places at risk of a COVID-19 outbreak, such as extended care facilities and hospitals, great care will be needed in preventing infected (potentially asymptomatic) service providers from entering. But in the initial stages of restarting the economy, such controlled access locations might be everywhere—even people's homes.

SafeEntryBC is a contact-less way to manage the risk of service providers coming into a space you control. As we gain a better understanding of the science, people could have a set of credentials (whatever those might be) to help manage that risk. Think of SafeEntryBC as a replacement for the "Visitor's Log" you saw in many businesses in the old days (you remember, back in January 2020). With SafeEntryBC, instead of writing down your name, company and date of visit, you are sent a real-time request for a set of (digital) credentials that you must present that are suitable for mitigating the risk of you entering the facility. In some places, that might be just your name and the company for whom you work. In high risk locations, such a request might include asking for a credential about your COVID-19 status—perhaps a recent "negative" test or (if/when such a thing becomes available) an immunity credential.

Folder with presentation and related materials.
A guide to the prototype: https://vonx.io/safeentry
Feedback and collaboration welcome - connect with us at https://vonx.io

Zoom Chat Log

11:05:17 From Tushar Phondge : Will the deck be shared?
11:05:18 From Laura Jaurequi : yes
11:05:34 From Tushar Phondge : thanks
11:11:59 From Stephen Curran : The presentation is ever evolving, but here is the Google Docs folder where it is being kept:
https://drive.google.com/drive/folders/1HalA8fQX73B-hIKllPbDbLfMvvg5dIMm?usp=sharing
11:28:13 From Stephen Curran : An overview/guide for the entire story can be found here:
https://vonx.io/safeentry
11:43:44 From aj-finema : Very cool. Thanks John
11:44:11 From Stephen Curran : Still a DIDComm channel...just not a permanent connection.
11:44:21 From rileyhughes : The connectionless credential still uses DIDComm
11:44:28 From rileyhughes : Oh I see Stephen got there first…
11:44:39 From rileyhughes : It's just an ephemeral connection, the same way the ephemeral challenge is done

11:46:21 From Mario Bonito : What is the benefit to connectionless over connection oriented issuing? Efficiency? Something else?
11:46:50 From Mario Bonito : Ahhh ...
11:47:45 From Andrew Whitehead : Hold on let me QR-jack that
11:48:18 From Ben Weaver : Q: what is visible to passive observers? Could anyone see which people go into which buildings
11:48:21 From Mario Bonito : Excellent thank you.
11:48:36 From Christopher Hempel : Kudos!
11:48:59 From windley : Really exciting stuff. Excellent
11:49:22 From Jesse Empey : That was awesome John. Thanks!
11:49:38 From Kalyan Kulkarni : I can think of a connectionless cred example where the credential is going to be for a shorter duration - may be for a week or so.
11:49:44 From Ramnath Krishnamurthi : absolutely brilliant stuff
11:49:55 From Mathieu Glaude : Really awesome demos John. And kudos to Streetcred and esatus teams!
11:49:58 From Stephen Curran : @BenWeaver - no different from today.
11:50:38 From Mario Bonito : Echo the Kudos, well done BC Team, Street Cred, and esatus team.
11:50:53 From Kalyan Kulkarni : +1 - awesome, quick, crispier demo
11:52:48 From Andre Kudra : Thank you so much, highly appreciated! BC Gov are the heroes, they are bringing SSI to life, with our tech. Impressive work, well done, John & Team!
11:53:22 From rileyhughes : +1 Andre! 👏🙏
11:53:49 From Michael Shea : good job!! well done!
11:54:03 From david mason : Amazing groundbreaking work.
11:54:48 From Philippe Page : Can you exchange credentials between wallets ?
11:55:00 From Gary de Beer : Loved seeing that inter platform compatibility. Awesome.
11:55:13 From Stephen Curran : You can do proof requests/responses if the wallet supports it.
11:55:50 From Philippe Page : Thanks -Really impressive demo. Great job.
11:55:51 From windley : Generally, you can’t move credentials between wallets for security reasons.
11:57:04 From windley : Credentials contain a credential secret which allows presenter to prove the credential was issued to them. If credentials could be easily moved, then it would be much hard to ensure that the credential isn’t being shared.
11:57:53 From Andre Kudra : Wallet to wallet VCs (between two persons) would be "only" peer to peer without a public DID.
11:58:24 From windley : Ah, sorry, maybe I misunderstood the question.
11:58:43 From windley : Thanks Stephen
11:59:01 From Andre Kudra : In the IIW SSI Spotlight 5 Prio Topics we are discussing possibilities for "on-device credential sync", i.e. you have more than one wallet on your device and want to have all your credentials in all of them.
12:02:27 From Mario Bonito : lol
12:03:39 From Christopher Hempel : So awesome to see the progress happening in ssi since last IIW and i'm so proud to being part of it at esatus
12:05:19 From Mario Bonito : +1 John for deeper application integration. Are you looking at offering SDK’s for this? Or is this the approach for you were thinking when you say deeper integration?
12:08:29 From Mario Bonito : Perfect thank you
12:09:12 From Mario Bonito : Very impressive everyone, great work really pushing this forward. Thank you again
12:09:24 From Kalyan Kulkarni : By the way, ARNIMA - React Native Agent is also underway to hit readiness sooner
12:09:37 From aj-finema : Thank you John

12:09:38 From Laura Jaurequi : Thank you!!
12:09:44 From aj-finema : Thank you
12:09:45 From Kim Anderson : Thanks!

ID2020 Certification: Feedback & Next Steps

Session: 10D
Convener: Aiden Slavin & Dakota Gruener
Notes-taker(s): Dakota Gruener

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Attendees: Aiden Slavin, Brian Behlendorf, Cam Parra , Nathan George, Sam Goto, Lawrence Liu, Dakota Gruener, Jeffrey Hallett, Todd Gehrke, AJ Finema, Maryam Shahid

Overview of the ID2020 Alliance and ID2020's certification initiative

- ID2020 is a global-public private partnership focused on privacy-protecting, portable and decentralized digital ID. Partners include Microsoft, Accenture, Gavi, the Vaccine Alliance,
- The alliance is meant to drive critical mass on three levels:
    - Agreement on principles and norms around what defines "good" digital ID (and what defines "bad" ID) >> advocacy and regulatory engagement.
    - Development and adoption of interoperable "good" digital ID solutions >> ID2020 certification
    - Uptake of ethical digital ID programs >> program support, either through our grant-making or advisory engagements
- ID2020 defines four key principles for good ID: private, portable, personal and persistent

ID2020 certification sets a floor for digital ID solutions. Meant to:

- Race to the top: as certified products gain distinction in the marketplace, the entire market shifts towards good digital ID
- Drives convergence on technical standards for interoperability
- Provide valuable shorthand for organizations looking to implement digital identity systems, particularly for those without great technical depth.
- Product differentiation: companies can demonstrate their adherence to the highest ethical standards by certifying their products as ID2020 compliant

Requirements were established by ID2020's Technical Advisory Committee. They are updated annually. Requirements here: https://docs.google.com/document/d/1X8wKvPr-xEnF43BK0Bg-qK-woVspQirP27bChEW8Y8Y/edit ID2020

- We are just about to begin the first annual review. Call to the IIW community to provide input on how these can be expanded or improved upon.

- One key question: there is a tension between need to be solution-agnostic and flexible in terms of *how* solution providers achieve the requirements and the need for some amount of prescriptive-ness around standards in order to drive meaningful interoperability.

Importance of stories from the ground, both to strengthen the solution requirements and inspire the technical community.

Necessity of ensuring we don't take short-cuts now that bite us later. What is good enough, not just for the immediate need, but also longer-term?

- In the context of COVID, the certification mark could be used as a third-party measure of what's good enough. Embed in RFP processes for immunity / health status certificate programs.

On the horizon (and suggestions to expand the impact of this work):

- ID2020 certification expands beyond certification of end-to-end solutions to auditing implementations of these solutions, ensuring that not only is the technology good, but that the deployment of the technology adheres to ID2020's values
- Upcoming annual review cycle:
- Todd: need to ensure that each requirements is easy to measure; some currently a bit objective
- Brian: marketing necessary to build the case for why organizations should verifiable credentials. Create a series of videos (slickly produced) that could be put in front of the general population to see the workflow, understand why it's safe.
- Todd: recommend design patterns (i.e. show what iRespond is doing for biometrics)

ZOOM CHAT WINDOW

From cam-parra to Everyone: (12:43 PM)
I have to hop off the call. Thanks everyone this was a really insightful call :)
From Aiden Slavin to Everyone: (12:43 PM)
Thanks!
https://docs.google.com/document/d/1X8wKvPr-xEnF43BK0Bg-qK-woVspQirP27bChEW8Y8Y/edit ID2020 Technical Requirements ^
From Brian Behlendorf to Everyone: (01:03 PM)
https://raw.githubusercontent.com/DP-3T/documents/master/public_engagement/cartoon/en/shortened_onepage.png
From Nathan George to Everyone: (01:04 PM) Worse execution of the same principle
https://people.redhat.com/duffy/selinux/selinux-coloring-book_A4-Stapled.pdf
From Brian Behlendorf to Everyone: (01:04 PM)
https://vimeo.com/378793095 <-- Accenture video, high production quality, on traceable supply chain
From Aiden Slavin to Everyone: (01:06 PM)
https://id2020.org/uploads/files/ID2020-Certification-Report-Kiva.pdf
https://id2020.org/uploads/files/ID2020-Certification-Report-Gravity.Earth.pdf
Evaluation reports of two so-far certified
From Nathan George to Everyone: (01:06 PM) Those systems are *awesome* credential issuers, they just need more interoperability system for them
From Aiden Slavin to Everyone: (01:09 PM) Please provide further feedback to: Aiden@id2020.org

Every Vault Has A Key That Needs To Be Secured Outside The Vault. Role of Central Entities At the Periphery (Edges) of SSI Ecosystem: Seeking Answers to Questions Faced When Presenting SSI To Consultants/Customers/Users

Session: 10E
Convener: Venu Reddy
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:
#CredentialVerification #IdentityRecovery

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Relevance of existing techniques – PKI, central administration.

- For users "identity management is not a primary goal"
- IdM schemes with a novel technological underpinning without improved end-user interaction are unlikely result in widespread use
- Key management remains to be a principal source of concern for users of Bitcoin/Blockchain
  - Non-technical users may be alienated by the technology
  - When things go wrong these users will be unable to recover resources or reputation attached to lost keys

Credential Verification

- DID resolution to obtain metadata (DID Doc)
  - How do we prevent spoofing of meta data?
- Authoritative Issuers
  - How does the verifier verify that the Issuer DID belongs to the issuer and the issuer is authorized?
  - Governance (Trust over IP - John Jordan and Drummond Reed)
- At run time – the mechanism is likely to be similar to PKI
  - Well known DIDs (PKI root certificates) and their metadata known to every agent/wallet
  - Credentials (CA certificates) to certify the issuers and their DIDs
  - Transitive trust

Concluded that PKI-like mechanism is needed.

Identity Recovery

- Key rotation – prevent key rotation by identity thieves after recovery
- Device transfer/replace a lost device
- 3rd party access (legal, health and other life events) – trigger and
- Portability
- Recovery of a compromised identity

Use of multiple factors can improve security and persistence of recovery

Example

- Two factors to perform any of the above
- Three factors to change the factors themselves

Today, loss of access can be remedied using predefined processes with a fallback where system administrators can potentially intervene.

What is the fallback in case of SSI if identity is irrevocably compromised?

- Suspend the use of the identity
- Revoke credentials

A mechanism external to SSI ecosystem may be needed.

- Controlled manual intervention
- Bank safe deposit access pattern?

No solution can be found. Best case is to use multiple factors. User has the responsibility to secure and keep track of the factors:

1. device based factors
2. external factors

Fundamental Problems of Distributed Systems (2/3)

Session: 10F
Convener: Dave Huseby
Notes-taker(s): Cam Geer

Tags for the session - technology discussed/ideas considered:

Distributed systems, decentralization, collaboration

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to slide deck presented in session, provided by Dave Huseby:
https://docs.google.com/presentation/d/1C78Wq3vw1W1VJFVAps0KIr3EWPUSg_Xl306sB5Va7_0/edit?usp=sharing

Nine challenges:

1. Discovery: How nodes find one another on the network
2. Introduction: How nodes establish secure communications and exchange credentials.
3. Coherence: How nodes **re**-connect in a mobile and frequently disconnected world.
4. Public Services: Functions that operate on a system-wide basis.
5. Trust: Proving what, not who
6. Privacy (anti correlation over time)
7. coordination: Are all communications handled in the system?
8. Membership: Managing access to services both private and public
9. Persistent state: How does the whole system remember?

Here is the link to Konstantin's blog post on a magical (non-existent) collaborative development tool: https://people.kernel.org/monsieuricon/patches-carved-into-developer-sigchains

I mentioned CCLang: https://crates.io/crates/cclang
Secure Scuttlebutt came up a lot too: https://ssbc.github.io/scuttlebutt-protocol-guide/

Notes:
Dave's view is that Decentralization is a spectrum and moves in "the direction in which User Sovereignty *Increases*"

More formal definition from Sam Smith:

Our definition of decentralization (centralization) is about control not spatial distribution. In our definition decentralized is not necessarily the same as distributed. By distributed we mean that activity happens at more than one site. Thus decentralization is about control and distribution is about place. To elaborate, when we refer to decentralized infrastructure we mean infrastructure under decentralized (centralized) control no matter its spatial distribution. Thus decentralized infrastructure is infrastructure sourced or controlled by more than one entity. Entities are not limited to natural persons but may include groups, organizations, software agents, things, and even data items. This control may lie on a scale from highly centralized to highly decentralized. A centralized administratively managed identity system may be under the control of a single governing organization. A governing organization might also be hierarchical in nature with multiple subordinate organizations that operate under the auspices of the next higher level organization. The associated operational infrastructure might itself be highly spatially distributed despite being under highly centralized control or vice-versa. For example although DNS is administered by a single organization, IANA, the operational infrastructure is distributed worldwide

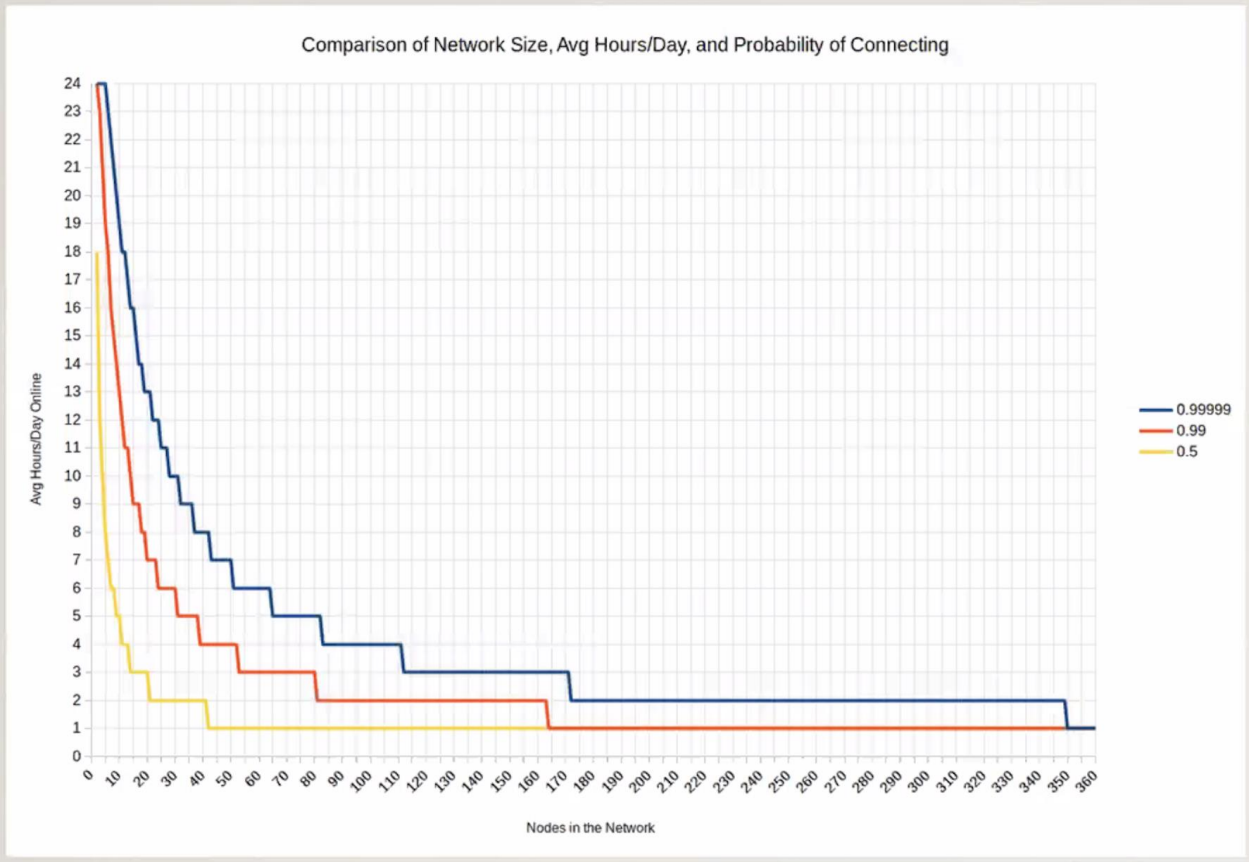
Nine Problems of Distributed Systems (with discussion points)

- Discovery
    - How new nodes discover another node to form/join a network
        - one of the hardest problems
- Introduction
    - How nodes establish secure communications and exchnage credentials
        - this is where SSI comes in
- Coherence
    - How nodes re-connect in a mobile and frequently disconnected world
        - context switching — mobile / laptop etc changes IP#'s etc makes it challenging
            - Q: is it deeper than the network protocol?
            - Q: how do you do this without central servers?
            - IPv6 could be a solution for this
                - needs further discussion
- Public Services
    - Functions that operate on a network-wide basis
        - (e.g. search, query, etc)
- Trust
    - Proving *what* not who and anti-duplicity (thanks Sam!)
- Privacy
    - Anti-correlation protection over time

- Co-ordindation
    - Are all communications handled within the system?
        - secure and private communication must be within the system
- Membership
    - managing access to services both public (p2p) and public (p2s)
- Persistent State
    - how does the system remember
        - blockchains are not be all and end all — just one method / others can be considered

Potential Solutions for the Nine Problems of Distributed Systems

- **Discovery Solution**
    - digital dead drops
    - distributed hash table with secure
    - P2P invites over text / phone QR code
    - BitcoinDB daemon for filtering / searching for payloads
- **Introduction Solution**
    - DIDComm?
    - Something Better such as Noise/Mega-Olm but with DID/KER
- **Coherence Solution**
    - **Last Known Whereabouts Protocol**



- Dave's thoughts
    - 5 am project to work without centralized server
    - each node must be able to act as a proxy for every other node
    - when over 50% probabilityto connect with one other node achieved — meta-stablity materialized

- Discussion
    - group of 10 friends to stay coherent
    - "seem like" fixed central server
    - fully coherent meta stable network
    - open source projects need critical mass to become self sustaining
        - sometimes social cohesion evaporates

- **Public Services Solution**
    - Bloom filters?
    - Query flooding?
    - No known good solution for public services without correlation
        - could Verifiable Claims cover this?
            - KERI — sam's work?
            - event receipt logs make full trust possible
- **Privacy Solution**
    - client-side encryption with crypto key escrow
    - PayPub-like protocol for sharing via cryptocurrency transfer
        - been discussing with Peter Todd
        - potential for subscription based crypto economy?

- **Coordination Solution**
    - all communication through a secure link, routed through the minxet network

- **Membership Solution**
    - key escrowing techniques from MegaOlm or Cryptree
    - token based access controls as long as token issuance is not tracked centrally
        - Dave & Mike Lauder have been discussing

- **Persistent State Solution**
    - Node based storage with erasure coding redundancy for reliability
    - Distributed ledger
    - IPFS or Tahoe-LAFS?
        - Dave's comment: "IPFS — too webby"

5am Project

- **Dave's vision to build an ideal developer tool from scratch. What would it need?**
    - client-side by default
        - no network required
    - offline by default
        - to support work in multiple modalities

- mobile by default
- Local hash-linked data structure container (ala SSB) with signatures in CCLang
- key value list in block header for higher level application (e.g. code patches, messages, file storage, key escrow, tweets, follows)
- Bitcoin OP_RETURN for discovery via dead drop payloads
- P2P discovery via secure text QR code
- Mixnet for IP making and secure information retrieval for store-forward async signaling
- Last known whereabouts protocol for minxes coherence and p2p-via-mixnet coherence
  - must have meta stability
  - needed for store and forward
- MegaOlm group key escrow for sharing coordination
- Did:Git like project/community based identity anchoring (provable hacker reputation)
  - should be the norm
  - preferred pronoun “Who?"
- Just works. Always in sync. Time and network agnostic.
- Replaces Github, JIRA, Mailing Lists, SSB, Web publishing

Dave’s 5am Project Summary Statement
I suspect a fully user sovereign, fully decentralized system will work like magic. Automatic discovery, automatic network formation, automatic synchronization, persistent and resilient and secure storage with instantaneous sharing regardless of data size. Automatic synchronization and ubiquitous integration via standard protocols and data formats. No need for any other system to use it effectively.

Zoom Session Chat:
11:04:44 From Grace Rachmany : I can't take notes for this one because I need to leave early.
11:05:07 From Grace Rachmany : I could take notes for the first hour
11:06:11 From Grace Rachmany : Thanks Cam!
11:07:27 From Grace Rachmany : It's going to be hard to reach you after this if you aren't findable online...
11:08:34 From dsearls : I see the left end here as living in a feudal castle, and the right end as being a free Samurai, a ronin.
11:08:35 From Wendell Baker : He's on Microsoft's GitHub ... the search engines will find him
11:09:58 From Wendell Baker : @marc, no worries ... the data markets idea seems to inflame emotion in surprising ways. I was fishing to see if ... Something for a garden talk.
11:10:19 From johnnyfromcanada : IMO, decentralization is about control, and distribution is an implementation detail. Orthogonal - i.e., you can have any combination of both (some combinations having less obvious cost-benefit).
11:10:32 From dsearls : Maybe there's a 2x2 here, with centralization-decentralization on one axis and distribution-? on the other axis.
11:11:07 From dsearls : Is there an opposite of distributed, if not centralized? Perhaps aggregated?
11:12:15 From dsearls : Dave, can you take a phone-shot or something that produces a .png or a .jpg of that graphic you just held up? If so, attach it to the session notes.
11:12:19 From johnnyfromcanada : “Centralized” is common for both - ambiguous use of it perpetuates the confusion of the difference.
11:12:34 From Cam Geer : dave .. sounds like the organic evolution of trust
11:12:43 From johnnyfromcanada : Perhaps monolithic?
11:14:01 From Grace Rachmany : Discovery on Distributed Hash Tables seems to be working.

11:15:21 From Marc Davis : I would argue that “degree of self-sovereignty” is an orthogonal axis to “centralized<—>decentralized” architecture. IMHO, degree of centralization is an implementation question and degree of self-sovereignty is a rights/duties/contracts question. It may be easier to “enforce” and/or implement self-sovereignty in a decentralized architecture, but you could imagine a centralized architecture with self-sovereign rights and a decentralized architecture with no self-sovereign rights.
11:17:39 From Grace Rachmany : Biomimicry can be helpful in thinking about how these things happen in complex systems. Expanding our view beyond how it's done in computing architectures opens up additional possibilities.
11:19:18 From Wendell Baker : https://en.wikipedia.org/wiki/Mobile_IP
11:19:26 From MarkL. @smartopian : A Security Problem -
11:19:30 From dsearls : @johnnyfromcanada, I think he opposite of monolithic is polylithic.
11:20:47 From Grace Rachmany : In some ways public services need to be built as separate apps that use types of polling and collection rather than tapping into a central servi8ce.
11:22:17 From johnnyfromcanada : @dsearls - Indeed, I am trying to brainstorm ;-) You like etymology (per “anonymous”). So perhaps “tributed”?
11:22:25 From johnnyfromcanada : https://www.dictionary.com/browse/distribute
11:23:22 From Elias Strehle : Is it possible to handle ALL communication within the system? What about communication that relates to the system itself (like Bitcoin's Improvement Proposals)?
11:23:50 From Grace Rachmany : I guess it depends on how you define "the system"
11:24:20 From Grace Rachmany : There isn't some intrinsic reason it shouldn't be possible within the system.
11:25:24 From dsearls : could be that "distributed" is the wrong word, inherited from Paul Baran in 1964: https://www.researchgate.net/figure/Centralized-decentralized-and-distributed-network-models-by-Paul-Baran-1964-part-of-a_fig1_260480880
11:26:05 From dsearls : It also carries familiar centralized assumptions, such as that a distributor is required for distribution.
11:26:11 From Michael Graybeal : “Voltron Effect” - a technical term
11:26:20 From johnnyfromcanada : Dfinity is establishing an Internet Computer, which should eliminate many of such problems, at least from a compute & storage perspective.
11:26:34 From Marc Davis : Language question: doesn’t “user sovereignty” still frame the problem in terms that privilege the system vs. the person? Framing “persons” as “users” seems to imply a power hierarchy that is not truly “sovereign” for persons. So @DavidHuseby, why are you using the term “user sovereignty” rather than “self sovereignty”?
11:26:50 From johnnyfromcanada : https://dfinity.org
11:27:15 From dsearls : Hm: https://dfinity.org/ Very interesting. hadn't seen that before. thanks.
11:27:36 From johnnyfromcanada : Very serious project
11:28:18 From dsearls : I've never liked "user," though I've always liked "sovereignty" when used with "self." Because that's what each of us are experiencing here, as we talk, and walk, and interact.
11:29:17 From johnnyfromcanada : So “user” is a wrapper of “self”.
11:29:22 From johnnyfromcanada : Or decorator.
11:29:30 From dsearls : Agree johnny.
11:30:06 From johnnyfromcanada : Fits with Dependency Inversion / Injection concept.
11:30:12 From Cam Geer : +1 Tim org or System perspective
11:30:38 From Marc Davis : “Self Sovereignty” assumes the “person” as having rights that exist outside of, and prior to, any particular system.
11:31:04 From MarkL. @smartopian : Its about who controls the data
11:31:05 From dsearls : We are all self-sovereign as independent beings. When we enter a system as a self-sovereign individual, we wear the definition of "user." I get that but I still don't like it. Computing and drugs are the only fields that call people "users."

11:31:23 From dsearls : Agree Marc.
11:31:26 From scottmace : Doc +1
11:31:35 From johnnyfromcanada : Actors
11:31:43 From johnnyfromcanada : Participants
11:32:15 From dsearls : Note that the group here has grown to 43. Peaked at 78 in the last session. Both strong.
11:32:15 From MarkL. @smartopian : I have challenged the use of the word User at IIW for over a decade - glad to see the User vs Human discussion happen now - self sovereign is a bit of red herring
11:32:53 From Marc Davis : That's why "self sovereignity" is a key concept, because it postulates a "person" as having sovereign rights that exist prior to and outside of being a "user" of any particular "system". IMHO, this is a key framing issue.
11:33:38 From Timothy Ruff : @Doc, makes sense about "user", and some orgs will have an allergic reaction to the word "sovereign." I spoke with Dave about alternatives, something that conveys a balance of power between orgs and people that's mutually beneficial. Maybe there's a "balance of power pledge" that orgs can publicly agree to...
11:34:00 From dsearls : Self-sovereign comes from Devon Loffreto, who coined it a decade ago and walked off. He still cares but isn't involved. He was contrasting the ideal from the purely administrative. Any system that has an identifier for you in their namespace is administrative.
11:34:39 From dsearls : Hmm... maybe the opposite of distributed is administrative. Just thinking out loud.
11:34:54 From Grace Rachmany : That is accurate. At Holochain we are considering that data needs to be held in 20 hosts in order for it to be fully accessible at any time.
11:35:24 From Grace Rachmany : Also, there isn't really a need for everyone to be online for any give amount of time. People could be off for days or months and get updated when they come back up online.
11:35:46 From Marc Davis : Helpful to think about legal concept of the "person" which can apply to human beings and to corporations/organizations. So perhaps "personal sovereignty" could bridge the gap between humans and corporations each having respective rights and duties.
11:35:59 From dsearls : Agree,Timothy, that some are allergic to "sovereign." But the baby got named. I remember the mainframe world disliking "personal computing," back in the late '70s. it wasn't until IBM made a PC in 1982 that "personal" got legitimized.
11:36:38 From johnnyfromcanada : Perhaps we should distinguish between "coherence" and "cohesion"
11:37:39 From MarkL. @smartopian : Its litterally self surveillance identity - an this title is something that I think I could trust.. because its transprent. But mis-labelling identity as Soverign in my opinion decreases trustworthiness -
11:38:01 From Grace Rachmany : Stributed?
11:38:06 From Grace Rachmany : Tributed?
11:38:15 From Timothy Ruff : Great points, Doc. Nothing beats hindsight, where wisdom comes from. Sovereign it is! Now what's the replacement for "user"?
11:38:44 From MarkL. @smartopian : Human :-)
11:39:02 From David Huseby : +1
11:39:08 From dsearls : Person.
11:39:26 From Timothy Ruff : @MarkL I agree that "sovereign" is inaccurate in many ways, but as Doc says, "the baby got named." Funny, I've got a blog mostly written about how SSI isn't identity and mostly isn't sovereign. :)
11:39:46 From Line Kofoed : Communal?
11:39:49 From Cam Geer : please add that tot he chat
11:40:34 From Riaz Zolfonoon : Could we say Consolidated as opposite of Distributed?
11:41:34 From dsearls : Riaz, what Sam said was helpful, but I don't remember it well enough to write down. So hopefully he can point to it here or somewhere.

11:44:49 From Iain Henderson : On terminology, the MyData Community has stabilised on 'human-centric', and 'individual' and those seem to be being well received across that global community. So there must be decent non-English language equivalents.
11:45:08 From Marc Davis : Who made the great distinction just prior on the Zoom call that centralization is about control and distribution is about space? Great distinction! It separates "degree of centralization" and "degree of distribution" into different layers of the architecture: degree of distribution is a physical layer of the location of physical system resources; degree of centralization is a rights/policies layer about control of data and lower level system resources? Did I get that right?
11:45:28 From johnnyfromcanada : Coherence is more about lower-level structural integrity and coupling / dependencies. Cohesion is more about high-level semantic meaning / understandability.
11:45:47 From MarkL. @smartopian : Working on human trust and transparency is a bit more difficult when SSI claims to do trust -when it really does assurance. — The Consent Record and Notice an Consent standards are external - and meant for human and sovereign type of interaction - Identity s a digital tool — that is used to surviel an attribute- SSI refers to identity Surveillance tech.. —
11:46:22 From Grace Rachmany : I'll be diving deeper into IPFS over the next month. For now, I can talk about how Holochain is dealing with these issues. Hosting is the one area where decentralization is most difficult for regulagory reasons.
11:46:35 From MarkL. @smartopian : Offline by default :-)
11:48:02 From Sam-Smith : See text file for definition of decentralization vs distribution. Control vs Space
11:52:22 From MarkL. @smartopian : Distributed ledger consent tech for storing fwd..
11:53:00 From Chris Winczewski : Sam, does Mobile IP also require full IPv6 implementation?
11:54:41 From dsearls : I like that: "The most easy to use software ever invented."
11:54:55 From scottmace : +1
11:54:59 From Dee Platero : +1
11:55:11 From Cam Geer : awesome Dave! thx
11:55:17 From Jsearls : new physics
11:55:47 From dsearls : I have a season at 3:30 in D to carry this forward.
11:55:53 From johnnyfromcanada : Re: earlier concept of how many nodes are needed to keep a coherent network. Related concept of Byzantine Fault Tolerance (BFT). There is an old math proof that says you need to be resilient at minimum against 1/3 of nodes being "corrupted" / inconsistent (intentional or otherwise).
11:55:54 From MarkL. @smartopian : Please share slides —
11:56:03 From dsearls : True Self-Sovereignty: What Will It Take?
11:56:50 From Grace Rachmany : One of the things that is notable is that it may be necessary to move off of the existing Internet infrastructure altogether.
11:57:22 From johnnyfromcanada : I recall an Internet 2
11:57:39 From scottmace : Which was mostly fat pipes, IIRC
11:57:57 From mitfik : where is the code ? :)
11:58:21 From dsearls : Sam Curran's Minimum Positive Human Application of SSI is at the same time. A difference might be that my focus won't just be on SSI. Just SS. I'm hoping developer types can make it.
11:59:16 From johnnyfromcanada : The alternative to replacing the Internet is to leverage it such that it cannot corrupt what you are intend. Basically, what DLTs attempt to do, with varying success / correctness.
11:59:26 From Grace Rachmany : +1
11:59:29 From Cam Geer : https://scuttlebutt.nz/
12:00:33 From Cam Geer : https://en.wikipedia.org/wiki/Secure_Scuttlebutt
12:02:15 From MarkL. @smartopian : Event receipts
12:02:40 From MarkL. @smartopian : Consent State Records

12:05:06 From johnnyfromcanada : Hashgraph inventor Leemon Baird is big on concept “share worlds”.
12:05:13 From scottmace : Great session!
12:05:18 From johnnyfromcanada : “shared"
12:05:20 From MarkL. @smartopian : Great !!
12:05:27 From Dee Platero : Fantastic! This has been awesome - I can't wait to start developing.
12:05:35 From Iain Henderson : Great session thanks

TxAuth And XYZ (and Maybe Someday OAuth 3)

Session: 10G
Convener: Justin Richer
Notes-taker(s): Josh Verbarg & George Fletcher

Tags for the session - technology discussed/ideas considered:
Authorization, Identification, https://oauth.xyz

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Started with… Justin thinking about “What’s wrong with OAuth?”
oauth.xyz - not a standard.

Talk given at Identiverse. What’s wrong with OAuth2 https://www.youtube.com/watch?v=OLwz7pIXOWQ

Blog post on that talk: https://medium.com/@justinsecurity/moving-on-from-oauth-2-629a00133ade

Simplify / Synergize OAuth, OpenID Connect, UMA and other related specs

Goal to simplify the protocol (see http://oauth.xyz for more details):

- Always start at the Authorization server
- Single endpoint (at the Authorization Server) and logically “defines” the Authorization Server.

Discussing the page: https://oauth.xyz/transactionrequest/
Request multiple access tokens simultaneously.

Should a request have the ability to mark a resource as required. Justin argues no. Reference to FHIR data elements

No Client ID, Client asserts identity via many different key methods.
-- Client ID’s replaced by a “key handle”
-- static registration still supported (obtain the key handle out-of-band)

Supports an Anonymous/Dynamic client making a request to an AS.
Request by Tom to explore different AS. AS on a persons phone vs cloud, for example.

Interact element
-- support per request callback url
-- supports multiple interactions at once.

User element
-- just the handle, or full user id_token

Discussing https://oauth.xyz/interaction/
The interaction allows OAuth and UMA to be combined in one request

Zoom Chat Log:

13:07:19 From Justin Richer : https://oauth.xyz/
13:07:52 From timcappalli : Probably the fix for the SMB path issue :)
13:12:56 From Jan Taylor : Can you link that blog post?
13:14:17 From Ryo Kajiwara : https://medium.com/@justinsecurity/moving-on-from-oauth-2-629a00133ade
13:14:30 From Jan Taylor : Thanks @Ryo
13:15:25 From Josh Verbarg (State Farm) : https://www.youtube.com/watch?v=OLwz7pIXOWQ
13:25:46 From Jan Taylor : That was the question I had. Good question and good answer.
13:31:05 From Alan Karp : Won't returning a subset of the requested permissions encourage clients to request a lot that they don't really need?
13:36:24 From George Fletcher : Alan - I'm not sure it matters... if the system supports multiple permissions, then this problem exists. Whether it's all or nothing doesn't matter. In fact, I'd argue that an all or nothing choice for the user will cause the user to consent to giving up more permissions than they would if they had granularity over which permissions were granted.
13:38:51 From Alan Karp : I agree what you say about users. I was thinking more about an UMA-type situation where the user's policy is managed by the AS.
13:47:29 From Tom Jones : wrt Justin's proposal on TXAUTH to HEART - i note one missing element - specifically how does the requesting site tell the sending site what data they want in a manner that permits the user to accept or request the request. I do not believe that a list of FHIR data elements is something that the user could evaluate. If we want to put the user in control, we must provide the user a choice that they can understand. I can share the Kantara doc on patient choice if that is desired. TXAuth does not currently do that, but could be adapted to do it.
13:53:10 From Tom Jones : I love the idea of a id for the client that is separate from the redirect URL
13:53:34 From Kyle Den Hartog : @Tom, I've thought about doing that for awhile now in a few different contexts, one being in the SSI space. The problem that it almost always comes back to is how to handle the dynamic nature of the IP address when operating on a mobile phone. There's some exploratory ways I've thought of using DIDs with a service endpoint that points at a domain that points at a dynamic dns resolver which mobile doesn't have great support for. In particular, it usually requires mobile networks to be configured in a particular way to make the dynamic dns resolution work properly, which the user doesn't have the ability to configure.
13:54:17 From Tom Jones : I presented a solution at session 9 today
13:54:32 From Kyle Den Hartog : I didn't see that. Would love to see that.
13:55:19 From Kyle Den Hartog : Are there links in the notes that I can look at?
13:55:19 From Vineet Banga : @Tom, to your point about user consent…the resource json does allow you to add label…which can be used for consent? Right?
13:55:55 From Tom Jones : Don't know how to parse that statement
13:56:47 From Tom Jones : @ Kyle http://tomjones.us/Home/Solutions
13:58:24 From Tom Jones : Another good idea from Juston - a single transmission with all the data
14:00:32 From Kyle Den Hartog : Thanks I'll take a look at that link

14:08:15 From Josh Verbarg (State Farm) : NodeJS - JavaScript running on a server
14:08:37 From Jan Taylor : NodeJS is a V8 JavaScript Server
14:12:35 From Terry Hayes : The QR goes to example.com!
14:14:22 From Tom Jones : Not worse is not sufficient
14:16:23 From Jan Taylor : Thanks Justin, great session.
14:17:12 From Kyle Den Hartog : Thanks Justin this was great to learn more

Deepfakes & Identity: Problems, Solutions, Focus on Technology

Session: 10H
Convener: Kathryn Harrison
Notes-taker(s): Sankarashan

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Evolution of the work presented at the last IIW - 6 months of work and research since then

Deepfakes as got a lot of attention but it is part of a much broader umbrella of disinformation. 96% of deepfakes are deepfakes porn (largely celebrities)

Categories of information

1. information which is false → misinformation (information which is incorrect, out of date, context)
2. True information but used to harm → malinformation (doxxing)

Disinformation exists in the intersection of the above. Is disinformation propaganda - Yes, generally. Depends on the content of the propaganda (but can exist in either category). Disinformation is one technique in a broader set of PsyOps. In modern information age era - disinformation is targeted to everyone (eg. deepfakes, bot attacks etc)

Cheapfakes (eg. Nancy Pelosi video : photo editing, miscontextualizing)
Deepfakes - generative adversarial networks (GAN) - uses AI [Generator | Discriminator]
Whose images are being used? Is there consent? ← first set of issues around identity as they arise

Lipsync video; deepfake audio ; real time re-enactment

1. Liar's dividend - that this technology exists - it is easy for anyone to introduce doubt in an image/message. Creates a fundamental doubt around trust - what is real/not real
2. Market manipulation via fake tweet (S&P movement of 26%). Other examples being French transport companies
3. Social engineering - whole new set of technical tools
4. Extortion and Harassment - case of Rana Ayyub (deepfake porn circulated extensively on social media)

Coalition of stakeholders across aspects needed to address the challenges

- Technology & Policy
- Education - attention economy and deficit causing unaware nature of impact (cognitive laziness). COVID-19 has been an exceptional test bed - large data gaps causing a lot of interest in addressing that

How do you create a vetting method? Consider the lifecycle of information:

Maker → Creation → Distribution → Believability → Impact
To what extent is identity tied to the production/creation of content?

Algorithmic propaganda = mass scale of distribution (technology and policy intervention to gate)

Believability - (1) confirmation bias (2) cognitive laziness.

'**One Single Solution**' does not exist. Rather an integration approach is expected to work. Detection techniques help identify what is fake. How do you verify the authenticity of a content? How do you help a much broader audience understand what is happening in the space?

Watermark/DID into specific images would allow tracking the images under review for authenticity. Would where it has been detected (uses cases of weaponized media) and similar point of information be recorded? "information virus vectors"

- identifying bots/non-humans
- identify what humans are being targeted through (what kind of data around the targets would need to be recorded) this deepfake

levels of combating information operations

- technology platforms and technology developers
- individuals
- society (herd/mass effect) - digital interventions/digital "de|re-programming"

Reverse image search is one technique that can help identify whether images are fakes.

"Digital integrity" - as an output result of the image under review.
Manual process → automated flows to make workflows such as KYC etc to be more efficient.
What are the possible next actions from the deduction?

As a group the potential areas of collaboration

- standardization of explanations (taxonomy, Digital Harms Dictionary)
- designing a common understanding of what the solutions and interventions would look like
- marketplace for forensic capabilities into commercial applications

Cross platform incident reporting and log (3rd party auditing) - questions around access and roles would need to be worked out

Casenet - Missouri : traction - well vetted repository of facts through jurisprudence

“false hope” - Self reporting at companies that do not often get taken care of. The tool could mitigate that if the reporting does go to the companies to encourage action to be taken.
Work being undertaken to understand the methods on which the inference can be translated into action - the scale and systematic process needs the right set of stakeholders. Privacy and usage policy would need to be strengthened as well. Working on items that could break the law providing guidance on how the reporter could report those that CAN take action. Connecting legal services to local law enforcement.
citation/reference of josh_emerson (Twitter) for methodology about identification of bots/fake accounts
People sharing information from fake accounts

https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Nina-Kollars-Confessions-of-a-Nespresso-Money-Mule.pdf | https://youtu.be/4fYZpRBuh-s - to be able to intervene and defang prior to the issue becoming an incident

http://stoponlinevaw.com/media/press-release-report-on-stop-digital-voter-suppression/
http://stoponlinevaw.com/media/report-facebook-ads-that-targeted-voters-centered-on-black-american-culture/

Introducing a concept of peer review on analysis and inference being created on content being processed by the system. Or, a “reputation framework”

Measuring an extent of editing and manipulated in the content - giving people tools and capabilities to make decisions on that.

https://github.com/alievk/avatarify

What datasets are available for training? (as an anecdote - https://thispersondoesnotexist.com/ did not lead to an image of (woman of color) PoC - more diversity is needed)

Creating A Knowledge Product For The Community – What Do You Want/Need Information-wise You Don’t Get/Takes Too Much Time? What Will You Pay?

Session: 11A
Convener: Kaliya Young & Infominer
Notes-taker(s): Kaliya Young

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The purpose was to consider the possibility of developing a knowledge product for the community.
We imagined attracting the overwhelmed to talk about what type of product they might want. We attracted the already connected and collectors of information. So there were several interesting outcomes.

The collectors and trackers of the industry are thinking about convening on a regular basis to share what we are seeing/sensing in the industry. If you are actively tracking the industry and wish to connect with other

synthesizers doing the same please reach out to Kaliya to get connected to this group. kaliya@identitywoman.net

If you would like to share your knowledge needs and what would be useful to you in a knowledge product feel you can fill out this google form Kaliya put together.
https://docs.google.com/forms/d/e/1FAIpQLSdiyYY7e_5VUpdZQ_aHoDDXmpfeAPVcdLrLI2lV1L02D14RDQ/viewform?usp=sf_link

Who came to the session and why:
Specialist in SSI - bigger project in JC
Neither part of DIF, W3C or Hyperledger <- most of the work is being done there. I think it would be great if there was more information easily accessible - i grapple with coming to a good understanding - SSI architecture stack whom to talk to.

There is a big need to put information together and curate. Big divide - knowledge and newsletters. most of the time very technical - most who is not in the community to really understand what we are doing. It is a big challenge and adoption barrier. Need information source accessible in different channels.

Jonas - Boston Consulting group looking for more than a year into the space. It is quite difficult to grasp the pace - benefit - what kind of companies working in the space - where is momentum. what are the use-cases that are proven. State of SSI.

Infominer sharing his interest in the space.
https://decentralized-id.com/
Pete from Utah - Medici Ventures - investing in area and developing his own product.
Government as a service - SSI is very important.
Looking for new opportunities - applications we could create and what we should be building into our applications.
DIF is a starting point. When I look at things and try to get into a new aspect.
IndyAries RFCS.
GitHub repos <- 60 companies
Markus' Awesome page was a starting point. <Kyle when wrote research page.
https://github.com/peacekeeper/blockchain-identity

Standards have feeds.
Adrian (SSI Ambasador)
Newsletter - basically - sign up for SSI newsletters - good and a lot of them.
LinkedIN - all my connections are SSI and blockchain
NewsAggregation tool.
Medium Blogs 40-50
Google Alerts.

Some ideas about what might be valuable.
check what is "real" and what is not real.
A lot of companies - claim it is SSI but it is NOT.
Huge struggle….with Blockchain space - but nothing happened.
Create this news - source that is used for a credible reference.
Editorial - could be powerful for the space.

Same subscription model into who is moving which standards
what is happening within the working gorups in that format
what is the short summary
translation to marketing/biz def.

If you want to share what you would find valuable if you are reading these notes please fill in this form.

https://docs.google.com/forms/d/e/1FAIpQLSdiyYY7e_5VUpdZQ_aHoDDXmpfeAPVcdLrLI2lV1L02D14RDQ/viewform?usp=sf_link

DPoP Introduction & Current Developments

Session: 11B
Convener: Daniel Fett & David Waite
Notes-taker(s): Daniel Fett & Mike Jones

Tags for the session - technology discussed/ideas considered:
OAuth, Proof of Possession, POP, IETF, Banana

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

1. **Links provided by Daniel Fett:**
   https://tools.ietf.org/html/draft-fett-oauth-dpop-04
   https://tools.ietf.org/html/rfc8705

2. **Notes provided by Mike Jones:**
   Daniel Fett and David Waite (DW) hosted a great session on OAuth 2.0 Demonstration of Proof-of-Possession at the Application Layer (DPoP) at the virtualized IIW this week. Attendees also included Vittorio Bertocci, Justin Richer, Dmitri Zagidulin, and Tim Cappalli.
   After Daniel and DW finished doing their overview of DPoP, I used some of the time to discuss feedback on DPoP from Microsoft Azure Active Directory (AAD) engineers. We discussed:

   - **How do we know if the resource server supports DPoP?** One suggestion was to use a 401 WWW-Authenticate response from the RS. We learned at IIW that some are already doing this. People opposed trying to do Resource Metadata for this purpose alone. However, they were supportive of defining AS Metadata to declare support for DPoP and Registration Metadata to declare support for DPoP. This might declare the supported token_type values.
   - **How do we know what DPoP signing algorithms are supported?** This could be done via AS Metadata and possibly Registration Metadata. People were also in favor of having a default algorithm – probably ES256. Knowing this is important to preventing downgrade attacks.

- **Can we have server nonces?** A server nonce is a value provided by the server (RS or AS) to be signed as part of the PoP proof. People agreed that having a server nonce would add additional security. It turns out that Dmitri is already doing this, providing the nonce as a WWW-Authenticate challenge value.
- **Difficulties with jti at scale.** Trying to prevent replay with jti is problematic for large-scale deployments. Doing duplicate detection across replicas requires ACID consistency, which is too expensive to be cost-effective. Instead, large-scale implementations often use short timeouts to limit replay, rather performing reliable duplicate detection.
- **Is the DPoP signature really needed when requesting a bound token?** It seems like the worst that could happen would be to create a token bound to a key you don't control, which you couldn't use. Daniel expressed concern about this enabling substitution attacks.
- **It seems like the spec requires the same token_type for both access tokens and refresh tokens.** Whereas it would be useful to be able to have DPoP refresh tokens and Bearer access tokens as a transition step. Justin pointed out that the OAuth 2 protocol only has one token_type value – not separate ones for the refresh token and access token. People agreed that this deserves consideration.
- **Symmetric keys are significantly more efficient than asymmetric keys.** In discussions between John Bradley, Brian Campbell, and Mike Jones at IETF 106, John worked out how to deliver the symmetric key to the Token Endpoint without an extra round trip, however it would likely be more complicated to deliver it to the resource without an extra round trip. At past IETFs, both Amazon and Okta have also advocated for symmetric key support.
- **What are the problems resulting from PoP key reuse?** The spec assumes that a client will use the same PoP key for singing multiple token requests, both for access token and refresh token requests. Is this a security issue? Daniel responded that key reuse is typically only a problem when the same key is used for different algorithms or in different application contexts, when this reuse enables substitution attacks. It's also the case that clients can choose to use different PoP keys whenever they choose to.
- **Could access tokens be signed?** Having the DPoP key hash in the access token is equivalent if the access token is integrity protected. But people said that many deployments don't use structured access tokens in which the key hash can be included. For instance, Ping Identity uses access tokens that are just database indexes. Would access token signing be needed then?
- **Why aren't query parameters signed?** Daniel said that canonicalization of query parameters that use different URL escape syntaxes for representations of the same characters would likely result in interop problems. People said that while SOAP deployments might have many logical endpoints differentiated only by query parameters, that's no longer the normal pattern for REST systems.

Thanks for the great discussion!

Sovrin Update

Session: 11C
Convener: Joyce Searls & Andre Kudra
Notes-taker(s): Bruce Conrad

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Phil spoke of the mission of the Sovrin Foundation: "Identity for All". Not only an identity metasystem that works for the organizations that created it, but for everyone. Open source code development, open protocols, governance, a network where credential exchange can happen.
https://www.windley.com/archives/2018/07/the_sovrin_foundation.shtml

A system upon which you build identity systems. E.g. the BC government has built an identity system for constituents in the province to provide safe entry.

https://www.windley.com/archives/2020/02/building_identity_systems_on_the__sovrin_network.shtml

https://vonx.io/safeentry/

Andre says Sovrin Foundation has been around for three or four years now. Done well in terms of community involvement and support of open source software. There are over 70stewards, including the main net supporting business use cases throughout the world, relying on it on a daily basis. One of the first real-life SSI systems in the world.

Sovrin Foundation homepage: http://www.sovrin.org/
Sovrin Governance Framework home page: https://sovrin.org/governance-framework/

A few weeks ago the Sovrin Foundation moved to a volunteer-led organization. Joyce and I are managing the transition period. Main net continues to remain stable through the transition period and there are no signs that that will change in the near future.

<insert here the work group descriptions>

The core takeaway: rest assured that we are making it work on a continuing basis, and main net will continue to operate.

Joyce asked Drummond to talk about details on the transition, the foundation that has been laid for the next phase.

Drummond Reed invited questions about what was just covered, foundation history, main net, etc. Showing a slide show entitled "Trust over IP Foundation: Driving global adoption." <insert link to slides here>
Brian Behlendorf, the Executive Director of Hyperledger, a part of the Linux Foundation (LF), gave some historical notes. Making sure the code is open source, and that the companies which contribute can be successful. There are now 15 projects in Hyperledger, with more in the lab.

Drummond says Linux Foundation provides a natural home for ToIP Foundation. Its goal is to provide a reference architecture for technology and for governance. He explained the stack; governance stack on the left, technology on the right.

Layer one, public utilities, is a place where DIDs and associated keys are available for all the higher levels to use. Sovrin is the first one of these built for this purpose. It has a DID method (did:sov:) and can resolve the DID into a DID Document containing all needed information. Other networks also have DID methods and fit into this layer. Hyperledger Indy is the first implementation for the Sovrin network.

Layer two, trusted peer to peer communication. End points can be people, organizations, or even things (IoT). Any two devices can connect. Each layer has a corresponding governance frameworks.

Layer three, trusted exchanges. We move from cryptographic trust to human trust. Verifiable credentials are issued by one participant, held by a second, and used by a third party to verify things as needed. E.g. a person might hold credentials that they are an essential worker, have immunity, etc.

Layer four, trusted services. E.g. worldwide Covid-19 service, government systems, etc. <add more examples>

Working groups: Steering committee. Foundry working groups: ecosystem and utility (for layers 4 and 1) to provide help and guidance to projects in their area. <missing the other two WG>

LF created a new branch for a legal framework for open governance efforts.

Back to Joyce. This was background for the transition team. There is a substantial place for main net to land, with a very robust forward path.

Question from Andre, is the LF a comfortable place?

Ben Weaver question, “How does moving to the LF solve financial problems?” The stabilization work stream deals with this, and administrative help available through the LF, sharing costs. Andre says they are determining the *minimum viable foundation*, working with stewards and endorsers, monitoring the network. These will move forward at their own time and pace.

Brian gives a LF perspective. Likes the term minimal viable foundation. You can always grow later. Answer the question, what is absolutely necessary to fund. The project needs to come up with a budget, and funding comes typically from membership fees (corporate members). E.g. profits from running events, donations. What are the benefits offered to members? E.g. a badge/logo on a home page. Members become part of a financial or budgeting committee. Will it be funded by stewards, or by large or small companies. Another option is fee for services. Hopefully reads remain free, but we’re used to paying to register (e.g. DNS). LF is not a charity foundation, and those running under its umbrella must be financially solvent.

Nicky Hickman shares a document <insert link here>:

1. Maintain a strong, stable MainNet (and others StagingNet and BuilderNet,
2. Establish a global SSI ecosystem and network of networks
3. Advance Identity for All and SSI as a basic universal service (in the manner of telco’s)
4. Repay the debts of the current Sovrin Foundation
5. Have a roadmap for launching the Sovrin token

Nicky enlarged on point 3, e.g. making sure that no one is excluded for any reason. Governments and big service providers have to step up to provide universal identity services and a functional digital identity as a basic human right.

Drummond says in chat, “Universal Basic SSI Service is IMHO an amazing concept—underscores “identity as a human right. The idea that SSI could be available to all people just like electricity and telephone service is revolutionary but also makes perfect sense. And Nicky’s insight that we can have it fit into the existing regulatory infrastructure for Universal Service is brilliant.”

Phil Windley spoke about obligations already implied regarding tokens. There is an opportunity to package this up, and to support business needs as they arise. Letting the community move this forward as the need to for purposes they have. Support the diversity of opinions.

pknowles points out that SSI is still in its fledgling stage. This should change dramatically over the next few years. As large industries begin to leverage SSI, the token could emerge naturally.

Kendra asked for clarification. Will there still be a Sovrin Foundation, and also the ToIP Foundation. How will this be organized going forward. Joyce says a large part of the work will likely move over to Linux Foundation or others. Still trying to figure out which parts go where.

Drummond says ToIP is defining the governance stack, giving templates, models and best practices that the Sovrin Foundation can use, and gave detailed examples at various points in the stack. He gave examples, including “findy” for the country of Finland.

Sovrin will do a town hall meeting towards the end of the day tomorrow so the decisions can be more “decentralized.”

Are VCs A Necessary Hurdle On The Path To DID Adoption?

Session: 11D
Convener: Adrian Gropper
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Background techy info from Tuesday's session 1D :https://bit.ly/IIW-SSI-Adoption

JH - Service Endpoint
MS - Provider vs. Patient same Identity?
PA - DID WG - VC maybe w/o DID
DC - Learn about separation / credentialing products
EF - avoid schema rigidity
JH - newbie
KK - workday product manager
OS - VC without DID - works on sidetree

Path A - SDS - Secure Data Store - Service endpoint to data store in DID

- a pipe between an identifier and an attribute
- where to get the info
- like an Info Endpoint in OpenID Connect

Path B - Service Endpoint to Authorization Server in DID

- Separation of Concerns

- DIDs don't have a business model so people bundle VC added value for business reasons
- AS first already has adoption /
- TxAuth as a new OAuth3 model for the DID service endpoint
- Gov wants a process to hold verifiers accountable
- Platforms don't benefit from a separation of concerns AS vs RS
- Issuer-held credential and signed credential
- VC not efficient for pharma or surveillance

Relevant paper:
https://blog.petrieflom.law.harvard.edu/2020/04/29/covid19-privacy-surveillance-community-organizations/

Saved Chat
15:48:21 From Orie Steele : Everything needs a business model, or it dies for lack of reproduction.
16:46:37 From Adrian Gropper : https://blog.petrieflom.law.harvard.edu/2020/04/29/covid19-privacy-surveillance-community-organizations/
16:49:19 From Adrian Gropper : https://bit.ly/Trustee-Summary

Search Warrants and Smart Devices: Encryption, Privacy & The Crypto Wars

Session: 11E
Convener: Dan DuBeau & Alex Rosen
Notes-taker(s): Dan DuBeau

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link from Dan DuBeau for slides provided at the session:
https://barlea.org/wp-content/uploads/2020/05/IIW-Exceptional-Access-20200509.pdf

Summary:
The current methods of exceptional access are untenable. Solutions such as back doors and key escrow create more problems than they solve, and there is a flourishing gray market for hacking smart devices. There are approximately 500,000 to one million exceptional access requests each year, yet there is no standard for whose data is accessed, under what conditions, and how much of the data—no standards for governments, no standards for manufacturers. We propose a method of exceptional access that ensures 100% transparency, as well as a consortium of manufacturers, privacy and advocacy organizations, and law enforcement agencies to ensure complete global transparency is assured.

Is Consent Broken? If Yes, What Can We Do?

Session: 11F
Convener: Clare Nelson
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to slide deck provided by Clare Nelson:
https://docs.google.com/presentation/d/1Ap91gHeXLdKwZkIUbbsJnU_v2RyWmCT5MowfIsVTSCE/edit?usp=sharing

Session Description: Is consent broken? If yes, what can we do? See the slides with the MORE titles for input from the group.
Consent means different things, and can be used in different ways.

Fred Cate – 2020 TED talk on Data Privacy and Consent. Has identified 7 issues with consent, along with suggestions

Daniel Solove – the privacy paradox myth, the difference between reported preferences and actions taken
Shoshana Zuboff – the age of surveillance capitalism. Data about individuals is the raw material that is used for digital advertising
Two kinds of privacy law – private vs. government.

7 reasons why consent is broken:

- Complexity of notices, and nesting
- Notices are long and dense
- Consent is ineffective since it is hard to understand
- Consent is illusory – contracts of adhesion, binary take it or leave it
- Burden is on the individual, liability is shifted from the data processor
- Consent choices are often a disservice to the consumer
- Leads to lousy consumer protection

Privacy laws are spreading, and thus conversations about consent

CCPA has the broadest definition of personal data – includes the notion of probabilistic identifiers such as cross-device tracking, device fingerprinting and digital exhaust

Myth of anonymization – de-identified data can be re-identified fairly easily

Marketing and advertising are finding new ways to track and identify specific individuals as techniques such as cookies fall under new privacy laws. E.g. Merkle Wallet

Data brokers can provide "hyper-personalization" to predict behavior. They create identity graphs that can include 10k+ attributes.

Data privacy laws are not necessarily covering all of this.

What can we do?

- Make stewardship of data the responsibility of companies/data handlers
- Create regulations that make data handlers/processors act in trust
- Provide redress
- Making giving consent meaningful, timely, and effective

Me2B project
Project VRM – Doc Searls

Addition to the 7 reasons – volume, number of times we interact digitally
Consent should not used as a form of protection – overarching protection
Legitimate purpose for collection

IndieBox – personal cloud server
CloudYoult
*There may be an incentive for data handlers/processors to stand up technology services to allow for personal data storage/choice schemas to remove their own liability

Concept of data trusts – board of trustees with fiduciary responsibilities. Mozilla
Kantara ISI: consent receipts – machine readable receipts for consent

-have published consent receipt 1.1
-they are fairly far along with defining the next step

Consent tagging and tracing (open receipts, a subset of open notifications) – ideally we can understand the conditions under which consent was given

Consent is a personal decision about a tradeoff, for what services am I willing to give what data

- Can individuals truly make these decisions? They don't have full information, very context specific
- But who can make these kinds of decisions on behalf of individuals?

First we need a common vocabulary for data – DPV (data protection vocabulary)

Need something where users can express their preferences and then that can map to legal terms and actions
Harvard – policy enforcement as data moves through a workflow

The idea of consent in terms of boilerplate legality is bad. The highest rendition of consent is the file upload dialogue box. Embodied consent – as an act of your body, you tactically are giving consent.

Privacy chain – idea is to control this vast network of machines. Need a control channel to demonstrate and track where data flows across the value chain.

Zuboff is a bit inflammatory - have been talking about it since David Packard
Jean Twenge – Filter bubble
Information snacking; mental health effects

Communication/vocabulary - triangle between legal, consumer friendly, and machine readable

The conversational nature of privacy policies is a joke – they try to make it so easy to understand, but they are still not read

Need to validate things – go through testing between regulators, and consumers
You need an advocate – COVID is bringing that up. Many individuals need interpreters, guides through much of this.

Differential privacy – has been shown to prevent leakage. Can it be applied in the advertising pipeline.

Music/entertainment industry viewpoint – limited use rights

BBS + JSON-LD ZKPs and Aries & Indy. Your Thoughts?

Session: 11G
Convener: Stephen Curran & Andrew Whitehead
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slides to trigger the discussion: http://bitly.com/BBSPlusIA

Recording of the sessions: Link

Tracking Identity On The Supply Chain: Curated Tour Of The Report

Session: 11H
Convener: Heather Vescent
Notes-taker(s): Heather Vescent

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Links provided by Heather Vescent:

During this session, I went through this deck: Sensors, Identifiers & Digital Twins: Tracking Identity on the Supply Chain

https://www.slideshare.net/heathervescent/sensors-identifiers-digital-twins-tracking-identity-on-the-supply-chain

You can download the report discussed here: https://bit.ly/GSCreport

Spotting Economic Opportunity In An SSI World (3/3)

Session: 11I
Convener: Dave Huseby
Notes-taker(s): Scott Mace

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to slide deck of presentation, provided by Dave Huseby:
https://docs.google.com/presentation/d/1uljRTBy8HqGSd8sfxUxMF1oAFswxzHYVsHu0AlPjc9s/edit?usp=sharing

Nine problems of distributed systems

Discovery
Introduction
Coherence
Public Service
Trust
Privacy
Coordination
Membership
Persistent State

SSI can solve introduction, somewhat trust & privacy by combining with blockchains for the persistent state.

Spotting economic opportunity, where some of the nine problems are not solved.

Adhere to the principles of user sovereignty. Offer paid edge services that do not violate user's trust.

My first victim today, how this model is applied to existing distributed systems and how they create economy opportunity.

Linus Torvalds relied on external systems like email to build Git. How do i find another developer to collaborate with? Failed to solve discovery. Introduction, no built-in PKI infrastructure. where I started the DID-GIT project for built-in PKI in a Git repo. Git relied on external solutions. Coherence, how do I reconnect in Git to submit my patches? They didn't solve that either. The original design was to email patches. A royal PIA. Membership, no obvious way to do this in Git. Automatic governance is possible but not in Git out of the box. Coordination, Git is about tracking changes to files. Doesn't have the other necessary doing collaboration for software development. GitHub was sold to GibHub for $7.5 billion. You don't want a company like Microsoft owning the revision control for all these open source solutions. Microsoft is starting to take advantage of this. Merging with Azure services. You could just run Windows. Recapture developers as Windows users. Existential threat to Linux Foundation? Wouldn't say it is, but wouldn't say it isn't.

Bitcoin is not decentralized. How can we harden it? Discovery and coherence is lacking. Code has a hard-coded list of IP addresses. Used to be done through IRC, at least more decentralized than IP addresses. Discovery, no mechanism for that. Bitcoin itself does not provide a mechanism. Very little privacy in bitcoin. Can trace. A compromise due to regulation. But wasn't in the bitcoin design. Coordination, no built-in to transmit a secure bitcoin address to a sender. How do I know I'm talking to who I think I'm talking to? Misdirection of funds is a big problem. Authorized push payment fraud, you get the wrong address. Knowing they didn't provide those solutions? Coinbase.com provides a centralized solution, also an easy way to send bitcoins to someone. Market share is big, like 50% of retail investors. Coinbase is bitcoin like AOL was the web back in the 90s in casual users Coinbase is now valued at $8 billion. Friends say this model predicts centralized solutions attacking decentralized tech.

Secure Scuttlebutt is not decentralized. Disc & coherence uses "pubs" at a specific DNS address to discover other users and get updates. That alone right there makes Secure Scuttlebutt subject to corporate capture. Supposed to be a distributed Twitter. Throw in a bit of Patreon, RSS. Build it up until it's a threat to Twitter and sell it to Twitter for a billion dollars. It will happen.

Before I worked at Hyperledger, I worked at Mozilla tasked with looking at surveillance and privacy. Worked a lot with the Tor project. I didn't know why the Web was constantly being recentralized. The Web originally had no discovery mechanism, so the search engine industry was inevitable. Originally no privacy, created the CA system. I want to know when Riley updates her blog, a rare case where the community came together. RSS. But Blogger.com was already making tons of money, launched the Atom protocol, corporate-owned, to have paid subscriptions for bloggers. Atom supports all that. This kind of coherence solution was hampered by RSS vs. Atom. Widespread adoption of RSS was slowed by that fight. RSS almost lost. Also no public service solution, Intermediary solutions like Blogger.com. And no persistent state. Money made by databases & middleware as a result.

Maybe dinosaurs need to start making oil. Whatever we do next needs to be designed to resist corporate capture from day one. We need to start from scratch. No way to fix the browser. Too much legacy that can attack our privacy.

Pick an existing legacy system. Say auto maintenance records. How would I get the maintenance records from the mechanic over to the dealer? Now that we know how SSI works, build companies that can exploit these. Make money teaching developers how to solve these problems. That's a great idea for a business. Any questions?

Scott Mace: Content payment problem.

David: The toughest problem. Let's put a pin in that.

Liam McCarty: Trend away from decentralization. Unless transaction costs are extremely low in a decentralized system, maybe we will have this trend toward centralization.

David: Hold PII is more and more risky.

Sam Smith: Transaction costs: triangulation, transfer and trust. Right now, much are hidden costs. A lot of the corporate takeover systems provide implicit transaction costs. We don't have decentralized trust systems to do trustful transactions. FB & Google have OAuth and a sign in. They take care of all that trust exploit stuff, making sure nobody's hacking their servers. When decentralized systems can solve the trust problem, then we can become competitive to centralized systems in terms of transaction costs.

David: Back to micropayment. One criticism I have of writers, happening in financial writing. You need to give away stuff so people will read more from you, then charge for things that have extra value. For instance, I could have a subscription service. I don't think anybody is going to be paid to tweet and to write an opinion blog. There has to be this asymmetric value.

Scott: Wondered how this could do it?

David: Could do micropayments without incurring too large a transaction cost. That's what Lightning Network is happening.

Robert Mitwicki…: Data monetization is a popular business model. Aggregate & sell data to maniupulate behavior. Would we get rid of those business models? Create a better next version of the Internet or still stuck with old business models?

David: Won't end that business model. Will make it respectful. User aggregation is a concierge servcie. Sign up with edge service that I feed them all the info about it, they become the intermediary. Show me all the Ford Truck deals.

Robert: Do we need to solve all 9 problems, or no matter if we solve them or not?

David: The surveillance economy will be here as long as we haven't solved these problems.

Johnnyfromcanada: FB & Google kill companies arbitrarily when they change their policies. His point, once we build this internet computer, you're coding against one computer. Just the problem you're trying to solve. How we just moved the goalposts. "Definity" in the chat.

David: Metastability, since you're always able to connect to at least one other node, you only need 10-15 nodes in a cluster, you get an island of stability in a world where people are frequently disconnected. Protocol called Last Known Wherabouts. Makes a statistical connection. You could discover the whole network. Even though none of us have a central server anywhere. Blog post by Constantine about a fictitious collaborative tool for software development. He's talking about a fully decentralized solution.

Vic Cooper: Is telecommunications (phone networks) an example of a distributed system?

David: Original system was decentralized. Modern telecomm is IP based with central control. Say I want a radio not tied to a provider. The FCC is about to open up the 6GHz spectrum. A lot of nonintereference rules will allow big commercial providers to squat on public property. A fully decentralized solution would be a ubiquitous fabric. Let's start building our own handsets.

Marc Davis: In a truly user-sovereign data economy, it's not just individuals but collectives that want to counter data aggregators.

Scott: Milton Pedraza is working on third-party representation of the rich to people with whom they want to do business. He was at Monday's Me2B Alliance day.

Sam Smith: You share stuff and they make a legal receipt that says they accepted that data, you can watermark it. They're liable for it. Differential privacy, the inverse is differential watermarking. Run an algorithm on it. Prove they distributed your data set without your permission.

David: That's captured in the informed consent principle, fees into trust & privacy.

Sam: Liability is a stronger word, a weapon against surveillance.

MarkL (smartopian): Trust means assurance, means liability, which is what Sam is talking about. Decentralized has to have this concept it's outside a system. We've been working on that for a long time with notice and consent standards. Notice just made it to ISO last month. Most companies pretend to have consent records, but they actually don't. That's been coming for a long time out of IIW.

David: I appreciate the feedback. This is just a work in progress. I'm the security maven at Hyperledger, plotting our way forward. A lot of navel-gaziong, should we host the code repos? How do we know who has contributed to allow them to vote in our elections? A lot of foundational problems we're looking for better solutions to. Home to a lot of SSI stuff. Brian Behlendorf wants to make a lot of our solutions more robust, private, decentralized, eat our own dog food. Also to predict centralization. It's a useful tool. Appreciate any more thoughts.

Zoom chat from this session follows:

12:30:35 From mitfik : TDA (Trusted DIgital Assistant) is a new browser :)
12:30:47 From rileyhughes : Is this Robert? ^^
12:30:54 From Michael Shea : of course
12:30:55 From mitfik : sure thing :)
12:31:04 From rileyhughes : ðŸ‘‹
12:42:13 From dsearls : Hate to say I'm going to be going in and out of this one.
12:45:56 From Robert Mitwicki *THCF* : They follow unix philosopy

12:47:27 From KathrynHarrison : Is there any way to make the same order of magnitude of profit (as a centralized system) through decentralized systems? Do the incentives exist to solve these problems in a decentralized way (esp when there is so much money to be made the other way)? Sorry to be the capitalist but...
12:48:57 From Robert Mitwicki *THCF* : we don't care much about technologies which are web related as we want to get rid of them ;) Let M$ take them.
12:51:27 From johnnyfromcanada : Dominic Williams (of Dfinity fame) is _very_ opinionated about _eliminating_ the need for centralized cloud platform providers (like Amazon, Microsoft, Google, Facebook), via an Internet Computer (which they are building). https://dfinity.org
12:52:52 From johnnyfromcanada : In the DLT world, Bitcoin is increasingly used as the counter-example to the principles of decentralization.
12:53:10 From KathrynHarrison : Coinbaseâ€™s marketshare is mostly US though. Not nearly as global
12:53:39 From KathrynHarrison : (Which just emphasizes your point)
12:54:09 From KathrynHarrison : So then why are decentralized solutions so frequently built with so many holes??
12:54:25 From Benedikt Olek : I think when dfinity succeeds and becomes very dominant, it potentially starts to threaten users sovereignty. Or other players enter, filling the gaps and becoming this threat - if I follow Davids argument correctly
12:56:37 From rileyhughes : FWIW, Greg Kidd was one of the first investors into Coinbase & blockchain.com. Coinbase uses a custody model and blockchain.com uses a self-custody model. Apparently, they each have similar market share globally
12:57:09 From Liam McCarty : Is it possible that thereâ€™s a â€œCoaseâ€™s theoremâ€ of centralization? Coaseâ€™s theorem says a firm forms when transactions costs are higher in the market than in the firm. Maybe the idea of full decentralization in the cases Davidâ€™s describing is as untenable as everyone in the market being an independent contractor. Thoughts?
12:58:13 From Cam Geer : and search needed a great customer experience â€” simply and effective
12:58:17 From rileyhughes : Just posted a blog post today, BTW :D
12:58:21 From Timothy Ruff : @kathryn: there is one way that top-end revenue potential player can be as large in a decentralized marketplace as it is in centralized marketplaces today: if the market grows significantly (as it did with Uber). Most of that effect is unpredictable, but there is at least one economic predictor: the degree to which transaction costs are reduced. The more efficient a market becomes, the bigger it becomes. With user sovereignty there will be many more players of all sizes, not just one dominant one in each category, because users can so easily move to the latest/greatest, as it should be.
12:59:33 From dsearls : That was Blogger after Google bought it. Ev & friends made no money onBlogger before that. Atom was created to flatten Dave Winer, and RSS won because it supported podcasting.
12:59:42 From johnnyfromcanada : Bitcoin mining is centralized in practice, since expensive mining encourages â€œpoolingâ€, two or three pools of which currently control more than 50% of node work. So not BFT (also no finality).
13:01:32 From Dee Platero : Preach!
13:02:30 From johnnyfromcanada : Maybe we need a new economic model
13:02:41 From dsearls : Amen brother.
13:02:53 From Robert Mitwicki *THCF* : :+1 no way to fix browser !!!
13:03:19 From KathrynHarrison : I think the answer lies in incentives. If people building the initial system could have made more money maybe there wouldnâ€™tâ€™ have been so many holes for corporates to capturre.
13:03:21 From Steve Todd : Web standards are developed by organizations that need centralization to survive.
13:03:39 From KathrynHarrison : Right somebody has to fund those orgs

13:03:44 From Cam Geer : +1 kathryn
13:03:59 From Gabe Cohen : +1 how to change the incentive structure?
13:04:02 From johnnyfromcanada : One possible way to shift the economy is to stop locally optimizing the stock market. See the Long-Term Stock Exchange (LTSE): https://ltse.com
13:06:27 From Cam Geer : https://en.wikipedia.org/wiki/Coase_theorem
13:06:33 From rileyhughes : Kathryn, itâ€™s incentives and speed. I totally agree with you about incentives. The other thing is that open development and standards work is painfully slow. Developing in a closed, centralized environment is super fast.
13:06:52 From johnnyfromcanada : Hedera folks talk a lot about microtransactions being a way to re-monetize industries that have been centralized, including media.
13:06:53 From dsearls : Dave is moving toward a theory of decentralization. At ProjectVRM we have one: free customers are more valuable than captive onesâ€"to themselves, too sellers and to the market. We await proofs in the territory Dave is laying out here.
13:07:59 From Cam Geer : +1 doc for free customers
13:08:02 From dsearls : Sam https://www.amazon.com/Tomorrow-3-0-Transaction-Cambridge-Economics/dp/1108447341
13:09:10 From dsearls : See emancay: https://cyber.harvard.edu/projectvrm/EmanciPay
13:09:35 From dsearls : It's about micro accounting, not micropayments
13:10:22 From dsearls : But it invites a fresh decentralized look at better economic signaling between demand and supply.
13:10:23 From KathrynHarrison : @Rileyâ€" totally agree on speed!!! Plus, most open source devs are being paid by someone to contribute.
13:10:25 From Cam Geer : like enterprise open source â€" free starter kit // then premium services
13:10:45 From MarkL. @smartopian : One issue here - is that the word Trust is actually Assurance - (in decentralised speak).
13:10:47 From KathrynHarrison : Also much easier to make difficult decisions when there is centralized leadership
13:10:48 From dsearls : We came up with it 13 years ago, but have been awaiting a perspective like Dave invites here.
13:11:00 From johnnyfromcanada : The primary concern with decentralized systems for enterprises is that there is no one to sue when things go wrong. That may not matter to individual people. So are we talking about people or enterprises? Or even possibly the elimination of the need for enterprises altogether?
13:11:23 From MarkL. @smartopian : Privacy is = Trust in Decentralised concepts
13:11:32 From Marc Davis : People are paid to post on Instagram today as â€œinfluencersâ€
13:11:49 From Matt Norton : By firms ^
13:12:04 From KathrynHarrison : Lots of people are paid to create content todayâ€" see you tubers who get paid to play fortnite
13:12:21 From KathrynHarrison : +1 Matt and Marc
13:13:26 From johns : And there is a shift with video content creators who now rely on Patreon, merchandise and Tips during live streaming away from advertising
13:14:50 From johnnyfromcanada : Of course David is in Vegas! What happens in Vegas, stays in Vegas!
13:15:06 From Marc Davis : The â€œconciergeâ€ sounds a lot like John Hagelâ€™s â€œtrusted infomediaryâ€: https://en.wikipedia.org/wiki/Infomediary
13:15:38 From MarkL. @smartopian : In the Pan-Canadian Trust Framework -for digital identity ecosystem - this (concierge role is) called Notice and Consent Processors -
13:15:39 From Cam Geer : in fact that is an intent that Dave cast with the conceirge for his interest in going to see a show

13:15:52 From johnnyfromcanada : â€œConciergeâ€ is a good analogy also because they do not ask who you are!
13:16:02 From johnnyfromcanada : They focus on â€œwhatâ€ you need.
13:18:39 From Marc Davis : The self-sovereign â€œPersonal Data Store/Serverâ€ concept can in theory outperform traditional â€œdata aggregatorsâ€ because it can have permissioned access to ALL of a personâ€™s data and thus provide a more holistic and valuable set of data and intents than any single data aggregator.
13:18:42 From dsearls : do we have a note taker here?
13:18:53 From scottmace : Yes I am taking notes right into the Google doc in real time
13:19:07 From dsearls : very cool, scott, thanks!
13:19:34 From johnnyfromcanada : Ya, a CMM for sovereignty
13:21:26 From johnnyfromcanada : Your network will be uncorrupted if no more than 1/3 of nodes can be compromised (BFT).
13:23:05 From KathrynHarrison : I think even the most idealistic people (developers) are looking for leadership and the most popular â€œdecentralizedâ€ systems all have them as youâ€™ve shown (though of course they arenâ€™t decentralized) â€” Satoshi, Linus, Vitalikâ€¦
13:24:39 From johnnyfromcanada : Indeed, do you trust benevolent dictators?
13:25:02 From dsearls : The Internet itself is distributed. Not absolutely, but pretty close.
13:25:29 From Laura Jaurequi : Sounds like a utility...
13:25:30 From johnnyfromcanada : But not trusted
13:26:14 From johnnyfromcanada : Trust in a trust-challenged environment is pretty much the whole point of DLT / Blockchain.
13:26:34 From Bill Wendel1 : @MarcDavis & @JohnnyFromCanadaâ€¦ Does John Hageâ€™s â€œTrusted Infomediaryâ€ goes beyond acting as a concierge to acting as an advocate, ie. a fiduciary? Hereâ€™s an example of a buyerâ€™s agent in the auto industry: http://www.authorityauto.com/about
13:27:02 From johnnyfromcanada : So like power of attorney?
13:27:21 From johnnyfromcanada : Or one form of guardianship?
13:27:48 From dsearls : peaking at 51 people now here. very good.
13:28:22 From johnnyfromcanada : The laws are criticalâ€¦. unless you really are going to defy the law.
13:28:58 From Sam-Smith : Dfinity uses a DCID (Data Center ID) that is managed by the Network Nervous System. Users must request and be issued a DCID. Its root of trust is not as decentralized as it should be. Entropy is the only root of trust we need.
13:29:02 From Bill Wendel1 : Johnny, Iâ€™ll answer your question from my experience as a buyer agent in real estate. n the past, conversations about fiduciary duties in real estate have focused on agency duties â€” essentially requiring the RE agent to disclose which side their on, buyer or seller. These principles Dave is describing point to where the agency conversation needs to go in the future in real estate â€” the role of Information Fiduciaries. More specifically, now real estate brokerage companies use data to help buyers, sellers and increasingly homeowners.
13:29:42 From Cam Geer : exactly! RISC -V!!!
13:30:18 From Cam Geer : would be great to have a RISC-V / IIW meetup
13:30:47 From Cam Geer : they are the silicon side of the SSI conversation
13:31:35 From Robert Mitwicki *THCF* : +1 for what Marc jus said!
13:32:22 From Marc Davis : @BillWendel1 Similar to John Hagelâ€™s â€œtrusted infomediaryâ€ concept, legal scholar https://en.wikipedia.org/wiki/Jack_Balkin has the idea of the "information fiduciaryâ€.
13:32:24 From johnnyfromcanada : @Sam-Smith - Indeed, however the Network Nervous System in theory at least is an effective DAO via a â€œliquid democracyâ€.
13:32:30 From KathrynHarrison : Someone has to pay!

13:33:00 From dsearls : https://www.luxuryinstitute.com/
13:33:01 From Cam Geer : my bad sorry
13:33:30 From Robert Mitwicki *THCF* : The way we think about collective data hubs is that you strip out the PII's and then you can do criteria search and do what Marc comment on.
13:35:19 From Bill Wendel1 : Question about Data collectives that would have value for consumers. As the real estate industry shifts from a sellerâ€™s market to buyerâ€™s market in a post Covid-19, would it be possible to organize a data collective for homebuyers to offset the seller bias, lack of transparency in organized real estate? If so, the market opportunity is HUGE!
13:35:23 From johnnyfromcanada : For any decentralization to be BFT, there must be some kind of â€œcontrolâ€ to ensure that 1/3 of work / stake / etc. does not get corrupted. That â€œcontrolâ€ is (currently) either a consortium (governing council, hopefully sufficiently decentralized) or a crypto-economics (with a high enough valuation to block capture of 1/3 of the value).
13:35:25 From Marc Davis : Link to my keynote from pii2010 that articulates some of the benefits of a personal data economy based on what we then called â€œuser centricâ€ (but might today call â€œself sovereignâ€) models: https://vimeo.com/14401407
13:38:10 From dsearls : good one, Marc. Maybe now we can finally make it happen.
13:38:53 From dsearls : i'm going to punch out and go to the session Brian is at...:-)
13:39:10 From KathrynHarrison : Despite my critiques, I think the work is awesome and Iâ€™d love to help find the right incentives and models to make decentralized systems competitive.
13:39:23 From johnnyfromcanada : Decentralization is an infinite regress. Do you trust the chip maker of the digital wallet that contains & computes on your behalf?
13:40:15 From johnnyfromcanada : Perhaps Trusted Execution Environments (TEE) and homomorphic encryption might offer solutions.
13:40:21 From Cam Geer : great job Dave!
13:40:23 From Cam Geer : thanks
13:40:29 From KathrynHarrison : Awesome conversation!
13:40:33 From Marc Davis : Thanks @dsearls! The work on SSI discussed at IIW looks really promising!
13:40:35 From Laura Jaurequi : Thanks!
13:40:46 From Alex Blom : Great conversation, txs

Kiva SSI Biometrics & How You Can Help!

Session: 12A
Convener: Cam Parra
Notes-taker(s): Cam Parra

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Since presenting and taking notes can be difficult these will be very limited and open to my opinion.
Kiva presented their project and their work in Sierra Leone. The architecture of the project was shown and discussed.

The floor was then open to the audience for various questions :

What can we improve?
This question then evolved on how in general biometric systems can be improved. Suggestions of multiple biometrics to use for Kivas system. Also how it is bad to keep raw fingerprint data.
Quick point was made that authentication should not be done with fingerprints to be real SSI.
A huge point was made that we should work on a minimum governance model for biometrics and SSI in developing nations.

Here is the Zoom Chat:
15:30:28 From Nathan George : Are there any fingerprint template standards or processing algorithms that would help move forward without risking a re-enrollment scenario?
15:31:43 From Asem Othman : There is a standard yes, but the risk of re-enrollment will be always there… this is the biometric
15:31:51 From Nathan George : heh
15:32:10 From Nathan George : Any pointers or homework assignments you can give me to help teach folks to be less-wrong?
15:34:47 From Asem Othman : Regarding fingerprint ? Or general biometric?
15:35:04 From Nathan George : Fingerprint templates and avoiding motion of raw scans
15:35:25 From Nathan George : And generic biometrics too, though we will be relying on things at an open source spec-driven level
15:35:42 From Nathan George : So specific business articles or device supplier approaches aren't as helpful
15:36:08 From cam-parra : Or scientific articles would be good
15:37:29 From Iain Barclay : I'm working with U of Notre Dame, my colleague is iris expert, and planning to release some open source algo's at some stage. We're going to figure out how to integrate into SSI for a pilot we have, over the summer
15:38:43 From cam-parra : Iain that is awesome ! Keep us updated
15:39:31 From Iain Barclay : Will do!
15:47:48 From Nathan George : Iain, that sounds very cool. We are looking for additional factors that we can make available. If you have an open source implementation, we should talk.
15:49:14 From Asem Othman : http://egovstandards.gov.in/sites/default/files/Fingerprint%20Image%20Data%20Standard%20Ver1.0.pdf
15:50:02 From Juan Caballero : I wish that statement were less controversial, Nathan!
15:50:10 From Nathan George : Juan++
15:52:16 From Nathan George : Asem++
15:56:53 From Nathan George : So a labelled trusted third party
15:57:05 From Juan Caballero : i'd love to see it, john
15:57:26 From Juan Caballero : not just because I've been to many human rights museums in Perú :D
16:03:10 From Juan Caballero : fpir
16:04:56 From John Callahan : @Juan: if you have experience in Peru and are interested in the project, please talk to rpimplaskar@veriidumid.com (Rajiv)
16:05:11 From Juan Caballero : Cool!
16:10:32 From Juan Caballero : https://www.businessinsider.com/scientists-designed-a-smart-toilet-with-butt-recognition-technology-2020-4?r=DE&IR=T
16:10:47 From Juan Caballero : smart toilets are going to be the new FBI cel phone charging station at DefCon
16:13:51 From Nathan George : T-2 minutes, so don't worry we can't leave too much more awkward silence to guilt anyone into participation
16:17:32 From Nathan George : What are the rules and who agreed to follow those

What Goes In Credential Subject? Let's Chat Credential Ontology

Session: 12B
Convener: Wayne Chang
Notes-taker(s): Wayne Chang

Tags for the session - technology discussed/ideas considered:
credentialSubject, JSON-LD, jsonschema, identifiers, industry use cases

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- How do we reconcile "B.S." vs. "Bachelor's of Science" vs. "BS"?
  - Some people refer to international standards that already exist or rapidly emerging groups.
  - Often you just have to ship something and see what happens.
- It's okay to make a credentialSchema that doesn't work for everyone. It has to work for one or a few people before everyone. It's an iterative process.
- Reminder that JSON-LD is isomorphic with RDF.
- There is a product opportunity for a collaborative JSON-LD context editor with ability to present & receive feedback on semantics from non-technical folks.
- How do we reference things? It's ad-hoc but mostly people use URIs.
- Why did DIDs come into existence? We tried to think about entity as email, URI, and realized there was a need for a user-controlled "thing".
- We prefer "control" over "own" for DIDs because the latter has semantic difficulties, esp. as it relates to guardianship.
- Recap of did-web, and risks of allowing large centralized authorities control large numbers of DIDs.
- DID operations are optional.

Reducing Correlation In Verifiable Credentials Without ZKP

Session: 12C
Convener: Rory Martin (Workday)
Notes-taker(s): Nikhil Wadwa, Gabe Cohen

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Rory giving overview:
These are topics we are considering but not actively developing
VCs are claims with provenance - Emerging WC standard
Workday credentials platform is a Verifiable Data Registry
The proof is signed by a key defined on issuers DID document
The credentials themselves are not the blockchain - only the public key infrastructure and the revocations are on the blockchain

There could be collusion between verifiers to aggregate data and gather extra information about the holder

Generating new identity for every credential - if the private key is lost, one may not be able to access / control the identity anymore - but it reduces correlation

BIP32 protocol:
Can be used to create an “extended public key”, and one can create the corresponding Private key by using the master private key - and the index of the corresponding public key

- Then only the master private key needs to be backed up

Key exposure risk can be reduced by using Hardened keys
Good security practice: Protect the master key by using a hardened child key
We need to create a stronger identity and reduce the risk of fraud
If multiple people hold a private key, they could utilize the benefits of that private key - however there is an increased risk of fraud for the verifier

rouven Question: what happens if the master key is lost or compromised:
Rory: We backup the master key / private key - encrypted - as a service for the wallet
rouven: Hypothesis is that we are moving towards hardware based keys
Rory: We use secure enclave to encrypt the keys

venu reddy question: are we holding keys on the holder side?
Rory: yes
Venu: How to aggregate credentials
Rory: the VC could be issued to a public key and not a DID

malwhere: a linked secret is a random number correlated to multiple DIDs. Also how does that solve correlation

Rory: The correlation we are solving is that the same credential doesn't get shared across verifiers
If we shared the same correlation to different verifiers they could collude - we reduce correlation but not completely solve it - the only correlateable attribute is the id.

Brent : BIP32 adds a lot of complexity. Why are we adding so much complexity, rather than support a signature that uses ZKPs?

Rory: WD does not use ZKPs because its hard to explain how they work and they won't be accepted in all transaction environments, e.g. government environments

Kendra: ZKPs arent approved for a lot of customers

Brent: BBS+ provides blinded signatures to hide attributes

Margo: Thanks for philosophical point about reducing bad correlation
Malwhare: ZKPs are not 100% anonymous but they give the choice of what to reveal

Rory: We are trying to be flexible and reduce correlation. We aren't trying to solve all levels of correlation - e.g. IP addresses based - we are trying to reduce correlation

David: Do you seek informed consent from users that they will be exposed to correlation? Data aggregates reduce the cost of selling data if you submit new data. if you disclose anything that is PII, they will toss the data into the global data market. There is a reasonable expectation of privacy for non-technical users. “Informed Consent”

Rory: From WD perspective all of our credentials are going to have PII that is correlatable - when we talk about informed consent - could we implement this via contractual obligations - we could also inform customers about how data is being used. WD will not be selling / aggregating that data. ZKPs do solve this from a tech standpoint - but we could also solve this from a business standpoint

Keith: We do full disclosure to the user about how they use the data and we can have terms and conditions as Rory said

Oliver: ZKPs arent fully understood

- Problem being solved: correlation across verifiers
    - If all creds issued to a single identifier, verifiers can collude and aggregate data
    - Risk of selling data to a 3rd party
- Creds not stored on blockchain, only PKI + revocation list
- The act of sharing a cred is privacy eroding (conveys info about the holder)
- Correlatable fields on creds:
    - Credential ID
    - Credential subject (DID)
    - Claims with PII (like a name)
- Solution? Multiple identities (pseudonyms)
    - Generate a new identity per cred
    - Pros:
        - reduce correlation x-verifiers that received different creds
    - Cons:
        - Increase # of private keys that need to be backed up
        - # of identities grows with # of creds
- BIP32 Hierarchical Deterministic Keys (HD Keys) (https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki)
    - New identities based on master keyset
- How does Bitcoin deal with this problem?
    - Accounts are public keys
    - BIP32 is an alg for dynamically generating a tree of keys
    - Hierarchical keys come in two forms: soft and hard
    - Each private key can generate a new child key
    - Each public key can generate a new soft child key
    - A hierarchical wallet can generate a new pub key without holding private keys
    - Only need to back up master key
- Vulnerability: not secure for sharing private keys
    - Sharing of a soft private key and any extended pub keys in the hierarchy can lead to exposure of all private keys in the hierarchy
    - Extended pub keys (public keys + chain code) need to be secured better than standard pub keys

- Hardened keys act as firewalls by limiting the ability to derive private keys back up the hierarchy
- Best practices dictates that the first key of a master key needs to be a hardened child key
- BIP32 + VCs
    - Holder register their master pub key to the blockchain
    - Master will be protected by a hardened child key, which will be used to derive all other child keys
    - Verifiable data registry will generate a unique child pub key and associated DID for each cred issuance, based on the credential ID (uuid)
    - ISsuer will use that child DID as the "id" field on the *credentialSubject* block
    - Holder will generate the associated DID Doc on the fly when they need to share the cred w/ a verifier
    - The holder only needs to backup their master private key
- Workday's cred IDs are UUID-4 (128 bits of randomness)
- Each private key in the hierarchy can have 2B soft child keys
- In order to have sufficient distribution in child DIDs to ensure that they will not collide, we will need to derive ..

Result:

- A stronger identity using BIP32
- Identity is more than an identifier-- it's the accumulation of all claims attributed to it; therefore splitting the identity into many independent fragments which has consequences
- With small identity fragments, risk of sharing the underlying private key is minimized
- Sharing private keys reduces trust x-system, since claims made about one person can be fraudulently verified against another
- Sec vuln of BIP32 maintains risk in sharing private keys and therefore increases trust in the validity of a cred

Rouven: how do you handle lost private keys?

Rory: we only have single keys that represent your DID (right now), and we back it up with a password, encrypted as a service with our wallet. can download and recover if you have the pw to unlock your key. similar loss scenario to a master link secret

Rouven: who is storing it? who has access to it? in this case, it's practical to have a trusted wallet, but not very self sovereign. we have DID because they are a KMS. if I create 100 keys to a 100 DIDs, or creds, then I have to rotate … a single public DID is simpler to manage in terms of rotations, re-issuance, etc. Hypothesis - moving towards keys more in hardware, less moving around. Direction is to use hardware to do encryption

Rory: we do use secure enclave keys to encrypt wallet, but they are not transferable between devices

Venu Reddy: keys are on the holder side? not issuer side? how would you use this information - proof from multiple creds?

Rory: we can ditch DID Docs, and issue creds to pub keys. if you can prove ownership of priv key, you prove ownership over the cred. DID Doc -- key profile over pub key (can be rotated, multiple keys). HD keys -- Verifiable Data Registry holds extended key, and can derive keys for you, but needs a deterministic way to

do it. Generates a UUID -> path -> pub key. HD key doesn't have a DID Doc which makes it easy to back up but hard to rotate

Malwhere: Link secret is not a master key or master secret. Link secret is a random attr you stick in every cred, similar to a DID. Random number, not a DID. How does this solve correlation? The signed data is not changed with BIP32. The data has to change every time you present, including the signature. Otherwise it's a unique identifier. DID, signature, everything would have to change per-presentation to reduce correlation. BIP32 alone doesn't reduce correlation.

Rory: Apologies for misrepresentation of linked secret, unaware of workings. Specified correlation we are trying to reduce -- sharing *same credential* with multiple verifiers. Any data (like the proof) is correlatable, but not a correlation problem we are trying to solve. Trying to solve different creds with different verifiers, they won't be able to create a master data set.

Malwhere: They still can create a master data set? Any data that is the same can be correlatable.

Rory: Varying levels of correlation. Same cred to two different verifiers, they can recognize they got the same cred from the same holder...but they can't correlate across credentials. If you had 1000 creds and shared with all different verifiers, no one can come up with a full dataset from collusion. The only truly correlatable ID is the cred subject (ID). Agree it does not solve all correlation.

Brent: Added a lot of complexity...why not use a ZKP signature?

Rory: Above my paygrade. Don't think they'd be accepted by all txns we use. Govt transactions, not a standard that's adopted. Hard to explain to customers. We are using Ed25519 signatures. Need to be FIPS complaint
Margo: thanks for bringing up the functional side of things. not all correlation is bad

Malwhere: "not the right excuse" re:FIPS. Not 100% anonymous

Rory: Not disputing. We are working within the bounds of Ed key

Keith Kowal: We are sharing names, skills, and directly correlatable attrs in the creds.

Brent: I applaud efforts to reduce correlation. Wish they went further (as some people would prefer).

David Huseby: Do you seek informed consent?

Rory: what can we contractually limit? abide by certain standards on signup

DH: How to square with CCPA? Share with entire possible chain and get consent. Are you building that in?

Rory: Contacts as we can.
….
Malwhere: Never said ZKPs don't leak everything…

Oliver Terbu: ZKP not really well understood by customers in our experience. Even people using Indy not clear on it. Still like and see value in ZKP.

Integrating DID Into An App in 10 Minutes

Session: 12D
Convener: Jonathan Lu (ArcBlock)
Notes-taker(s): Matt McKinney

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

We discussed how to implement DID capabilities into any application or website using Arcblock's DID:CONNECT and decentralized identity wallet.

www.abtwallet.io (decentralized identity wallet)
login at www.arcblock.io using DID:CONNECT service to connect external applications to decentralized identity service

Anyone can run their own DID service in the cloud - AWS, Azure, etc

Scan to login experience - https://www.arcblock.io and on the upper right hand corner.
Demos to try: https://www.arcblock.io/en/try-identity-now.

Walk through developer experience using DID:AUTH with React. https://github.com/ArcBlock/did-connect-examples/tree/master/examples/did-auth-with-react

Host walked through the demo and had the up and live in about 7 minutes.

confirmed that ArcBlock's identity service can be used with Hyperledger, Ethereum and others as ArcBlock has decoupled the identity service and allows for users to adopt different backends to support their use case.

JSON Web Messaging (JWM): What Are They & Why Are They Useful For Secure Messaging Systems?

Session: 12E
Convener: Kyle Den Hartog
Notes-taker(s): Ryo Kajiwara

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

https://tools.ietf.org/html/draft-looker-jwm-01
https://github.com/mattrglobal/jwm

(related: Consent to Create Binding https://wiki.idesg.org/wiki/index.php/Consent_to_Create_Binding
short-lived vs long-lived: when consent changes over time)

JWM: way to encode application-level messages
use JWE to protect integrity
JWS to associate messages with a non-repudiable digital signature

https://medium.com/mattr-global/jwm-a-new-standard-for-secure-messaging-a21d3daa4403

JWTs are good as tokens, except it's not good for messages
more optimized towards secure messaging use cases

multi-recipient architectures
JWMs do not allow `none` format of JWT

not dealing with the delivery mechanism
-> usage of DIDComm

IETF working group? -> trying to get it to dispatch
trying to present it at next IETF

didn't specify anything like DIDs at this level (for recipients/senders)

unguessability of the ID?

Authenticated Encryption
signing is one thing, you can also use AE
ECDH-1PU https://tools.ietf.org/html/draft-madden-jose-ecdh-1pu-03

intermediaries that want to make decisions without knowing the content
signatures that are understandable by intermediaries
multi-level nested JWM
    sign then encrypt, not encrypt then sign
    but if "sign then encrypt" (=e2e encrypted), intermediaries can't interpret the sign

differentiation of metadata of the message and content of the message
standard attributes of JWM is message metadata-y
you can put whatever in the body
it will be a useful feature
or else everyone will have to invent a way to not collide

Q: Was JWS built with transports without encryption in mind? What protocol (for transport/delivery) was on your mind when you were developing this spec?
-> HTTPS. keeping the message when the user is offline. with HTTPS the transport is secured, but data at rest is not secured, so having the message encrypted at message level also helps.

Comment: Direction for taking this draft forward. Contact Application Area Director at IETF. JMAP WG does something similar (not exactly fitting current charter)

Trust/Risk Metrics In SSI – What Can We Learn From Technical Trust In Order To Inform Human Trust

Session: 12F
Convener: Will Abramson & Nicky Hickman
Notes-taker(s): Scott Mace

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Nicky: Will & I have been working on establishing SSI with blockchain paper. We want to get to emetrics. Get your input. Interest from Sovrin framework governance WG. Want ultimately to get to a Net Promoter Score for trust.

See the slides here
https://drive.google.com/file/d/1J_dpAdP5c641QhJCmatCcaq6ZVc1uCdl/view?usp=sharing

See the spreadsheet with some ideas on measuring Sovrin Governance Framework principles with 'fancy maths'
https://docs.google.com/spreadsheets/d/1NHs-3rmfu8z59LeaE2Ey9HkEu0OoRUjJufbMhfewmls/edit?usp=sharing

see Will's paper on 'What can a verifier learn'
https://docs.google.com/document/d/1Y_qACJ6wcaLQXqd2zRboK0l7c02pnmz0tOTc2AkCWHg/edit?usp=sharing

Will: Crypto is the hard facts we can use to help us make decisions.

joehsy: NPS is based on surveys.

Nicky: It's the softer side of trust, an NPS survey. Qualitative metric. One of a number of metrics you might use. See how systems are performing. What that means in terms of repeatability in anatomy of trust. NPS works across industries. We all struggle with trustmarks. In world of brands & retailing, people tell you when brands they trust and which they recommend.

Will: What perspective are you measuring from. Who are you, what role do you play? What metrics can you use? And are they measurable?

Dennis: SSI is private?

Will: Some markers can be used.

joehsy: Session yesterday talked about ways to measure SSI adoption. Level of activity.

Nicky: KPIs when managing consumer-facing identities, adoption comes in here with reach, number of customers. Number of wallets wouldn't necessarily tell you the number of unique individuals. Then density, number of relying parties, verifiers, how useful is this wallet. Helps you build momentum in the market. Then things like frequency. A customer who has a wallet that he or she never uses is not that valuable to a corporation.

[Shares ToIP Stack slide]

Iain Henderson: Used to run 2007 Trust Index, reverse engineers getting a good score. [Shares slide]. In the process of building that again for GDPR]. [Link in chat to this slide.]

pknowles: This is proper trust.

Will: Is it worth it to me to become a verifier?

Nicky:What will drive trust in SSI? An application in healthcare, academia, elsewhere?

pknowles: SSI will save companies a huge amount of money. Measure it before & after

Nicky: No one got what the guy who invented the first water turbine had made. “That water made the light come on.” We need that for SSI. Just demonstrating the applicability.

Karyl Foster: Feels like identity is a pervasive innovator. I’ve been told it’s the death of good entrpreneurs. Different events will accelerate the market. Like COVID, more secure contact lists.

Nicky: How could it enable interoperability? Single sign on, account matching.

joehsy: Workday is a mainstream enterprise company, successful adoption will drive a lot of consumer trust. Need a set of killer apps where everyone has a DID wallet, and people realize what else they can do vs the usual authentication by other means.

Will: How many DID wallets do people have.

joehsy: I have a few, no place to use them.

Iain: Until 3 months ago, I worked for a company that had Workday. HR record request took about 4 weeks to get. Employee should have access. It’s not the SSI that’s important, it’s what I can do with it.

Jeffrey Aresty: SSI for voting, everyone would have it. Vote by mail is what we get. Notary is a form of a trust. Real estate closing is a piece of digital truth. No question if both sides to a transaction are authenticating this is what we signed, hashed in pic & doc form, that’s the closest thing you can get to 100% truth. Who’s issuing the birth certificate? The midwife knows what happened. The bureaucrat has least knowledge. We’re doing a lot of that in Africa. You don’t have the state involved unless you have national ID cards. They want to use them to empower themselves. A lot of interesting transactional business there.

Nicky: This picture [User stories will fit into standard IAM workflow] is the whole human trust thing. Excited with some of the work being done in Aries with continuous integration of governance frameworks. Governance typically a document, the rest being computer processes, was well made. Measuring conformance could reinforce trust.

Jeffrey: In Africa, imagine 60 years ago in the U.S. Regional setups, growth opportunities. The justice frameworks aren’t nearly the obstacles they are here. Unlikely to happen where politics are involved. You can put SSI into motion in these countries. We are training HS kids to HS kids, Texas to Zambia, kids can do the work. They need something that shows they graduated with a competency in something...justice typically measures cost, not impact.

Nicky: I love the certainty of cryptographic trust. Is there an intermediate between that and human trust - call it technical trust in a business process.

pknowles: Cryptographic trust is assurance. A little weird to me.

Zoom Session Recording (link provided by Will Abramson):
https://www.dropbox.com/s/1b4fiji2kjxn984/zoom_0.mp4?dl=0

Zoom Session Chat:
14:02:37 From Sterre den Breeijen : fine
14:14:47 From Elias Strehle : Could you share a link to the presentation?
14:15:33 From Nicky Hickman : will put online after this to share
14:16:01 From Elias Strehle : Could you share the link to the "fancy mathematics" on the previous slide then? :)
14:16:57 From Nicky Hickman : https://docs.google.com/spreadsheets/d/1NHs-3rmfu8z59LeaE2Ey9HkEu0OoRUjJufbMhfewmls/edit?usp=sharing
14:19:49 From Karyl Fowler, Transmute : @Iain that reminds me of this privacy plugin from Osano: https://www.privacymonitor.com/

14:20:25 From Karyl Fowler, Transmute : trust ratings that just measure what companies are doing against their own T&Cs
14:20:44 From Iain Henderson : Thanks Karyl, i'll have a look
14:21:59 From Iain Henderson : Yes, PrivacyMonitor looks very useful
14:22:27 From joehsy : PrivacyMonitor reminds me of this: https://pribot.org/polisis
14:23:22 From Karyl Fowler, Transmute : ^^THAT is cool.
14:25:10 From Nicky Hickman : great links, please put them in the notes. Thank you!
14:26:28 From scottmace : I will copy the entire chat to the notes when we conclude
14:33:08 From joehsy : Sorry got to drop off to a meeting. Great stuff!
14:33:24 From Nicky Hickman : thanks for coming bye..
14:34:31 From Nicky Hickman : Thank you scott
14:51:10 From Wip : https://docs.google.com/document/d/1Y_qACJ6wcaLQXqd2zRboK0l7c02pnmz0tOTc2AkCWHg/edit?usp=sharing

Determining Demand & Feasibility For Your SSI/VC Use Case

Session: 12H
Convener: Timothy Ruff
Notes-taker(s): Jonas Jetschni

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presentation based on following document:
https://docs.google.com/document/d/1_Usxxug9jubChP1yfNjE0wOKFfQYr3eebwAW8QyZCVg/edit#

Key challenge for the SSI space “if you build they will come” - talk to your customer, fall in love with their problems and understand what they want

Five Steps to determine market demand

- Know your ideal issuer, holder and verifiers
- Find market viability with the verifier by speaking with them
- Test interest and capability of issuers by speaking with them
- If interest or capability of issuer is weak, build pressure through verifier / holder demand
- If you don't get your ideal issuer, talk to Proxy Issuer

Onfido integrated with Evernym Connect.me wallet, has the capability to issue VCs. Onfido is issuing credentials as part of the UK legal sandbox with Evernym Connect.me wallet and uport wallet. Legal is still a challenge for Onfido, mainly due to legal cost to make it work

For many identity provider, legal obligations is a challenge, e.g.
Lucy Yang to Everyone: “*** cannot support your requirements due to our contractual obligation with our data vendors that prevent us from having this business relationship with organizations who provide any sort of identity certification, including self sovereign identity.”

NetKey is able to issue verifiable credentials

Credit unions moving towards product as they want to go touchless (~500.000 people)

- Credit unions issues credential to member
- Member presents this credential to credit union
- Issuer/verifier same Authority but not same department

To reduce complexity of driving adoption with issuer/verifier/holder, combine issuer/verifier in one authority. This will serve GTM efforts.

Every customer of an IAM solution provider is an ideal target customer for SSI. Advantage of VCs, the addressable market is bigger as they allow for context switching.
IAM players have not moved into SSI due to the innovator's dilemma, they are making money and growing

People spending time and money on tech, without talking to customers and understanding their real needs
Book recommendation: Running Lean: Iterate from Plan A to a Plan That Works. Avoid spending time on building code. You can find product market fit without building.

Great compromise between building a prototype and slide deck is a clickable prototype
---
SSI stories and SSI could explode this year
SSI Tracker: Track momentum, Startups, Consortia
The industry needs to start understanding what is happening in the community
Showcasing demand to governments can be a driver for adoption.
Eat your vegetables ;-)

Zoom Chat log:
From Timothy Ruff to Everyone: 11:02 PM
https://docs.google.com/document/d/1_Usxxug9jubChP1yfNjE0wOKFfQYr3eebwAW8QyZCVg/edit#

From johnnyfromcanada to Everyone: 11:05 PM Fallacy: If you build it, they will come.
From Tushar Phondge to Everyone: 11:06 PM Totally agree @johnnyfc
From johnnyfromcanada to Everyone: 11:06 PM Solutions looking for problems. ;-)
From Juan Caballero to Everyone: 11:07 PM AKA "notary" issuers
From Cam Geer to Everyone: 11:10 PM like Okta for IAM
From Derick Grey to Everyone: 11:11 PM And most of them are actually laying off or reducing IT workforce because other tests have significantly reduced.
From johnnyfromcanada to Everyone: 11:12 PM The steps are necessary, but not sufficient…
From Cam Geer to Everyone: 11:15 PM core product discovery work — customer problem discovery // product solution discovery
From johnnyfromcanada to Everyone: 11:15 PM It's a decentralized consensus problem!
From Cam Geer to Everyone: 11:17 PM it's the product manager's job to synthesize the customer input's to create an organizational consensus toward something that is worth doing
From Juan Caballero to Everyone: 11:17 PM I think there's some companies here at IIW
From johnnyfromcanada to Everyone: 11:17 PM Onfido
From Juan Caballero to Everyone: 11:21 PM I can't blame them
From johnnyfromcanada to Everyone: 11:22 PM https://onfido.com Legal seems to be a key blocker
From Dima Postnikov to Everyone: 11:22 PM Liability…
From Juan Caballero to Everyone: 11:23 PM Yeah, Riley's accurate-- they wouldn't issue VCs for us, but were happy to let us issue credentials based on the results of their API calls
From johnnyfromcanada to Everyone: 11:23 PM Timothy says: Revenue trumps legal
From Juan Caballero to Everyone: 11:23 PM LEGALLY (not technically) they said they weren't issuing any time seen soon
From johnnyfromcanada to Everyone: 11:24 PM OK, Timothy did not say "exactly" that. :-)
From Lucy Yang to Everyone: 11:24 PM *** cannot support your requirements due to our contractual obligation with our data vendors that prevent us from having this business relationship with organizations who provide any sort of identity certification, including self sovereign identity.
From Juan Caballero to Everyone: 11:26 PM !!! congratulations everyone, we're officially a threat to other business models :D Onfido told us they were very bullish on SSI long-term, just not issuing now
(side note: amazing)
From johnnyfromcanada to Everyone: 11:28 PM Indeed. Although "better" solutions have often died on the vine… LaserDisc, Betamax,...
From Juan Caballero to Everyone: 11:30 PM ^ This is actually my biggest concern about onfido, tbh--- something about the timing of their round makes me think all covid ID functions will be powered by "AI", not SSI...
From johnnyfromcanada to Everyone: 11:30 PM Yay! Credit Unions going to Production!
From Andre Kudra to Everyone: 11:30 PM Johnny, I had LaserDisc! Still a fan. Anyways into retro-tech.
From Paul Jackson to Everyone: 11:33 PM Do you have a list of all the VC use cases going to production? Would be good to find out more about the credit union examples and others.
Having that list alone would help to encourage others to move to production. Few want to be the first, encouraging for others to see that they aren't the only ones going forward.
From Cam Geer to Everyone: 11:33 PM this is the problem / opportunity I want to chase
From Stew Whitman to Everyone: 11:35 PM Just joining, Was there a link to the Google doc chared?
From johnnyfromcanada to Everyone: 11:35 PM Notes: If possible, make Issuer & Verify the same entity (make one of your variables a constant).
From Juan Caballero to Everyone: 11:36 PM They're more likely to do all employee testing at gunpoint
Ah, interesting she makes an interesting point re: cross-context VCs
From johnnyfromcanada to Everyone: 11:37 PM

https://docs.google.com/document/d/1_Usxxug9jubChP1yfNjE0wOKFfQYr3eebwAW8QyZCVg/edit
From Bill Wendel1 to Everyone: 11:37 PM Agree, Paul. I'm interested in real estate use cases. My experience is that some credit unions offer residential mortgages in-house, and others outsource the process to a service center. As fiduciaries, credit unions have a trust relationship that can be turbo-charged as their mission is to help members save money. So, yes, the cost saving approach should sell.
From johnnyfromcanada to Everyone: 11:39 PM Notes: IAM have not moved in this direction - Innovator's Dilemma: https://en.wikipedia.org/wiki/The_Innovator%27s_Dilemma
From Juan Caballero to Everyone: 11:40 PM Awesome, thanks for having me, I'm gonna butterfly around to some other sessions!
From Matt Norton to Everyone: 11:41 PM Getting that list might be difficult, many firms going to market are still in stealth about it
From johnnyfromcanada to Everyone: 11:42 PM Another emergent incentive is to alleviate the cost risk of liability due to rising data protection regulation (whether agree or not).
From Paul Jackson to Everyone: 11:43 PM Even having a starter (and evergreen) list would be helpful. Even a couple of examples would help. The National Health Service example is a good one but more examples are needed. Even details on the Credit Union ones would be big.
From Derick Grey to Everyone: 11:45 PM YAS Leans!
From Cam Geer to Everyone: 11:46 PM
https://www.amazon.com/Running-Lean-Iterate-Plan-Works/dp/1449305172/ref=sr_1_1?crid=W5XTI966GDHT&dchild=1&keywords=running+lean+ash+maurya&qid=1588196784&sprefix=running+lean%2Caps%2C196&sr=8-1
From Vic Cooper to Everyone: 11:48 PM https://www.albertosavoia.com/therightit.html
From johnnyfromcanada to Everyone: 11:50 PM There is a strategy that some contemporary startups follow is to grab money and make a solution. See also: Is the Lean Startup Dead? https://steveblank.com/2018/09/05/is-the-lean-startup-dead
From Cam Geer to Everyone: 11:54 PM and publish the stats in real time!
From Matt Norton to Everyone: 11:54 PM Bill Gates' digital credential quote
From johnnyfromcanada to Everyone: 11:54 PM The problem with standards… the aren't. ;-) Actually, I think that the "meta" philosophy of providers like Sovrin, Hyperledger, etc., sounds good in theory. But it also fragments the market - ripe for corporate capture.
From Darran Rolls to Everyone: 11:55 PM Can you share the doc link here
From Timothy Ruff to Everyone: 11:57 PMhttps://docs.google.com/spreadsheets/d/1egn-ZXVSD_LMPpJVZdD12d_VvLMIPpYrFJdLmOOlqNE/edit#gid=0
From johnnyfromcanada to Everyone: 11:59 PM Notes: Portable identity "Transitive Trust"
From Cam Geer to Everyone: 12:01 AM it is an info / PR war
From Brian Richter to Everyone: 12:01 AM Whos Vick? Oh nevermind
From Timothy Ruff to Everyone: 12:01 AM the guy speakin :)
From Cam Geer to Everyone: 12:01 AM Founder of HearRo https://www.hearro.com/
From Timothy Ruff to Everyone: 12:02 AM Paul jump in when Vic is done
From johnnyfromcanada to Everyone: 12:04 AM It's a war of information & "truth". Beware the "Industrial Complex". Numerous domains have been taken over by entities that have coopted the terminology, concepts, meme, fad, etc. For example, where I work, which is "Lean-Agile".
From johnnyfromcanada to Everyone: 12:10 AM Beware sunk effort / cost on solution built too soon
From Me to Everyone: 12:11 AM For me its always about desirability, viability, feasibility
From johnnyfromcanada to Everyone: 12:12 AM Design Sprints: https://www.gv.com/sprint
From Me to Everyone: 12:12 AM +1
From Cam Geer to Everyone: 12:13 AM used design sprint a lot
From johnnyfromcanada to Everyone: 12:13 AM Einstein: Spend 55 mins on the problem, and 5 mins on the solution.

From Derick Grey to Everyone: 12:13 AMLook into Dual Track Design. Dont' just have a design sprint. Do vision design, and then always design.
From Dima Postnikov to Everyone: 12:14 AMGreat session. Thank you.
From Derick Grey to Everyone: 12:14 AMErr Dual Track Development
From johnnyfromcanada to Everyone: 12:14 AMDual Track Agile as well… Discovery & Delivery

Building Technology & Successful Use Cases Based On The Most Marginalized As The Answer To the Problem.

Session: 12l
Convener: Shireen Mitchell
Notes-taker(s): Grace McCants

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

How are we creating successful models particularly during development. Background: digitalsista started coding when she was 10, created first women who code/women & girls fo color in 1999. Moved into space around online harassment and how tech companies were not paying attention to how platforms were being weaponized. Overarching problem: There's no tech fix for the human behavior. We start with the framework for building the tech and nudging the humans. I believe that is flawed--we should nudge the tech instead of nudging the humans.

Other viewpoints are welcome.
Model: "move fast and break things". A lot of things have been broken because we've been moving fast. We've been looking for a social solution tech can solve versus looking at social problems. Been looking at how social groups form and if we watch that we can look at how tech can support the most marginalized. We can see "trickle down" hasn't worked.

Broad conversation, these things are new, and there are some jarring frameworks. We are built into a system that we think "should" work this way. Failure of AI systems in terms of face recognition, how it's used to surveille. Some of that is built on concept of building for greater good-- the fix is not the problem -- the problem is we design things without thinking about the concepts.

Grace: Some of the underlying issues are based on how money is designed and the fact that the playing field is not fair. The system is
Digitalsista: Often the people solving the problem aren't the population for whom they are solving problem.

JeffO: Agreed, the human operating system-- everything we are writing to is writing to our human nature. Staring with "most vulnerable first" starts with ancient times, where the root communities had to care for the fragile people. It's "encoded". Underneath, the most vulnerable, the idea of "reaching from the height down" is ideal. How can we play from the human operating system forward. P2P alliance is looking into that.

Digitalsista: Awareness of the fact that we are part of how the system moves. the system disproportionally impacts certain groups. Especially the harms--they think they're separated from the harms and they're not.

Celine: Was looking at an attendee demoing a solution, and I asked about how that might impact people who are suffering from abuse at home and his response was "Well, nonprofits deal with that". There's a disconnect and it starts with teh creators and builders and technologists. If we don't think of ourselves as at the top of a system where it will affect the bottom (I hate that language) but we have to think of ourselves as part of the system. It's not enough to think about how we are going to reach marginalized solutions what's more important is bringing them to the table or going to their table.

From Celine Takatsuno to Everyone: 11:02 PM thank you for asking
From Lisa LeVasseur to Everyone: 11:06 PM don't get me started on agile and lean as they contribute to going fast and breaking things....
agree with that hypothesis/observation.
From Lisa LeVasseur to Everyone: 11:15 PM dissociation
Digitalsista: Especially with identity part. There are two groups of people… anonymous was a woman.. I used to get on line pretending not to be a woman or pretending to be black. I would pretend to be somebody I wasn't. It's not fair that people have to take away parts of their identity to get something done or participate fully. Eventually I chose this name because I didn't want to hide anymore.
From Marc Davis to Everyone: 11:16 PM One of the approaches to a "human-centered" design process is "participatory design" (https://en.wikipedia.org/wiki/Participatory_design) which directly involves "users" as stakeholders in the design process much earlier and more fundamentally than traditional "user testing" approaches. Are you advocating for a participatory design approach?
Digital Sista: When talking about anonymity, for example, the protections for people who are being harmed are different than the protections for people who aren't
From Lisa LeVasseur to Everyone: 11:22 PM
- Use Cases
- Abuse Cases
- Misuse Cases- identifying blindspots
Grace: Example from Anna De Liddo from Open University in Milton Keynes near London. She was creating a discussion platform where people were able to state their opinions by posting articles or videos, and then the responders were able to discuss the source of those articles or videos, or the info in the articles. Because people were talking about the articles, it was not seen as a personal attack and the people were able to improve their decision-making and sensemaking skills and even change opinions. Even people with vehement opinions were able to change their opinions. So we can create digital systems like this which are able to improve outcomes if we observe how the human psyche works and design for that.

Digital Sista. There's rage quitting because people didn't like the process and then there are people in the system who might be intentionally causing people to quit. We also want people to have their voices heard while the work is being done versus just using the system that's supposed to change. We notice the people who are missing and feel frustrated but we don't see that as part of the final product or the use case.

Marc. What would a design process look like? 1. You must have use cases that included marginalized people. More than that would be 2. Design first for marginalized populations. 3. Not only do that, but have the people who are included in the design process as stakeholders and participants in the design process. Scandanavian, "co design process". Are those the kind of things you're advocating? Wanted to get clarity.

Digitalsista: I appreciate that, and Lisa commented, so I'm going to ask her to jump in. The way you though through that process, from a design process, we need to look at the users themselves. We have the procut and then we have beta users. In that moment we have already confirmed that this is the core product. We're dealing with the stresses of where the users built it out rather than where the users would have built it in a core system
For example, simple example, everyone has heard the term "black twitter" The term "blakc twitter" is a concept based on a specific community that's carved out a piece of twitter just for them while twitter is a public platform. Only certain groups of people are communicating with each other in this group. Some who step into "black twitter" step into something they haven't seen before. Those who don't understand the push of twitter into what becomes "black twitter" they see something foreign or abnormal, yet that community existed the entire time but they only notice it when it's in a mainstream media narrative. Twitter has done a horrible job of understanding this phenomenon.

From Celine Takatsuno to Everyone: 11:27 PM one challenge/problem with an expressed participatory design approach is the failure to consider/include/realize the impact on passive or recognized stakeholders —they're not users, but they may be affected by what we design and build. tech has social impact no matter if it's 'social impact tech' or not.

(yes to participatory design, and @mark great observations)

From Jody to Everyone: 11:29 PM no (oh - just see zoom has a button for that)
From Kaliya Identity Woman to Everyone: 11:29 PM There is also Native Twitter, Disabled Twitter, Autistic Twitter etc…

Mark: In participatory design, that impacts the design process on day 1: Who is in the design process.

Lisa: It struck me that we have the idea of "use case". If you're not building use case around misuse and abuse, you're missing the boat. The participatory design process is to minimize blind spots. I do have a practical question --in some sense some technologies are really for everybody. Like Facebook, it's broad for everybody. How do you have everybody at the table? Is there some checklist or model or tool. There need to be some tools to help identify blind spots.

Digitalsista: About FB, when we think about the design, we have to think about the origination of the design. FB was designed for "Hot or Not". We've done the research. Because it was designed for "hot or not" it was not designed for whether the hot woman was black or brown. When you build out from there, you aren't building from a use for everybody. It's already a system that is excluding or biased for a certain kind of system. The core design was exclusionary. We got there, it was not just exclusionary in terms of race and sexuality. It was exclusionary in terms of age and education. The system is now stretched and you are trying to do a fix for something that was built into the core. the people who come to work for that company are going to be oriented towards that framework. FB is the perfect example of core design that was not for everybody that people still think is for everybody and we are watching how the platform is being used to harm people, and FB is struggling to fix. At least I think the 3 things you said, Kaliya and I work on the concept of threat models. I do like the frame work in terms of use cases, abuse cases and misuse cases. I think that helps to find the blind spots. Thank you.

From Lisa LeVasseur to Everyone: 11:33 PM intention vs actual adoption

Shannon. To questions about how we be informed as we move forward. I'm a community organizer and there's a slogan (Nothing about us without us.) If "they" think they're "reaching down" for someone they think is "other" therein lies the problem.
Digitalsista: they also get defined as sub-cultures as if their inferior

Shannon: the erasing of the creators. Someone creates something amazing and someone more resource-centered takes it and the founder gets erased. That needs to not get erased and the media can be part of that. I'm interested in going into communities and starting there. TikTok -- it's been interesting to see the algorithms and ideas about some of the people feelign threatened by older people and the racism and transphobia have been overt. This happened in FB when they didn't have awareness of who

From Marc Davis to Everyone: 11:38 PM @CelineTakatsuno Great point about the social impact of technology on non-users. Definitely need to consider that in the design process and the iterative redesign process given unexpected outcomes. One common way to deal with designing systems for "everybody" is to identify representative "personas" (not a real person, but a fictional representative of a user population) and to detail "scenarios" for these personas. Other technique in designing for "everybody" is to do A/B testing of different designs across large populations to see which design is most effective. Problem with both of the above approaches is they do not require that users are co-designers or stakeholders in the design process from the beginning. Participatory design does ideally accomplish that.
From Lisa LeVasseur to Everyone: 11:38 PM FB highlights an interesting problem: post-launch product pivoting . How do you (1) recognize it, (2) inject participation of new stakeholders in a moving/live product.
From Lisa LeVasseur to Everyone: 11:43 PM FB highlights an interesting problem: post-launch product pivoting . How do you (1) recognize it, (2) inject participation of new stakeholders in a moving/live product.
exactly. we aren't separate.

Grace: It's naive to think that we can fix a system that is much deeper in how business models and money work. It's impossible for our brains to function in a way that would really honestly even out the playing field between the haves and have-nots.
From Marc Davis to Everyone: 11:46 PM So to answer @Grace, can the design process itself (and the structures of collaboration and ownership the process is embedded within) be structured so that it both embodies the socio-economic relationships and structures we would want to move toward as well as produce systems that help move society towards that change?

@ Marc, that's a great inquiry. I'm particularly interested in new forms of currency and interaction that will replace the current system as it continues to prove itself inadequate to resolve the problems humanity is facing today.

John: Works in public service. It's a privilege to work in an area that's about public service rather than money. It's a piece of the cultural fab that is great. And one thing that is troubling around technology is that we've forgotten that there is a good that government can serve in creatin software that is grounded in service values and not in business values. Government can and should invest in software that is for the public good and regulate more carefully how private sector uses that and leverages that work that was done with the public money.

We need to grow the tent. Problem with not having enough diversity in our little community is that our community is little. I think the tent gets grown by considering the social aspects, we call that governance aspects. We live in the world of people and in the world of relationships and those are human relationships. It's those human relationships and norms ceremonies that are too often shaped by the technical

implementation. THink about the human elements first and turn apply them to the community you belong to.
Digitalsista: I was part of a movement to try to get Wifi to people who didn't have, and we had huge fights with the tech companies coming after us, and the government either participating or the government trying to come up with their own version, and the tech companies going after them because tehy perceived it as taking away their profit margins. Today in the days of Covid, there are families that have to drive to the school, even though the school gave them a laptop, to get access to the internet. Those are the kinds of phenomena that we don't ven think about. there are people who don't even have running water. That includes the way government operates as well as business. It's not just what Grace pointed to.

John: Idea of verifiable origins and greater observability on operations that could be helpful.

Jeff: Taking a step back and thinking about who we are… and thinking about sensitivity training. the idea of "the other" causing a disturbance and being an offensive issue is a very anciet issue. The ide of the other wasn't generally a great thing. In terms of human OS sensitivity training, you can use some grace to understand that's how we are constructed and help people learn and move away from that.
Another thing that came up from e around glack twitter it reminded me about a software called "Drive" designed from street level up, navigation. Looked at all things in the space. What won was Google Maps, architected as search. Had to include all search, but search only elevated the places that mattered to lots of people. So some places didn't have the gravity. The root concept of navigation was superceded by being driven by search.

Johanas: There's also a trend that next year will be a trajectory from last year. Right now we "overshoot" in CO2, farmland, oceans, money creation -- and if you were going to design a pinprick that kills the overshoot it would be hard to design something better than the Covid pandemic. We have to get that the future will be very unlike the past. The people who will get first is those who are already marginalized. We have to go forward in a way that is very different than everything we do. It would be a mistake to think that next year will be anything like this year.

Digitalsista: Where we are right now is a conglomeration of what we did at the past. We should start all over and go back to the root. I dont think when we talk about design, technology design, that we can do anything like we did it before. People who want normalcy are people who weren't living in a marginalized framework.

Johanas: I looked at history around pandemics. Spanish Flu, 3 emporers stopped being emperoar. The black death in the 14th century is credited for ending feudelism. and that's just the pandemic not including the otehr things.

From Marc Davis to Everyone: 11:50 PM @Grace sounds fascinating and needed.
From Lisa LeVasseur to Everyone: 11:51 PM @Grace interesting related talks about that in VRM/Me2B Day--trending towards coops.
From Me to Everyone: 11:54 PM @Jeff, not to mention that Google makes money from advertising businesses.

From Jakki Bedsole to Everyone: 11:58 PM I just wanted to share, I work for an organization where we have implemented a participatory design framework and development process to build an application for survivors of human trafficking and gender based violence where the people who thought of the software product, those informing it, those leading the design and development and those who will be involved in the testing, are all members of the community. This has given us the ability to build AS a community and

WITH our community rather than going to the community to solely check our assumptions. We're at the very beginning of our work together but there's so much value we've already seen, being part of a community, and designing and developing with our community. It's been both empowering and more productive which is cool. We very much have to sit in constant reflection of how we are part of these systems that harm our survivor siblings and communities, and how what we develop needs to fight and not perpetuate those harms.

From JeffO-StL to Everyone: 11:58 PM St. Louis, MO USA was a model for overcimng the Spanish Flu and became a precident model for the management of such this! Go StL!
From Me to Everyone: 11:58 PM at a Europe friendly time, please Johana

Dee: When we talk about marginalized communities, there's a problem with native indigenous women going missing and are usually murdered. You're telling me that these people have 10X probability of these women being murdered and nobody knows where they are? People who are marginalized don't have a voice at all. How are you reaching out across the nation? The technology that we have and develop is made for people who are already wealthy. We don't cater to how these communities could use the technology. I met relatives who live on the reservation. I just typed it on Google Maps, but they don't have street names. It was a surreal experience. Somewhere 20 hours away, my privilege was so embarrassing but I was happy to see that my technology privilege is so different.

From JeffO-StL to Everyone: 11:59 PM https://www.businessinsider.com/history-of-how-st-louis-vs-philadelphia-treated-1918-flu-pandemic-2020-4

From Celine Takatsuno to Everyone: 11:59 PM @jakki awesome
From JeffO-StL to Everyone: 12:00 AM https://www.influenzaarchive.org/cities/city-stlouis.html
Fro John Jordan to Everyone: 12:01 AM 15 mins
From Celine Takatsuno to Everyone: 12:01 AM thank you for that @dee

Jakki: In our organization for survivors of trafficing and abuse, building tools and resources for our community has been productive because we've beena ble to work with our community and with each other as we build. Hundreds to thousands of people and hopefully growing all the time.

Johannas: Practical advice anyone? Resource constrained for a long time. How do we think about this. how do we bring in these people at this time?

Grace: Take on interns from marginalized communities and pay people from areas of the world where it's cheaper to hire those people.

Digitalsista: There was a place in DC where we were sharing space and connecting people to the communities that they say they're building for. From startup to big version. Typically, in those moments, I'm one of the only black women who can see it's not going to end well. Sometimes I tell them, sometimes I don't. They don't have the resources. I'm a proponent of what happens in the tech startup framework. But there is a failure in what you're saying. before they get the funding they've already built their core and the core becomes unmaleable.

From Lisa LeVasseur to Everyone: 12:11 AM it's the fish saying "what the heck's water?"
how do we practically work with the reality of our blindspots?

Marc: Have the population be stakeholders in your enterprise from the beginning. Also represnet the popuations that you want to talk to. Standard: Talk to and involve people who are different from yourself.

From Celine Takatsuno to Everyone: 12:11 AM @johannes it's terrific that you are aware and seeking perspective. but diversity of thought isn't necessarily diversity in hiring. and, even the best funded companies fail to think about harms or impacts outside of their intended ones. look at zoom - with the ceo saying they simply "never seriously thought about harassment"

JeffO: This thing takes me back to an experience, I spoke as a parent to a school community in 1994, and I represented a professional career in technology. I said it does not matter the color of your skin, your head pouring into these tools carry value. I didn't impart to them that there are prejudices… but technology is agnostic in the ability to contribute to software and I hope the rewards come back.

Kaliya: At least 2 different things within community are happening to improve diversity equity and inclusion. Myself and Shannon are going to be co-leading an ongoing learning group to help leaders increase capacity and Lisa is also doing something in this area.

Lisa: We have very little diversity in the P2P alliance and I had this sudden feeling we are doomed. I've been seeking information from my mentors and there's a woman out of Georgetown University and she's put together a custom training. she said you have to build the culture that you want and it's not just about diversity and inclusivity and you can't just say, you have to be. I'm thinking about opening up that course to the whole community of how we want to be, how we want to treat each other.
Yes thank you @digitalsista! These conversations are essential and I'm so glad we're holding these spaces!

From Celine Takatsuno to Everyone: 12:17 AM exploitative. and accepted. sigh.
From Shannon Casey to Everyone: 12:17 AM I'm offering a session tomorrow with Infominer on effective connection/communication (NVC) This topic will support better understanding where we might have blind spots.
From JeffO-StL to Everyone: 12:17 AM Relative value though sometimes. A few US dollars is a bunch "over there" sometime too.
From Marc Davis to Everyone: 12:18 AM NVC rocks :-).
From Lisa LeVasseur to Everyone: 12:18 AM ohh nice @shannon we should do NVC training every iiw!!!!

From Me to Everyone: 12:18 AM That is one perspective. The other perspective is those people would have no way to make so much money in their society. I have people on my team who make double and triple what their neighbors make. That's not exploitive of those people.

Digitalsista: We should be aware of the way in which that we take advantage of societies where people are paid less because we don't want to pay US wages. We need to take care of our framing.
We need to continue to consider how to build these systems from the ground up.

OAuth Metadata: Mix-up Machine?

Session: 12J
Convener: Daniel Fett
Notes-taker(s): Daniel Fett

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

A Mix-Up Attack on OAuth is an attack wherein the attacker manages to convince the client to send credentials (authorization code or access token) obtained from an "honest" authorization server to a server under the attacker's control. In this session, we discussed the risks introduced by new OAuth extensions such as Metadata, PAR and JARM.

Notes: https://danielfett.github.io/notes/oauth/Mix-Up%20Revisited.html

Cards Against Identity

Session: 13A
Convener: Justin Richer

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

What Is A Test Credential?

Session: 13C
Convener: Gabe Cohen (Workday)
Notes-taker(s): Nikhil Wadwa

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

At WD we have been trying to standardise test credentials tied to our VC specs We use only as much JSON-LDs as much as the specification requires

An issuer might want to issue credentials with different levels of Trust
Option 1: Type
Option 2: Status: downside is that it relies on another WebService, have to do another lookup
Option 3: Schema: Another idea is to register a separate schema
Option 4: Change the specification itself - anyone can implement it easily - has to proposed to W3C working group

Another point is that it is up to the verifier whether they trust it or not

What is a Test Credential? At Workday, our customers are asking for test credentials, or provisional credentials, or any other type of status We would like to come up with a standard mechanism for creating non-production credentials

It's important to root the trust in the issuer's signature, but even within that we might want to have different levels of trust.

The most straight forward mechanism might be to use LD with a TestCredential type. This would be an immediate way for someone consuming the credential to see that it is a different type.

A second option would be to modify the credential status property, which is used for revocation checking, but this could also allow for other types. We don't want to require another call to get the status type.

The Credential Schema property. We've appended a status matrix variable to the schema ID to indicate the credential type. This also allows us to not create multiple schema types.

Fourth approach would be a classification field in the Verifiable Credentials specification. This would make this widely known and not a custom extension. This would need to go through the W3C for approval.

Keith - Maybe we'll need to do some integration. The customer needs to issue test credentials in order to verify that everything is working, but we don't want those credentials to be accepted in the broader ecosystem.

It's up to the verifier whether they accept it or not.

Rory - JSON-LD extensions don't need approval by a centralized governing board, but there's a concern that external verifiers, like the Universal Verifier, would just ignore any "test" extension property. That's why we added it into the schema URI, since that's the semantic backing of the credential.

True Self-Sovereignty: What Will It Take?

Session: 13D
Convener: Doc Searls
Notes-taker(s): Scott Mace

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Doc: I saw before what Dave's topic was. He moved the ball way downfield. Bruce Caron is a novelist, wrote a series of 3 books, one of his characters is encouraging development of new software that will change everything. He says to its developers I invite you to think fundamentally. Here is the first one: <https://archive.org/details/junana/mode/2up>. Iain Henderson sent out to many of us a link to the new MyData paper that lays out the field as it now exists. That field is still top-down. Screen shot of Dave's slides. Fully decentralized system. Spotting economic opportunity slide. What we have now are distributed systems that don't follow Dave's principles. I think they are a high hurdle but not a wall for developers. I started Project VRM really here at IIW in 2006. Helped start IIW itself in 2005. Project VRM is a one-year project that is now in the 14th year. Joe Andrieu thought we should be a point of integration of what's ours. Not just data. People are the real edge. Our theory, free customers are more valuable than captive ones. Gets us to something that works like magic and does better signaling than supply and demand. The book I wrote about this, the Intention Economy, came out in 2012. Intentcasting came out of that. None of that has taken off. But for lack of what we're trying to do here. Project VRM begat Customer Commons, doing for terms we would proffer what Creative Commons did for licenses that artists might have. We've done some work on that. We created IEEE P7012 WG. A number of us in this call are on that. A standard for machine readable privacy terms. Here's an important thing. The IEEE in the person of John Havens and others approached Joyce and I for giving the machine readable version of personal privacy terms. Scott's our note taker there. We're making some headway now. JLINC Labs is a P2P protocol to allow party A and B to have an agreement. An active WG. Our chair is David Reed. Authored end to end principle design embodied in SMTP, IMAP, other things we depend on. Also Project VRM begat the M2B Alliance. I see M2B as the inheritor of Project VRM, which is a wiki and a list.

Lisa LeVasseur: I come from a standards background in cellular. I thought all we needed was a spec compliant with the principles we hold dear. We are creating a certification criteria and will start testing connected products. Been doing this for about a year. Very close to having MVP of our specification. There's a lot under the hood, so we're breaking it off in bite-sized pieces by listening to what everyday people want. We do not reflect their understanding who think identity fraud and theft of credentials are the most important thing. Most people don't understand there's another kind of currency in the world. Maybe it's ads. Will go on a journey together with people.

Doc: What Lisa is doing is still new. The title of this is what's it going to take. We need the invention that one look and you got to have it. I knew the original web from links, but it wasnt until I saw Mosaic demonstrated, the web in a graphical way, I learned HTML, owning searls.com. I had to be there. It was one of those things where it was a demo sell. That's been true for many of us with a lot of other things. I couldnt get Joyce to use a phone until the iPhone. Timothy wrote a piece the other day about the wallet. We use in everyday world, could also use it online. Complies with all 7 of Kim Cameron's laws he wrote in 2004. I have a wallet, haven't used it. Dave, what gives you hope with that right now?

Dave Huseby: Six principles of user sovreignity that we apply to nine problems of distributed computing. My hope is that with these talks about principles and the problems, we could get on the same page, in terms of looking at existing systems and accurately judging them whether they are user sovereign. I am no longer

hopeful that existing systems will be reformed. I won't change Facebook. Every day at 5am I write more code or thoughts. Wanted to build a model where I could hold myself accountable. To design a system that resists corporate capture, I have to follow these principles. Also helpful to enterpreneurs to make money in a way that is compliant with the IIW conscience. We come to IIW all the time and express these wonderful values. Every time I dig into a company in my role at Hyperledger, companies compromise to make money. I wanted to put a stake in the ground and call bullshit.

Doc: You spent 3 long sessions on exactly this. Put together a bunch of principles and goals.

Dave: Just to hold me accountable.

Doc: Grace wrote, it's self-immolating before our eyes. A majority of people don't want contact tracing in their phones.

Adrian Gropper: I agree with Dave. Thinking this will be solved by private interests is a fiction. A few of us Rebooting Web of Trust, titled Will SSI Survive Capitalism? In the MyData white paper, I don't see how we achieve the Huesby test in a commercial framework. Some of it was discussed in a session bvgfoere this. It's the separation of concerns problem. If they want to be authorization and storage server, it's making the authorization server independently chosen. In Europe, banks forced not to have a captive credit card. As far as I can tell, neither small operators nor big platform vendors have any interest whatsoever of damaging the business model that mushes authorization and storage server. The entrances can be sold for a lot more money than traditional surveillance capitalism. The benefit of being the gatekeeper and seeing the information. The Post Office and the telcos, those days are gone. This is the elephant in the room for what you and Dave are talking about.

Doc: I scanned the MyData paper. Looked like an incremental move in our direction, but more of the same. I think we're going to have to be truly disruptive. We do them what the internet did to AOL and CompuServe. Will take a thing. The browser did it. Maybe taking the authorization server and ubiquitizing it somehow.

Cam Geer: Transaction analysis is valuable because it's concrete, based in fact. At PayPal, we talked about that internally a lot.

Kyle Den Hartog: Comes down to the economics of computation and the time to manage it. Why did email naturally centralize? It's cheaper for a centralized service to manage all that, economics of scale. Second, the amount of time I have to spend to manage it. I'm also the lazy user. How do we develop around the lazy user so they can manage on their own?

Doc: Spam had an awful lot to do about it. Email was too open. In my case, I ran my own mail server from 1995 until last year. Bad guys set up something inside of it and used it to spam the world. SpamAssassin couldn't do the job. Contracted it out to RackSpace. I've got a contractor who is handling that for me. But you're right, the computation is cheaper. The big back end for all kinds of stuff. AWS. Zoom is using AWS. That's how they scale.

Adrian: Yes there's computation cost to those running their own auth server. But the problem of configuration, can it be inherited from someone who can choose. Choose your caucus and inherit complicated policies. Then the two dimensions Kyle mentioned can be separable.

Doc: Something Grace said is important. We need to work on these things together. Easy to gather people in conversation. Hard to get developers to collaborate. There is not one breakout thing yet. VRM is a

terrible name in the first place. Someone else came up with it. I think M2B is better than VRM. Not just consumers. I've been troubled by the degree the term self-sovereign by Devin 10 years ago, the idea we should be in charge of ourselves. 90+% of the SSI talk has been about big companies. How about us working together?

Grace Rachmany: I wrote a whole book about how we work together. We don't even think of ourselves about being inside a community. Our language is competition. Open source has disproved that quite a lot. Women tend not to operate that way. The system is tilted away from collaboration and toward winner take all. Everything can be resolved in communication. Social distancing will further fragment our community. Recognize ourselves as part of a community, even with competitors. We're not competing for anything anymore.

Doc: I know of at least two intractable conflicts in the last 2 days resolved exactly that way. I already know what you think. In both cases it got worked out because they talked. Self-sovereign, what Devin meant about that, as a teacher of mostly little kids, everybody learned on their own, and share it with each other. Wrote a piece for Linux Journal about kids teaching each other. The word fail to them means first attempt in learning, rather than competing for grades. In the first 25 years of the internet, we kind of ignored the individuals. Survivalists own this sovereign thing as well.

Grace: Our ontology is so prejudiced. Everybody learns alone. We speak that way all the time.

David Huseby: Adrian's comment not able to build fully self-sovereign company. Timothy Ruff, etc., myself, we think the correct model is an edge service. If you are doing a function focus on what not who, skip identification and go straight to authorization, there is a way to make money. You need standard protocols and standard data formats. Spent political capitals before W3C in Amsterdam...if a company is dedicated to principles of user sovereignity, you don't have to compromise.

Adrian: Where does separation of concerns come in?

David: If I don't need to do anything about you...I'm bumping up against NDAs. There is a lot of theory about this, people building companies around this.

Adrian: Your car can avoid other cars. As long as you make the car, applies to Apple/Google coronavirus search, Apple and Google want to control the app store. You can make lots of money on all aspects of this, including being the operator and data storage, but if you won't introduce a protocol in the middle of your own platform and introduce substitutability in the middle. Nothing in cars.

David: Not true. Automotive grade Linux. We'll see. I know what you're saying Adrian. It is about protocols and standard data formats.

Adrian: I'm saying it's about separation of concerns.

David: I would introduce it even in my own company.

Adrain: Change your credit card without changing your bank.

David: I do agree with you Adrian. Just using different words.

Nadar Helmy: The point Dave made about spotting economic opportunity, making it more lucrative to provide an edge service. Doc to your point on the human side, no barrier to entry, a no-brainer to join via social or privacy aspects. They have to work in concert. Without economic incentive it's dead in the water.

Phil Windley: Sovereign raises hackles with some people. I talk about autonomy. We are autonomous by default. We give it out in certain circumstances to do things. On the Web, we are always in someone else's administrative system. Autonomy starts with architecture. That is the key thing we have to get right. So it won't get hijacked later on by even well-intentioned people who make a mistake.

Doc: Example of architecture?

Phil: Pure DIDs, an architectural feature, necessary but not sufficient, reduces our need to be inside someone else's administrative domain. Structural design that makes us autonomous by default rather than administrative by default.

Kyle: The direction I was thinking as the counteraction for management. From a development perspective I haven't figured out how to do that. I want users to be able to select a trust framework, like a CA, root certificates. We've gotten close many times, but there's always one slipup that manages to push us in the wrong direction. It's cheaper for a business to run software on my device rather than running it in the cloud. It takes a perfect storm and that perfect storm can go away very quickly.

Marc Davis: When the internet started, meant setting up your own server, creating your own domain. Delegating your autonomy to services that handle all that complexity resulted in us losing that autonomy. Replacement systems would have the simplicity we have today with the autonomy that was once lost. Dave would say a server that handles all that. That's the big challenge. The complexity has led people to sacrifice autonomy for simplicity.

Doc: I haven't really delegated my authority over my email. Just jobbing out something to a substitutable service. Substitutability is the key thing.

Marc: Gmail is not just managing your email but reading your email. That's the tradeoff. The terms are unfair and don't tilt toward autonomy.

Kyle: One of the things I've realized on this, my idea for the longest time, the router is the one thing that's held up. People have to handle their own routers today. I would run my own cloud agent in the router, a $200 device that's a Raspberry Pi. ISPs still want to manage this for people, still. I want to tackle the router market to make this easier.

Doc: I own the Santa Barbara router. The one in NY is rented from Spectrum. I don't have a sense of running that one. I have a Eero (sp??) mesh wi-fi here, set to dumb. Eero owned by Yahoo. Hacking that is a real important thing. Moving from dumb endpoint out to rest of world is critical. How to do that I don't know.

Adrian: The Freedom Box project is exactly that. A noncommercial thing. A bit of an ability to inherit from others. Will take another decade to make it simple. Has to be done as a non-commerical thing.

Doc: Johannes Ernst and Marcus Sabadello do this.

David: All my traffic is always over the Tor network. Throws away the sandbox at the end of the day.

Doc: Tor just slowed the shit out of everything.

David: I always turn the safety stuff off in the Tor browser. Cookies can track me from one page to the next, but there's nothing persistent, forgets everything at the end of the session. I can browse the web unfiltered and still sleep well at night. Tor is the best solution we have now...Kyle said something about routers earlier. Some people are asking me about this 5am project. The hope is if it's possible to use a fully

decentralized solution for discovering other nodes, and also to design a protocols, the Last Known Wherabouts protocol, to reconnect in a mobile, disconnected world, without a DNS system in a decentralized way, imagine a router that looks at IP addresses are noise, picks out the signal. That will then get us fully independent of a naming system. Zucko (??) triangle flattes to a line.

Adrian: How is 5G going to factor into this?

David: Light the towers on fire . :)...I want to reinvent the Web from scratch. Maybe it's something that grows out of the wallet.

Doc: JLINC has something outside the browser. Look at what they've got. John Wunderlich is in Toronto.

David: Iain is in Scotland somewhere. I said earlier in my presentation whatever solution we build should be app-based. App users are much larger than the web now. An existential threat to Mozilla. Maybe we should be looking at apps.

Doc: Maybe the Web is AM radio.

David: Network news groups still exist too. Whatever we build next, just to hold myself accountable as I write new systems. My biggest criticism of DID com is that it's HTTP REST-based...how to route packets through a network in a privacy-addressed way that doesn't rely on static IP addressing or naming. The biggest problem with TLS was it tried to be agnostic. I'm coming for DID COM. I'm going to light it on fire, we need to make it better. Slowly building a coalition. The new version of MegaOm or Group Noise (sp??) we would be on to something. A routing fabric that is anonymous and private by default.

Jim Fenton: The problem I have with apps, I feel I have so much less transparency about apps on my mobile devices than I do on the Web. I use privacy-enhancing browser plug-ins. I don't have those opportunities with my mobile devices.

Kyle: One of the things worth mentioning here, the DID based on routing layer is where you ultimately do have to start. You do have to push down to that layer but you're fighting protocol legacy aspects of it. As a protocol grows in size, it becomes harder for it to die. Harder to change, harder to replace.

David: I don't disagree. There is a phone from Purism. I had a hand in designing when I was at Mozilla. A phone with a real security story. Decentralized, encrypted communication. It's a step in the right direction. It runs stock Linux. It has an app ecosystem on it. Matrix, I like for a lot of reasons. The Libram 5 phone and Matrix infrastructure is a step toward decentralization and increasing user sovereignity. I didn't even get a free phone.

Jim: What was the one a few years ago?

Doc: There were a lot of those.

David: Firefox tried to do it, but moved away from it. A $7 smartphone in India. Ran Firefox OS. Became Tor WiFi router.

Doc: It was loved by a lot of people in the less-developed world.

David: Google gave away Android phones for free for $100 per phone to keep us out of the market.

Doc: We haven't talked about Inrupt or what TBL is doing with Solid.

David: I love what TBL is doing with Solid. What he's acknowledging is we need standard protocols and data format around our data. But that's just one slice of a pizza. I sent you a phone book of a email to you the other day. There are more problems to be solved. He's solving the persistent data problem which is only one of nine.

Adrian: The session I did yesterday morning was about the paper about Inrupt and Solid. I put a link in the chat. It is philosophically exactly the right thing to do, but not doing the standards. I know from people that have worked there they could be doing. It's a shame.

Doc: RINA is a forklift change that's probably not going to happen.

Cam Geer: I sent you a link.

Doc: They're in Boston

Saved Zoom Chat:

15:32:32 From David Huseby : LOL
15:32:42 From David Huseby : Phil Windly, the radical fighter
15:33:23 From Lisa LeVasseur : didn't know you were here Dave
15:33:40 From David Huseby : I live in Summerlin
15:34:38 From Lisa LeVasseur : huh.me too.
15:34:54 From David Huseby : 215 + Sahara
15:35:08 From David Huseby : Traccia
15:35:18 From Lisa LeVasseur : 215 & lake mead...
15:35:29 From David Huseby : ahahaha
15:35:34 From David Huseby : we're basically neighbors
15:35:38 From Lisa LeVasseur : yup.
15:35:50 From Lisa LeVasseur : I think joyce mentioned that to me last year, now that I think about it.
15:35:53 From David Huseby : awesome we have to give each other corona virus sometime soon
15:35:59 From Lisa LeVasseur : exactly.
15:36:59 From Lisa LeVasseur : love that background, Doc.
15:37:57 From Micah McG : http://blog.harvard.edu/vrm
15:38:24 From David Huseby : we're there now
15:38:54 From Timothy Ruff : Get a room ;)
15:39:06 From Micah McG : Oops sry blog link not working
15:39:46 From Micah McG : http://customercommons.org/
15:40:40 From Lisa LeVasseur : https://standards.ieee.org/project/7012.html
15:42:07 From David Huseby : :)
15:42:41 From Jim Fenton : SMTP is end-to-end? News to me…
15:42:55 From Micah McG : https://www.jlinc.com/technology
15:44:28 From Micah McG : https://www.me2balliance.org/
15:48:11 From Lisa LeVasseur : two pieces of kindling for that: (1) socializing the harms dictionary, and (2) getting the score or a label on products
15:49:54 From dsearls : Dave: "get on the same page"
15:50:01 From Grace Rachmany : it doesn't look like we will need to burn everything down-- it's self-immolating before our eyes.
15:50:19 From Lisa LeVasseur : yeah--sunlight is disinfecting.
15:51:26 From Lisa LeVasseur : (oh god....pls forgive the completely unintended connection to our prez.)

15:51:32 From Grace Rachmany : I think that you need to be careful about "making money" as a primary driver.
15:52:02 From Cam Geer : with a clear principles to build the right tools
15:52:09 From Adrian Gropper : q+
15:52:25 From Lisa LeVasseur : are those principles published? pls share link
15:52:38 From Grace Rachmany : This is also extremely difficult to build. I've been working with some of the projects that are trying to do this and from what I can see there are a lot of good reasons why this is incredibly difficult technologically.
15:52:44 From David Huseby : I am a purpose-driven purpose
15:52:49 From David Huseby : money means very little to me
15:53:26 From Dee Platero : @David are you planning on doing more sessions? I would like to hear more about purpose-driven development.
15:53:27 From David Huseby : @Lisa, they aren't
15:53:36 From David Huseby : I will be putting them in the notes
15:53:45 From David Huseby : and I'll drop them on my web server later tonight
15:53:49 From David Huseby : I will reprise my talks tomorrow
15:53:52 From Lisa LeVasseur : thanks!
15:54:09 From David Huseby : I disagree with that
15:54:14 From David Huseby : a commercial edge service
15:54:16 From Grace Rachmany : +1
15:57:12 From Lisa LeVasseur : I will also mention that no current product is poised to fulfill the Me2BA best practices.
15:57:49 From Lisa LeVasseur : Virtually all fail with not allowing individuals to manage the Me2B Relationship, or to specify the terms of the relationship.
15:58:43 From David Huseby : I can tell you exactly why it centralized
15:58:53 From David Huseby : my nine problems of distributed systems tells you
15:59:37 From Jim Fenton : Agree with Doc that spam had a lot to do with it. Dealing with spam is much more effective at scale.
15:59:43 From Grace Rachmany : @David, agreed. This is very difficult to develop. I think there are some profound efforts going on right now, including your work. These are difficult problems we need to work on together.
15:59:55 From Lisa LeVasseur : Going to jump to Kaliya's session. Great discussion--hope someone's taking good notes for the rest of it!
16:00:48 From Gabe Cohen : They just signed up for oracle cloud!
16:01:01 From Gabe Cohen : https://techcrunch.com/2020/04/28/in-surprise-choice-zoom-hitches-wagon-to-oracle-for-growing-infrastructure-needs/
16:01:27 From David Huseby : I bet Oracle use pricing to woo them
16:01:31 From David Huseby : free for one year
16:01:33 From David Huseby : or whatever
16:01:53 From David Huseby : with the CNCF and kubernetes standard, the underlying cloud is mostly irrelevant these days
16:01:58 From Micah McG : Adrian Grooper: if configuration is shared — great pint!
16:02:08 From Micah McG : *point
16:04:21 From David Huseby : my 5am project is about a fully user sovereign, fully decentralized collaboration tool.
16:04:46 From David Huseby : secure scuttlebutt + git + mailing lists + twitter + facebook + jira
16:04:51 From Kyle Den Hartog : @Dave, I need to follow up with you later in the gardens to get the low down
16:05:05 From David Huseby : @Kyle, I'll find you

16:05:08 From David Huseby : I know where you live
16:05:21 From Kyle Den Hartog : The bottom of the world :)
16:05:48 From dsearls : Grace: "Everything can be resolved in communication"
16:06:00 From Dee Platero : ^ +1
16:06:10 From Nader Helmy : I'd like to know more about the 5am project Dave. Fully supportive of the concept
16:07:57 From Tom Jones : montessori education
16:08:01 From David Huseby : @Nader it is largely theoretical at this point. But at least I now have a set of principles and an understanding of the problems that need to be solved.
16:08:15 From David Huseby : +1 Tom (my kids are Montessori kids)
16:08:38 From Marc Davis : The internet came out of government funded research, so one issue Doc seems to be addressing is the funding mechanism for developing a working self-sovereign architecture. The other question I have is if that self-sovereign architecture is layered on top of the web, which is layered on top of the internet, or is it replacing the web layer, or also replacing the internet layer?
16:08:39 From Tom Jones : My wife & I started a school
16:09:07 From David Huseby : burn down the web
16:09:12 From David Huseby : can't use the web
16:09:23 From Marc Davis : @David Huseby. I knew you'd say that ;-)
16:09:49 From Tom Jones : Just revert to ip - build up from their - trust over ip
16:09:57 From Dee Platero : As a new developer getting into the identity space - where do you suggest I start?
16:10:22 From Grace Rachmany : Internet came out of the government's need for an anti-fragile system and the concept of distributed computing was the way they wanted to do that. The internet has become fragile because of the centralization of a number of services.
16:10:37 From dsearls : https://www.linuxjournal.com/content/kids-take-over-0
16:10:52 From Tom Jones : The only centralization is the dns - what's wrong with that
16:10:58 From dsearls : That's Devon Loffreto's project. Actually his family's project.
16:11:16 From dsearls : Key point, Grace.
16:12:04 From dsearls : I've always wanted DAs: disclosure agreements. You have to tell others.
16:12:13 From Grace Rachmany : Exactly, NDAs and profit-making come out of a system that puts self-interest in front of common good. Common good must be slave to the common good.
16:12:15 From dsearls : Open source is that.
16:13:10 From dsearls : I feel like I'm Adrian's Hors d'oeuvre tray. :-)
16:13:39 From Marc Davis : So does the development and deployment of a self-sovereign architecture need to be developed within structures and processes that are not corporate, but more of a collective or coop where economic incentives are also collective?
16:15:10 From David Huseby : @Dee you should start by getting radicalized and become an absolutist like me :)
16:15:23 From Kyle Den Hartog : LMAO
16:15:24 From Dee Platero : YAS!!!
16:15:34 From Dee Platero : I'm in :D
16:15:46 From David Huseby : just hang out with me and i'll wear you down until you agree just to get me to shut up
16:15:54 From David Huseby : :)
16:15:56 From Dee Platero : hahahaha!!
16:16:46 From Grace Rachmany : @Marc, I would say yes. We are at the edge of collapse of our existing financial systems and we have an opportunity to define what an economy is, what money is and what it means to provide value. Our current money is almost completely anti-value.
16:17:00 From dsearls : Phil: think autonomous if sovereign troubles you. It's not the default model.

16:17:21 From dsearls : Autonomy starts with architecture. Build it in structurally.
16:18:31 From dsearls : DIDs for example. Necessary but not sufficient. But part of a structural design that makes us autonomous by design rather than administrated by design.
16:18:36 From Grace Rachmany : To Windley's point, it is useful to think about the Cryptographic Autonomy License as a potential structure for that.
16:18:41 From dsearls : Phil, make sure I have that something like right.
16:18:45 From Nader Helmy : @Grace totally agree but I also want to avoid the idea that people on a human level are motivated by economic incentives. I think corporations and businesses obviously are, but I cringe a bit when people describe a "radical" future where people... can monetize their data. I think people are motivated by more organic reasons
16:18:57 From David Huseby : @Grace hodl bitcoin
16:19:35 From Nader Helmy : @Grace I should say motivated *only* or *primarily* by economic incentives
16:19:51 From Grace Rachmany : @Nader, I agree. Our data is not going to be worth much monetarily. We should not have to sell our autonomy for money.
16:20:09 From David Huseby : To Doc's point earlier, it wasn't the web that ended AOL. To be more precise, it was Mozilla Firefox
16:20:10 From Grace Rachmany : and I also agree that people aren't motivated by economic incentives nearly as much as we pretend.
16:20:33 From David Huseby : it was open source software designed to be 100% standards compliant and respected users' interests.
16:20:38 From David Huseby : that's a model we can replicate
16:20:45 From windley : Our default model for the web was one of location.
16:20:48 From Kyle Den Hartog : +1
16:20:50 From Grace Rachmany : People are only motivated by economic incentives up to the survival level. When people want to get rich, it's usually about something like security or status, not about economic incentive.
16:20:59 From Nicky Hickman : @ Nader - most people didn't used to be paid for their labour in the feudal system, then we had the black death and the scarcity of labour and then people finally got paid for their labour, isn't data similar?
16:21:04 From Micah McG : @David didn’t DSL kill aol?
16:21:23 From David Huseby : the web's reliance on DNS is a major weakness
16:21:36 From David Huseby : don't need DNS for discovery
16:21:39 From David Huseby : or coherence
16:21:41 From Jim Fenton : DNSSEC FTW
16:21:53 From Grace Rachmany : +1 David about DNS
16:22:05 From Micah McG : +1 David about DNS
16:22:26 From David Huseby : @Micah, no. AOL was dead by 2000. The first DSL/cable was ubiquitous in 2001
16:22:32 From David Huseby : Firefox was released in 1998
16:22:42 From David Huseby : AOL's decline started at almost the same time
16:22:44 From David Huseby : sure sure
16:22:52 From David Huseby : correlation is not causation
16:23:09 From dsearls : Note: letting Rackspace handle searls.com mail is not delegating autonomy. It's just handing off work to a substitutable service.
16:23:24 From David Huseby : but I'm almost certain that all web pages working in Firefox was a major piece of AOL losing any value add through providing a curated walled garden
16:23:30 From David Huseby : it was finally safe to wander the hinterlands
16:24:24 From mahod mah : Yes.. AOL fell apart due to walled garden

16:24:24 From Micah McG : @david: sometimes it is;)
16:24:27 From Grace Rachmany : I've seen at least 2 attempts in the DLT space to try to create self-hosting in a distributed manner.
16:24:27 From Marc Davis : @Kyle yes!
16:24:28 From dsearls : Kyle: we all still have our own routers.
16:24:32 From Jim Fenton : @dsearls The fact that you have your own domain gives you a lot more options than the people that use gmail addresses or addresses provided by their ISP.
16:24:34 From Adrian Gropper : That's the Freedom Box project
16:24:44 From David Huseby : @Kyle stop thinking in terms of IP and DNS
16:24:59 From Marc Davis : https://freedombox.org/
16:25:14 From David Huseby : what if your home router used Last Known Whereabouts protocol to maintain statistical connections to the nodes you need to talk to
16:25:26 From Grace Rachmany : The transport layer makes us vulnerable as well, and we haven't talked too much about that.
16:25:27 From David Huseby : IP is just a transport but it is fully dynamic from you perspective
16:25:47 From Cam Geer : +1 grace — on the transport layer
16:25:59 From Micah McG : @david - what about mobile?
16:26:09 From David Huseby : @Grace Tor 100% of the time and sleep better
16:26:22 From Kyle Den Hartog : @David I think that would be amazing to handle it
16:26:38 From Kyle Den Hartog : @Adrian yes it is, that's what make it obvious to me
16:27:16 From dsearls : Adrian: the Freedom Box is a good example of a router with bonus autonomous features.
16:27:38 From dsearls : Tor is another one, using the tor browser with first party isolation.
16:27:40 From Kyle Den Hartog : Wait how is your video so clear over tor?
16:27:41 From Grace Rachmany : The Holoports are also an attempt at making it easy to be a host.
16:28:23 From Micah McG : TOR has become a lot faster lately
16:28:42 From Kyle Den Hartog : Hmm this is convincing me to at least try it again
16:29:30 From Micah McG : The biggest pain of TOR was all the cloud flare captcha2. That's been greatly diminished too
16:30:17 From Micah McG : Anybody using Matrix Protocol?
16:30:55 From Grace Rachmany : That's a bit like how IPFS works
16:31:09 From dsearls : Dave: imagine a router that looks at signal amongst noise. We can be independent of a naming system.
16:32:56 From Marc Davis : @David Huseby and @Kyle Den Hartog, what layers of the current internet and web stack can be used as is vs. have to be replaced/redesigned?
16:33:20 From Kyle Den Hartog : I would assume you keep to the IP layer and redesign from there
16:33:42 From Kyle Den Hartog : I could even see IP layer being replaced with DIDs
16:33:43 From dsearls : Dave: the app world is bigger than the Web world now
16:34:03 From Grace Rachmany : +1 on creating a new infrastructure
16:34:27 From Grace Rachmany : Web 3 is trying to address that and the first attempts are extremely clunky, but that's to be expected of first attempts on anything.
16:34:37 From dsearls : The web won't die soon.
16:34:39 From Grace Rachmany : Yes, also agree with the replacement with some kind of DID
16:34:52 From Grace Rachmany : AM radio didn't die yet either.
16:35:01 From dsearls : Sam Curran had a thing about privacy enhanced routing.
16:35:03 From Nader Helmy : DIDComm is designed to be transport agnostic. it's not there yet but that's the intention
16:35:13 From dsearls : Agree about AM radio. I'm still into it. :-)
16:35:31 From Nader Helmy : please do Dave!!!

16:36:09 From Grace Rachmany : @David, is Secure Scuttlebutt looking towards that type of implementation?
16:36:30 From Phil Windley : wait. format agnostic is ok. but the transport should be opinionated?
16:36:41 From Kyle Den Hartog : To a degree they are. We've been working with Dominic Tarr a bit and he's taken a look at JWMs and DIDComm
16:36:59 From David Huseby : opinionated means that we pick one encryption algorithm and one protocol and don't allow for "negotiation"
16:37:05 From Grace Rachmany : I also worry about the mobile devices themselves...
16:37:12 From David Huseby : like the new wireguard in linux
16:37:21 From dsearls : Jim Fenton on apps vs. Web.: apps are opaque.
16:38:17 From Marc Davis : @David Huseby are you familiar with https://inrupt.com/ and https://solid.mit.edu/ and do you think they don't rearchitect enough of the existing web stack?
16:38:20 From Phil Windley : feels like we've rabbit holed a bit better
16:38:27 From dsearls : Kyle: the DID based browsing layer is where you have to start. A protocol grows in size and becomes harder to die.
16:38:41 From dsearls : BTW, I have friends who are all about replacing TCP/IP with RINA.
16:39:34 From Grace Rachmany : @marc do you have more info on inrupt? I was not really able from their website to understand what they are doing as far as tech stack
16:39:42 From Micah McG : Yes Matrix!
16:40:09 From Micah McG : Sold me
16:40:26 From mahod mah : phil zimmerman's black phone
16:41:35 From Micah McG : Don't be evil
16:41:39 From mahod mah : Standard Oil in action
16:42:30 From Adrian Gropper : Inrupt: https://bit.ly/IIW-SSI-Adoption
16:42:45 From Kyle Den Hartog : This is SSB's take at DIDComm messaging format: https://github.com/ssbc/envelope-spec
16:43:34 From David Huseby : @Marc solid is a possible solution for persistent state. But there are 8 other fundamental problems of distributed systems.
16:43:43 From Kyle Den Hartog : @Doc is this this RINA stuff you're referring to? http://csr.bu.edu/rina/about.html
16:44:13 From Cam Geer : https://puri.sm/products/librem-5/
16:44:21 From David Huseby :
Nine Problems of Distributed Systems

Discovery
Introduction
Coherence
Public Service
Trust
Privacy
Coordination
Membership
Persistent State

16:44:42 From Micah McG : 👍
16:45:04 From Grace Rachmany : Thanks!
16:45:11 From Wenjing Chu : Thanks!
16:45:15 From Marc Davis : @Grace this website perhaps: https://solidproject.org/

IIW SSI Spotlight: 5 Priority Topics of the SSI-Community

Wednesday 13E
Convener: Andre Judra
Notes-taker(s): Andre Kudra

Tags for the session - technology discussed/ideas considered:

5 Priority Topics of the SSI-Community incl: 1 wallet backup, 2 on-device credential sync, 3 public DID verification, 4 control over public DIDs, 5 third-party identities

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

IIW SSI Spotlight: 5 Priority Topics of the SSI-Community

Even though the global SSI community has cleared significant roadblocks for practical productive SSI use: There are still optimization potentials. Following a list of top topics currently being worked on or collectively deemed relevant, based on the author's judgment call from his work in the SSI domain: 2 in user cluster, 3 in organization cluster, 2 in bonus cluster.

User Cluster
Things that just have to work on the end user side. Reliably, securely and convenient.

Wallet backup – People are used to data being stored (and backed up) in a cloud and they can call or escalate to someone if data becomes unavailable. As pure SSI postulates the use of an "edge wallet" on the user's personal smartphone, this goes along with the responsibility of securing the data on this device, on their own. Usability considerations demand a fool- and fail-proof backup solution, easily activated when installing the app. Policy setting possibilities are advised, e.g. in corporate scenarios, to stop the app from accepting new data if the backup mechanism is non-functional for a certain time period.

Discussion / comments / requirements

Secure data storage working group. How can we store something? See document: https://drive.google.com/file/d/1vf2CsD9QZstzrd6CJ4WFVHw0WKwwNLHf/view
It does not backup the keys, though. Different philosophies for key management.

Backup for a) restoring to same app b) exporting for import to new app/device (portability). Keys have to be stored somewhere else.

May not be necessary to standardize. Could be vendor-specific. How flexible can individual vendors be? Counter: "My thought, though it may not be necessary to standardize it, today it is a need universally. It certainly is worth to have some guideline to enable starting point towards standardizing."

Wallet backup is a crucial problem to be solved in SSI (coming from a federated identity world). Phones may fail, get stolen, get handed over to others. Security perspective: Backup mechanism may become the weak link.

Real-world analogy: What do end users have to do if they lose their physical wallet? They understand they have to go to great lengths to replace everything in it. This can be leveraged!

Secure elements / enclaves are getting accessible on common smartphones (iOS/Android).

Keeping keys in hardware is preferred. Need to be able to rotate keys in an easy manner. Key management is a critical success factor.

Layering required to get to the secure enclave. What goes into the wallet needs to be secured. Making the backup is the easy part, decrypting the key to decrypt the wallet is the hard part. Tying backup to hardware is required, with decoupling the decryption key.

Standard enterprise backup and restore can be applied to a wallet app. If portability is required, which should be considered crucial, a standardization is required. A “switch to another app” should be standardized.

It is a multi-layered problem. Digging deeper is required.

Maybe standard key chains on OSes are enough for now. If the VCs get more important at some point, reconsidering is needed.

Bringing convenience to SSI would be helpful, users don’t like managing their keys. Probably not so aligned with the core understanding and principles of SSI.

Splitting the master keys across different service providers is wise. We will put in trusted entities again (third parties) to ring-fence undesired things from happening. I can choose where to put the keys and change my providers. A standard enables the choice!

On-device credential sync – Especially in the nascent stage of broader SSI use, innovators and early adopters may desire to implement their own wallet app or enhance their existing apps with SSI wallet capability. This will not only be confusing to end users as they may not understand why they need more than one wallet app and credentials are handled in different apps. Best way out is a synchronization of credentials across different wallet apps, with the possibility to filter for relevant credential types within an app and a “master wallet” showing all credentials. However, it is technically challenging as well: Popular smartphone operating systems have restrictions for sharing data between apps, i.e. a synchronization mechanism may not be straightforward to implement.

Discussion / comments / requirements

“Wallet first” paradigm. Your device becomes your wallet. Multiple wallets on a device is tricky: Requires key to be present in those. Might be able to do the querying in an encrypted state. Use of credentials across multiple apps not possible without key sharing.

Secure storage outside of the app is key. Sharing of keys between wallets required. Shared wallet is necessary. Even if apps are operating independently, using credentials from different apps will be required. Cloud service may be the way around, data is not on the device any more!

Organization Cluster

Concepts for integrating SSI into organizational contexts. Trust-reinforcing, easily and flexible.

Public DID verification – In a business context, most organizations will have a public DID on their network of choice for creating schemas and credential definitions, issuing credentials and being generally reachable with SSI mechanisms. In a digital trust network, knowing with whom an interaction is happening is vital. Even though a DID can be public on an identity network, its ownership is not published with it (anyway, it could only be a self-attestation). Hence a trusted public DID vetting process resulting in a verified

organization mapping is a necessity. Properly extended, GLEIF (Global Legal Entity Identifier Foundation, https://www.gleif.org) records have a high potential for addressing this challenge.

Discussion / comments / requirements
Concept is cool, would be beneficial to the community.

Methods to resolve DIDs described here (like DNS): https://w3c-ccg.github.io/did-method-web/ and https://identity.foundation/.well-known/resources/did-configuration/

BC Gov is doing it: https://orgbook.gov.bc.ca/en/home

Option could be jurisdictional business registries, e.g. Handelsregister in Germany.

Not comparable to certificate registration as DIDs are self-registered. Making known who is behind a Public DID is the important part.

Control over public DIDs – A transaction executed via an organization's public DID is always an official, clearly attributable act of this organization. As usual in power of attorney settings, these acts are conducted by natural persons on behalf of the organization. Hence, exerting control over a public DID means power and demands responsible action. The related private keys must be ring-fenced and only made accessible to those who are legally permitted and eligible for speaking on behalf of the organization. The related terms of the SSI community are guardianship, delegation and custodianship, concepts and technology are work in progress. Access-controlled institutional SSI agents are available now to accommodate, in future built-in technical methods for DID control may be developed.

Discussion / comments / requirements
Not needed to secure THE key. Give users a credential to act on behalf of that organization.

Root admin cannot be erased. And should not.

Registering the stakeholders (like company owner) is the root, then delegation of authority is possible. Liaise with Sam Smith regarding KERI.

Delegate responsibility to multiple stakeholders or entities, e.g. assign five keys and three have to be present for transaction execution. Shared keys.

Third-party identities – One of the major SSI design merits, i.e. flexible certificates called credentials, allow a multitude of cross-organizational use cases. They often encompass a data or system access requirement. In a classic world, the organization has to "onboard" the relevant third-party staff members in its own identity systems – a procedure causing tremendous work, trouble, and delays. In case the trust relationship allows, with SSI, third parties may easily be enabled to maintain "their" identities in the target organization's realm. Being closest to who is performing work for a client, representatives of the trusted external service provider can manage who of their staff is active in the target organization.

Discussion / comments / requirements

Give managers credentials which determine what they can hand out. Shared responsibilities. Revocation mechanism is vital for handling this. Revocation solution must be more scalable.

Bonus Cluster

Topics everyone talks about already. Not desired to reiterate here, just if time allows.
Network interoperability – An omnipresent topic is network interoperability, i.e. the capability to manage and use DIDs and credentials of various identity networks, with one wallet app. This is relevant as currently dedicated networks are designed and implemented in diverse contexts. This requires not only trust in the respective network governance but also technical interoperability, ideally based on commonly defined and broadly used standards. Many resources of the community are flowing into network interoperability as of now.

Data schemas – Another often-addressed topic is data schemas for the various application domains. In some industries relevant data attributes, formats and suitable contents may be common knowledge. However, most likely in many scenarios to which SSI is first applied, innovators and start-ups will be breaking new grounds and come up with their own schemas. They have the chance of creating de-facto standards without clunky standardization processes.

Zoom Chat:
00:32:20 Von Andre Kudra : https://docs.google.com/document/d/1xxPkU9wbWkjsSk6VvzFyB3Digb-RjcdwxyF_H5mZ7HM/edit
00:36:21 Von rouven : https://drive.google.com/file/d/1vf2CsD9QZstzrd6CJ4WFVHw0WKwwNLHf/view
00:36:31 Von rouven : Secure Data Storage ^^
00:43:08 Von Eddie Kago : Is there a link to the document?
00:43:18 Von Christopher Hempel : https://docs.google.com/document/d/1xxPkU9wbWkjsSk6VvzFyB3Digb-RjcdwxyF_H5mZ7HM/edit
00:43:24 Von Eddie Kago : Thanks
00:43:27 Von mikhael : Scroll down to the bottom
00:48:46 Von rouven : Ahh - as host, I cannot raise my hand?!
00:49:15 Von swcurran : That's exactly the diffentiation I was making - backup (one app/vendor), portability (across vendors)
00:49:33 Von swcurran : Rouven - no. I was doing q+ on the last call :-)
00:49:55 Von rouven : haha - ok :(
00:50:17 Von rouven : q+
Von Kalyan Kulkarni : My thought, though it may not be necessary to standardize it, today it is a need universally. It certainly is worth to have some guideline to enable starting point towards standardizing.
00:57:45 Von johnnyfromcanada : Ephemeral perfect future secrecy
00:58:52 Von johnnyfromcanada : Perfect Forward Secrecy
01:02:15 Von Kalyan Kulkarni : Another perspective to bring here - we are not far away from guardianship/delegation. This also brings immense importance to backup/restoration.
01:06:57 Von mikhael : No one has mention biometrics. A chip in your arm isn't very palatable, but it removes the need to create 'back-ups'.
01:12:29 Von Kalyan Kulkarni : +1, it does compromise the SSI concepts
01:13:30 Von Ryo Kajiwara : +1 too, even when many people entrust organizations to do key management, we need to have options to do key management ourselves to be "truly self-sovereign"
01:14:10 Von Jonas Jetschni : i agree, this is what i meant with done right - users needs always the options to control there if they decide so
01:14:46 Von Jody : +100
Von Jonas Jetschni : You always need a choice! Most likely a legal framework for this would be fantastic
01:15:09 Von swcurran : Yup - agreed. Rouven said it really well.
01:15:35 Von swcurran : But we need to make it as easy as we can to do the secure thing.
01:19:29 Von rouven : https://w3c-ccg.github.io/did-method-web/
01:19:34 Von rouven : https://identity.foundation/.well-known/resources/did-configuration/

01:22:45 Von rouven : https://orgbook.gov.bc.ca/en/home
01:27:31 Von johnnyfromcanada : For CA vs. Public DID, per a cost-benefit analysis, the “benefits” are roughly the same, but the “costs” are not.
01:38:32 Von johnnyfromcanada : estatus SeLF (on Sovrin) demo yesterday talked about integrating SSI into existing IT-infrastructure. “SSI credential-based access rules are transformed into authentication and authorization objects that can be synchronized and used by conventional technologies like SAML or OIDC.”
01:41:22 Von Kalyan Kulkarni : Its almost dawn here in India :)
01:41:28 Von Kalyan Kulkarni : 5:15 AM
01:43:22 Von Kalyan Kulkarni : Thanks for a great discussion
01:43:25 Von Jonas Jetschni : thank you
01:43:35 Von Ryo Kajiwara : thank you!

Minimum Positive Human Application of SSI

Wednesday 13F
Convener: Sam Curren
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:
SSI, Credentials, Mobile DIDs

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Minimum Positive Human Application of SSI

Top Idea
Credentials for online training

- mobile app to hold credential
- mobile app to verify
- website library to issue credentials after training
- Trust framework to manage schemas and requirements

Useful not only for pandemic reasons, but anytime public service requires some training or certification.
Easy for existing credential companies to support.
Huge benefit is easy verification.

Candidate projects

We hate passwords. So key management without key management.

- app + library that allows for DID based auth in a dev easy way.

Tools to help people protect and help their less informed loved ones about key custody and delegation.
Elder help for fraud prevention.

Social recovery of keys/passwords/etc

- app enabled behavior to close social contacts

End of Lifing that works for all.

- Helping people retire old identities

Avoiding in-person interaction at businesses

- signature cards for a business account at a bank.
- part of the ongoing WFH and remote business transformation.
- "paperless" is healthier post pandemic

UX that keeps you from losing crypto accidentally. (off topic?)

Create a **standard to apply Linked Data Signatures for originating devices** (like cameras).
Embedded in picture with steganography? (hiding data in low order bits)
Maybe a combination of IPFS + supply chain techniques so the data doesn't aggregate in the transmitted content.

Organizational wallets (as a transition path)

- Fanny pack of wallets?
- UX to organize, navigate, discover, search, catalog a gazillion wallets and credentials

K-12 common core **curriculum on identity** principles, practices.

- Content:
    - what's in scope?
- Delivery
    - Homeschool curriculum as a start?
    - how do we explain in plain language, using visuals and stories and games

Interop and Cross Vendor usage.

- Import Export

Agent or **agents useful for a kid**

- focused on education
- Inspire kids to push the boundaries of their knowledge in areas that they are interested in
- Self/Agent-curated curriculum
    - Learn at your own pace
    - Connect to teachers at a level appropriate for you

Natural interactions (The Expanse example)
Emerging Markets with basic problems. Basic identification in a country with poor records.

- A cousin to banking?
    - I like the idea of focus on poor and emerging markets. I think it's important but also forces an inclusive solution.

The **Anthropologically Rich Human model**.

- patterns and templates for identity designers/architects
- show how people think about themselves, interact with each daily, and engage the world.
- e.g.
    - Multiple IDs per family and acting as a family vs a person on behalf of the family (think dinner reservations), and other formal/informal groups.

- Many Faceted IDs and personas per person (I'm Mrs. Smith to my 3rd grade students but Mistress Jim to my slaves).
  - This is a great topic, but it's been hard for me to convince people that they actually maintain multiple personae. It's hard to explain and I always get push-back.
  - Yes. In part because there's a lot of effort starting and ongoing cognitive burden.
  - I often use a few examples that are easier to get: that you want to show a different face, control your privacy in different contexts. Family and school, job search vs work, banking and billing, healthcare and patient.

Kids able to verify identity of others, both online and in person.
Personal Asset tags (**lost item recovery**) SquareTag

Training Certifications

- Getting certifications upon course completion
- Proving completion
- examples: food bank service, team coaches
- examples: disease spread prevention training & pledge

What benefit is required?

- Decreased Frustration with a process (like form filling)
- Increased Safety
- Usability measures (task completion rates, perceived satisfaction, speed of workflow)

Contextual, Trans-silo, On-Demand Groups (Incident Resolution) - Pragmatic Challenges to Forming Persistent, Formal, Credential-Based, Conversations Across Enterprise Boundaries To Solve Problems.

Wednesday 13G
Convener: Eric Welton
Notes-taker(s): Eric Welton

Tags for the session - technology discussed/ideas considered:
hear-ro style incident-response groups, trans-silo onboarding, credentials, customer service

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The discussion was a deep exploration of a multi-business customer-service scenario, exploring key concerns - insights included:

- DID & conversation based customer engagements
  - change task to authorization (ZCAP, VCs) instead of authentication
  - are closer to 'omnichannel' outreach than ever
  - remove major federated-identity obstacles

- it is unlikely that businesses will be pressured to provide improved customer service, but can create draw from within customer service ranks (a tool desired/needed by operators)
- ZCAPs look useful for passing authorization to participate in incident resolution
    - between one organization and another
    - from organization ingress to individual representatives
- the ability share a conversation w/ history
    - a risk - institutions may not want information shared
    - a value - sharing of information decreases cost / expedites resolution
- the key is ad-hoc cross-company collaboration
    - chat & internet tools are massive game changers
    - still an obstacle to "get to chat" for classic customer service engagements

SSI & COVID-19 Health Status Certificates – Ethics, Policy & Next Steps

Wednesday 13H
Convener: Dakota Gruener
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Dakota began by introducing ID2020 and its work.

She then moved to explain that ID2020 has been swept up (along with many others) in the demand for verifiable digital credentials for COVID-19-related use cases. She said that last week, ID2020 and Harvard released a paper about the potential issues with "immunity certificates".

Note: "immunity certificates" is a misleading term (used intentionally because it is the term used in common vernacular). When we talk about immunity certificates, it is meant to be inclusive of:

- infection status, as determined by a recent PCR test
- immunization status, once a vaccine comes online
- immunity, if/once immunity is proven and antibody tests are widely available that are reliable

Immunity certificates offer a compelling opportunity to facilitate an incremental and orderly return to public life. At the same time, they raise a variety of concerns about privacy, exclusion, and inequality.

https://ethics.harvard.edu/files/center-for-ethics/files/safracenterforethicswhitepaper8.pdf

ID2020

Immunity passports are an idea fraught with risk, both technical and in the implementation of the programs.
Policy makers are weighing the risks of such a program against the risks of not moving forward with such a program.
Dakota provided an overview of several risks, as described in the paper:

1. Science of immunity is unproven **and** antibody tests coming to market appear to have low sensitivity and specificity

2. Technical Risks:

    a. The technology used must be privacy-protecting and secure (while we in this community take that as a given, there is material risk that a less privacy-preserving approach be adopted)
    b. Are the solutions we are putting forward ready for prime-time?
    c. Where are we falling short on interoperability? And how does that change the calculus for policymakers weighing the risks and potential benefits of such a program?

c. Policy Risks:

    a. Exclusion — unequal access to testing magnifying inequities; digital divide (those without a cellphone or less tech fluent)

        i. Ubiquitous testing a necessary precondition > important temporal implications. We should be trying to slow programs down until this is met.
        ii. Need paper-based solutions in parallel.

    b. Risks posed by privileging immunity - credential fraud (paying a healthcare provider to issue a certificate that shows you're immune/non-infectious, even if you're not), people intentionally risk exposure to get to an immune status
    c. Necessary scale—there is a long route between the near-zero adoption today, and the level of scale necessary for societal impact.

d. Liability—what happens if someone uses a fraudulent credential

See these slides.
Four priorities that ID2020 considers important for the conversation:

Four priorities for immediate collaboration

1. The development of a standardized schema for describing the state of immunity, without reference to any specific serological method and history of symptoms and testing. This should be developed, ideally, at the international level.
2. Development of fit-for-purpose legislation and regulation, and agreement on a trust framework that clearly defines, within a given jurisdiction, who is eligible to issue a certificate.
3. Agreement within the technical community on an authentication and communication protocol appropriate for this use case. ID2020 will support this through the ID2020 Certification Initiative, certifying only those solutions that are truly interoperable.
4. The establishment of government-led national- and state-level working groups of policymakers, health care providers, laboratories, businesses, and civil society to serve as fora for the consideration of needed measures to ensure the establishment, integrity, utility, and adoption of an effective and civil liberties-protecting certification system.

Discussion Takeaways: (full notes below)

1. Health status credentialing programs carry significant risk. Need to emphasize that within our community and in discussions with policymakers and health authorities.
    a. "We have to know the risks we are walking into."
    b. Inclusion/exclusion could be magnified by technology.
    c. Open debate on whether we should be dissuading these programs overall, or whether we should stand ready to help mitigate risks should the programs move forward.
2. Really important temporal aspect:
    a. "To move fast in this area is not an excuse to ignore the risks."
    b. Important to slow down programs to adequately reckon with risk, create time for testing capacity to increase, etc.
    c. Vaccine is 18 months - 2 years away. Given uncertain science of immunity and unproven technical readiness, might be more appropriate to focus on use of decentralized ID for vaccination records.
3. Trust frameworks / governance critical for any program to move forward.
    a. Question about how to speed up the development and adaptation of trust frameworks as a resource for governments, in order to ensure it keeps pace.
4. Technology *might* be ready for prime-time, but it's not proven.
    a. Lack of interoperability within stacks and across stacks. Will take years to get there, but is complete interoperability necessary in the short-term?
    b. No one can prove the technology scales until it scales.

Drummond asked if there was any connection to the COVID-19 Credential Initiative?

Dakota explained that there is a dialog with some of the leaders of the CCI Use Cases workstream.

John Jordan then described a concept prototype (https://vonx.io/safeentry) work by his team in the Province of British Columbia to demonstrate an approach for digital certificates for essential service

workers. He said that the BC Gov health authorities were not as interested directly in COVID-19-related credentials (testing, immunity, vaccination) as they were interested in healthcare worker certification and mobility testing. They have 100,000+ healthcare workers in British Columbia, so that's a major credentialing and verification task. Those same credentials can be applied to other categories of governmental workers, so that's a larger and less risky adoption population.

Juan Caballero observed: "Also, in the US there is a legal greyzone/permanent leniency zone for liability and regulatory issues around "first responders" and emergency operations."

Dakota noted that first responders is a much narrower class.

Brian Behlendorf noted that vaccination credentials offer a less controversial early adoption option (immunity passports are politically explosive and science is uncertain). There are also many other uses for vaccination credentials. In all of these cases, decentralized (but safe) but fast is better than centralized but slow.

Juan: "People operating with out-of-state licenses, emergency-staffing of hospitals, field hospitals... all of these contexts are required by Covid, disproportionately represented in this credential environment, and luckily loosened from the usual liability restraints and healthcare system... disincentives."

Brian noted that contact tracing is another COVID-19-related technology that is being looked at very quickly—and with lots of controversy. But there are first steps that can be taken with those solutions that can have short-term value.

Dakota asked two questions:

1. Is the technology ready?
2. Can it scale?

Orie Steele answered that, with the technology that he's working with, the issues are not technical, they are about the design and governance policies. He pointed out the analogy to credentials that are already accepted in the travel business for traveling while sick. They are paper documents.

Drummond first said that some tech stacks are working. But he stressed the bigger issue is one of governance frameworks, and that the fastest path to adoption is to implement against governance frameworks from healthcare authorities.

Anil said that the timeline on a vaccination credential is several years. The earliest any vaccination has been developed in the past is four year. In addition, I noted that COVID-19 disproportionately targets communities of color who may have existing conditions, and as such, the possibility of exclusion becomes magnified.

Anil also pointed out that the actual interoperability challenges are far from being solved, and that is still going to take a while and as such to deploy this technology at scale on something where these things need to be solved is concerning.

As such, Anil said that the advice he is sharing within DHS is that "immunity credentials" is an idea that should die quickly due to all these issues. Secondly, essential workers exist in many industries, so we may need much broader applicability of such credentials. Further comments by Anil highlighted that there are

serious risks with COVID-19 type credentials in particular for people that are already marginalized in some aspect of their lives be that social, economic, or otherwise.

John Jordan: “One part of the answer is we continue to deliver services in many ways … and I hope that we can do more for the many small communities we have which will never have the ability to deliver digital services themselves. The province can offer SaaS for example one I call “Permitify” that would allow small communities to fire up their permit store with a few clicks and it is backed by the province.”

Karen Advocate: “Check out my post about the divide between those that work at home and those who are forced to go to work, written 7 WEEKS ago about Seattle: http://letshaveaplan.blog/2020/03/06/not-all-workers-can-stay-home-workers-need-safe-workplaces-paid-sick-leave/”

Juan talked about the path of starting with paper credentials and then showing how they can be done digitally. He also talked about the example of the air travel industry, where the credentials required to move between countries are already well-established, with a cellphone/qR-based fast lane and a paper-credential slow lane that is simple enough to get the plane boarded pretty quickly. In particular, the existing “yellow passport” immunity certificates that are accepted at airports and border gateways today seem relevant to serology/vaccine paperwork (note: they include lots of batch/lot info, signature of administering nurse/doctor, etc.).

Dakota asked John about what other Canadian provinces were working on digital credentials. John said several were, but that few were as progressive right now as British Columbia.

Orie observed quoted Marshall McLuhan: “We shape our tools, and then they shape us.”

Chris Eckl observed that the health authorities that he is working with have realized that many of the problems are not technology problems.

Dakota observed that the concepts of “trust frameworks” and “governance frameworks” are still new to many people. And many of them are developed in very transparent, very slow processes. But she asked the question about how it can go faster?

Orie observed: “HTTPS is a trust framework. Its the green lock in your browser.”
When you buy from amazon.com and the lock is green, you trust that you are talking to amazon.com because you trust that your web browser and the web server, are in the same trust framework…. You trust the system that secures the internet.

John Jordan Noted: HTTPS is a technology that implicates third parties into your relationships so I don’t really trust that .. I just have only the option to participate or not methinks

Timothy asked Anil if what he was saying, “Don’t try to use verifiable credentials for these use cases at all.”

Anil said that no, the reason he’s cautioning that the problem space not a good one for this technology at this point at time. We need to wait until we can be confident in the underlying data.That data doesn’t include the level of impact of this virus on the communities of color and the most marginalized.

They don’t actually look at interoperability across the multiple stacks.
Covid is not the only virus we have ever had to deal with or will ever have to deal with. Without a vaccination this is far from being able to be implemented.

Lack of interoperability within stacks and across stacks.

Karen Advocate: " www.letshaveaplan.blog is to help us transition to a new society - subscribe. Lots of medical and legal and health research sent via MD, JD, RN, PhD friends goes into each piece."

"To move fast in this area is not an excuse to ignore the risks."

Darrell O'Donnell: "We have to know the risks we are walking into." It is best if the technology being implemented is replacing something that's inherently broken.

Anil: From the government perspective, we don't have the ability to "pivot away from a customer base". We can't exclude a portion of the population—we have to serve everyone. DHS thus needs to be risk-averse when it comes to technology. So when you have to roll out a population-scale solution, he prefers the Abraham Lincoln quote, "If I'm going to chop a tree, I first spend five days sharpening the ax." Anil recommends that we spend that "five days".

Dakota recommends that we can use all of this discussion and these notes to help examine the risks.

Orie wanted to thank the whole community for rising to this occasion. He is seeing the level of effort going into the COVID-19 Credential Initiative community, and is very impressed by it.
Drummond shared that the Rules and Governance workstream of the COVID-19 Credential Initiative is highly aware of the risks and is very focused on addressing them. He also thanked Anil for everything he does to help move us all toward government-grade credentials.

Karen spoke to the reality of the digital divide that is very real in Seattle, and that it's critically important not to speculate as to what those on the "other side of the divide" need, but to go and actually ask them. Don't sit in your technology golden castles trying to fix something when you haven't spoken to those communities directly.

John Jordan shared that the Province of British Columbia healthcare organization received over 400 different suggestions for how to deal with the COVID-19 crisis, and that they simply cannot process them all. They also don't have the tools to understand some of the proposals. So please be mindful that when you are offering your help, it is actually difficult to accept sometimes.

Brian Behlendorf offered that we also need to look at it the other way around: how about if the restaurant can prove it was cleaned, or a meat-packing plant can prove it has implemented safe practices.

Dakota thanked everyone and said it has been a great conversation about the risks. She will be feeding all of this back into the partners ID2020 is working with.

Some links to related work is W3C CCG / DIF:
https://github.com/w3c-ccg/vc-examples/blob/master/docs/covid-19/v2/v2.md
https://c19-vc.com/
https://vonx.io/safeentry (Concept Prototype leaning towards essential worker scenarios from the Province of British Columbia) https://www.covidcreds.com/

Zoom Chat Transcipt:
15:49:29 From Dakota Gruener : https://ethics.harvard.edu/immunity-certificates

15:50:35 From Brian Behlendorf : The framing of essential workers may be a much less politically explosive place to start.
15:50:57 From Darrell : Agreed Brian.
15:51:24 From Juan Caballero : Also, in the US there is a legal greyzone/permanent leniency zone for liability and regulatory issues around "first responders" and emergency operations
15:52:26 From Juan Caballero : Man, I wish California were paying attention to the California of Canada on this issue :D
15:53:09 From Brian Behlendorf : We can certainly draw California's attention to it
15:53:19 From Karen Advocate : And US corporations are lobbying to shift COVID-19 liability from employers to employees. Very sad given all of the $$ they continue to receive. Money more important than people.
15:54:13 From digitalsista : Karen it's money more important than human lives which the economy can't exist without.
15:54:14 From Juan Caballero : I was referring in particular to the people who administer and/or notarize on-the-spot test results
15:54:51 From Karen Advocate : Hoping COVID allows us to do a major reset!
15:55:20 From Juan Caballero : People operating with out-of-state licenses, emergency-staffing of hospitals, field hospitals... all of these contexts are required by Covid, disproportionately represented in this credential environment, and luckily loosened from the usual liability restraints and healthcare system... disincentives
16:03:10 From Karen Advocate : From a public health perspective, contact tracing thru technology will likely not be effective with communities that are traditionally oppressed and discriminated against, including immigrants, refugees, low-income, people of color, homeless, victims, traumatized, uninsured etc. Relationships with people they trust will be key to do the work.
16:05:24 From Brian Behlendorf : collaborating with public health authorities on governance is essential
16:05:53 From John Jordan : Kind of my point earlier …
16:06:09 From John Jordan : They already know how to do paper and traditional IT systems
16:06:41 From Brian Behlendorf : (folks this is Dakota's session, let's let her recognize & call the raised hands)
16:06:49 From Drummond Reed : I wasn’t saying that the interop problems have been solved, sorry if there was any misunderstanding.
From Dakota Gruener : Sorry all - didn’t see the raised hands. Will use that going forward.
16:07:24 From Orie Steele : Interop has to be proven with tests… its a measurable thing…. And its remarkably hard to prove.
16:07:44 From Juan Caballero : ^CF our demo table :D
From Juan Caballero : Mass transit commuters, long-commute commuters, non-insured people...
16:08:31 From Juan Caballero : It's an inequality tsunami
16:08:32 From Darrell : Agreed on interoperability tests. DHS used to run a lab that we could use for conformance for some of the OASIS standards (EDXL - Emergency Data eXchange Language). It was very helpful and stopped vendors pointing at each other.
16:09:06 From John Jordan : Yay for Public Service :)
16:09:10 From Juan Caballero : +1
From Karen Advocate : Yes! Disproportionate impact is why I wrote my earlier comment.
16:09:21 From Juan Caballero : North America is very lucky to have you both
16:09:27 From Celine Takatsuno : @juan inequality tsunami indeed…
From Juan Caballero : You know any native speakers of germans looking for work over here? hehe
16:09:40 From Orie Steele : I worry about how digital solutions will further the gap between digital natives, and the rest of us, including those without access to smart phones / technology / healthcare or

funds.
16:09:52 From Juan Caballero : ^ this
16:09:58 From Orie Steele : We shape our tools and thereafter they shape us
16:10:06 From Karen Advocate : Agree with Orie. The divide is getting wider.
16:10:08 From Dakota Gruener : We agree strongly w/ the points everyone is raising about potential inequities of these programs.
16:10:18 From Orie Steele : Marsha Mclueens quote not mine.
16:10:31 From Orie Steele : marshal*
16:10:40 From digitalsista : And some are forced to work.
16:10:41 From Juan Caballero : Marsha McQueen is my drag name
From Karen Advocate : Will the chat be captured in notes? Good stuff to have for digital community to read.
16:11:34 From John Jordan : I was answering the question of what about people without phones just today in a briefing note …
From Juan Caballero : Your honor, I'd like my jokes about drag names stricken from the record
16:13:04 From John Jordan : One part of the answer is we continue to deliver services in many ways … and I hope that we can do more for the many small communities we have which will never have the ability to deliver digital services themselves
16:13:22 From Orie Steele : Totally agree regarding cost of education
16:13:29 From Celine Takatsuno : +1 @Orie @Karen @Brian
16:13:48 From Karen Advocate : Check out my post about the divide between those that work at home and those who are forced to go to work, written 7 WEEKS ago about Seattle: http://letshaveaplan.blog/2020/03/06/not-all-workers-can-stay-home-workers-need-safe-workplaces-paid-sick-leave/
16:14:17 From John Jordan : The province can offer SaaS for example one I call “Permitify” that would allow small communities to fire up their permit store with a few clicks and it is backed by the province
16:19:50 From Juan Caballero : john, can we clone you?
16:20:27 From digitalsista : Thanks Karen. this is so good.
16:21:38 From digitalsista : The most marginalized are forced to work. And John thank you for continuing the conversation here.
16:22:09 From digitalsista : yes. Orie!!
16:23:32 From digitalsista : We shape the tools and when we don't like them any more we throw them out and create new ones.
16:26:40 From Orie Steele : HTTPS is a trust framework. Its the green lock in your browser.
16:28:14 From Orie Steele : When you buy from amazon.com and the lock is green, you trust that you are talking to amazon.com because you trust that your web browser and the web server, are in the same trust framework…. You trust the system that secures the internet.
16:28:44 From John Jordan : HTTPS is a technology that implicates third parties into your relationships so I don’t really trust that .. I just have only the option to participate or not
16:29:04 From John Jordan : methinks
16:29:23 From Drummond Reed : The notetaker is doing his best!! Please help!!!
16:30:21 From Dakota Gruener : Thanks, Drummond! This conversation is moving fast and hard to capture everything. Please help Aiden out.
From Dakota Gruener : https://docs.google.com/document/d/1bKxrhhg_MxENpXWQuFXEfI_djTC-mgaeCwQCJ45AITk/edit?usp=sharing
16:31:31 From John Jordan : Takes time and millions of dollars Anil
16:31:47 From John Jordan : Not helpful to keep saying we don’t care or are ignoring it

16:33:04 From Juan Caballero : Everyone, feel free to add to the notes, add details to your own contributions, etc: https://qiqochat.com/breakout/9/iiw30
16:33:43 From Karen Advocate : Thank you Digitalsista! this is my first time blogging! Kaliya has patiently taught me. www.letshaveaplan.blog is to help us transition to a new society - subscribe. Lots of medical and legal and health research sent via MD, JD, RN, PhD friends goes into each piece.
16:34:58 From Juan Caballero : ^ wow this site is great, kudos
16:36:17 From Celine Takatsuno : yes, thanks for sharing this @Karen!
16:36:31 From Karen Advocate : Thank you Juan!
16:36:53 From digitalsista : I think the key thing missing here is what Anil said. We've had pandemics and viruses before. But the move fast in this one moment is not an excuse to ignore the risks.
16:36:54 From Timothy Ruff : Excellent points, Dakota, Drummond, and Anil.
16:38:00 From Karen Advocate : Thank you Celene!
16:42:13 From Brian Behlendorf : +1 to Celene
16:42:58 From Juan Caballero : +1
From Anil John : +1 to what Orie said about the amazing desire of this community to HELP!
16:43:40 From Celine Takatsuno : Thanks for leading this discussion Dakota, so much to unpack here. These conversations are crucial getting it right.
16:44:09 From Dakota Gruener : +1 to Orie's comments.
16:44:10 From digitalsista : I really wonder who are in those groups.
16:44:22 From Orie Steele : And thank you Dakota for running this session!
16:44:25 From digitalsista : and which communities are represented in those groups.
From John Jordan : https://www.covidcreds.com … there are links to docs with the people involved
16:44:56 From John Jordan : FWIW
16:45:00 From digitalsista : Thanks John.
16:45:51 From Orie Steele : W3C CCG / DIF / CCI the whole community has been working together :) and its been awesome to see.
16:46:44 From Stew Whitman : sorry, bad dog :)
16:46:44 From digitalsista : yeah. I've very anxious by both of these groups based on my personal experiences in this space.
16:47:20 From digitalsista : This what Karen is saying is why I'm so concerned.
16:48:59 From Anil John : @Karen +1 (As the husband of a middle school principal who has been thrown head first into the digital teaching in a community that on a day to day basis depend on the school system to provide breakfast/lunch and don't have computers at home)
16:49:17 From digitalsista : + to what John just said.
16:49:35 From John Jordan : Absolutely … Brian
16:49:52 From John Jordan : https://silvicultureoperatorscreening.gov.bc.ca/
16:49:59 From John Jordan : For tree planting camps
16:50:10 From John Jordan : https://www.farmoperatorscreening.gov.bc.ca
16:50:23 From John Jordan : Temporary foriegn worker for farming ...
16:50:54 From Karen Advocate : Homeless in King County:
https://www.cdc.gov/mmwr/volumes/69/wr/mm6917e2.htm
From Darrell : +1 John - my son is looking at Ontario's equivalent as he heads out tree planting.
16:51:03 From John Jordan : This are just forms right now although the silviculture app looks up legal names from OrgBook BC which its a verifiable credential registry of legal entities in BC
From Kaliya Identity Woman : Please save the chat and put an edited version into the notes
From Celine Takatsuno : yes @shireen and @karen — a lot of voices assume the community service orgs will step in. but they don't have the resources or tools either. tech needs to engage the communities directly and *listen* to what communities say, before deciding (their) tech has the solution .
16:51:23 From John Jordan : I will save the chat!

16:51:28 From Dakota Gruener : dakota@id2020.org
16:51:34 From John Jordan : Chat saved
16:52:21 From Karen Advocate : Thank you!
16:52:46 From Juan Caballero : thx all
16:53:17 From Stew Whitman : +1

Overlays Capture Architecture (OCA)

Wednesday 13l
Convener: Paul Knowles & Robert Mitwicki
Notes-taker(s): Paul Knowles

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Overlays Capture Architecture (OCA)

OCA is an architecture that presents a schema as a multi-dimensional object consisting of a stable *schema base* and interoperable *overlays*. Overlays are task-oriented linked data objects that provide additional extensions, coloration, and functionality to the schema base. This degree of object separation enables issuers to make custom edits to the overlays rather than to the schema base itself. In other words, multiple parties can interact with and contribute to the schema structure without having to change the schema base definition. With schema base definitions remaining stable and in their purest form, a common immutable base object is maintained throughout the capture process which enables data standardisation. OCA facilitates a unified data language so that harmonised data can be pooled into multi-source data lakes for improved data science, statistics, analytics and other meaningful services.

Here is the video link from the session (live demo included) ...

https://drive.google.com/file/d/13yuupet1o_oysdEjM99avsT5aPqs4DY9/view?usp=sharing

Secure Data Store Working Group – Review the Charter, Meet the Chairs, Invitation to Get Involved

Wednesday 13J
Convener: Kaliya Young, Dmitri Zagidulin, Tobias Looker
Notes-taker(s): Paul Knowles

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Input document from

WE are working towards and interoperable Spec for dropbox/Google
"Competing" with WebDAV
"Competing" with ___

Expecint way to mount a thing to /MNT
Replication and syncing.

From a productization it is hard cut out.
file system - entirely different way of storing data - competing with SQL on some level.
Why are we doing this?

Why not focus on one simple aspect.
The engineering choices in order to make work client side encryption. Have implications on all these other layers.

The choices you have to make on encrypting data influence access control and synchornization.

Henus acts of violating layered models.

Tobias - Mattr - New Zealand company. DIF Hyperledger W3C CCG - DID working group. Interested in this technology in general.

Kaliya - worked for 15 years.

Dmitri - favorite subject SDS - living and breathing for 15 years. Vertical stack for
Lead engineer for that - became clear to me - if we are going to have encryption. WE can't add on to it after the fact.
If going to do access controls on SDS - we have to build it in.
As engineer building on lot of pre-spec implementations.
Earlier today's SCIM - user management API.
They definitely need to join the conversation.

Make sure the 4 original "camps" communities - that their interests are met. All the decentralized folks.
Including the European work MyData, MAIDSAFE, Redecentralized folks.

Out of scope Design or Development non-HTTP

We need an Architecture Reference Model
We need Marchitecture Diagrams

Someone - actually a sellable product - what this product does and how it is different then other produtcs.

Unless there is some common terminology - what the “thing” is and across competitive boundaries.
People will only spend money on a thing if there is actually a category.
What we do is that we are extremely different.

Competing about the details…

What is the market going to be called and the
The money was on in the software.

There was a tone of technologies that have to interoperate.
3-4 letter acronyms.

Play around in so many different ways.

Input documents
Ultimately doesn’t matter what the name is
it matters if people use the same thing.
People use it…

MARKET BUILDING opportunities.
Common language.

The market was defined by the reference architectures.
You are right about this. Telco’s Celular - Mobile. Did grow this way and Microprocessors.

Someone hacks something together in the market and it gets solved.
We are going for something like that here defining standard interface.
Question. List from working group.

Encryption of Metadata.
Can indexing work on client side encrypted data.

Some members require indexing to be only encrypted.
Also capabilities for unencrypted meta data.
techniquest - solar and elastic search do for encrypted search - the search terms are hashed.
I think exactly like you are saying - exact matching encrypted storage is not hard.

The Digital Harms Dictionary – Review of the Tool & Its Mission

Wednesday 14A
Convener: Jeff Orgel – Me2B Workgroup Chair
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Harms dictionary based on English speakers, but are different economic groups covered? We don't often think of problems that we don't see. One organization that works with the homeless has a newsletter that had an article title "Sheltering in Place When You Don't Have a Place."

Day 3 Thursday April 30 / Sessions 15 - 22

DIDComm Over Satellite Communication

Wednesday 15A
Convener: Lohan Spies
Notes-taker(s): Gary de Beer

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Censorship resistant communications using DIDComm via LEO satellites.
After COVID mass surveillance may become much more prevalent globally.

Satellite based communications to become much more accessible and useful in rural or disconnected/warzone regions.

https://docs.google.com/presentation/d/1raouqtTNgvIcMXuX0AUvyVixIsl-hBFHiEgVBk5FIvE/edit#slide=id.g7542e3983a_0_210

Use cases:
IOT
Natural Disaster
Humanitarian
Refugee
Censorship Resistant comms
Store/Forward messaging. did:space
Broadcast over GEO - Broadcast Identity ledgers updates

Building UI's For End Users

Wednesday 15D
Convener: Christian Hildebrand
Notes-taker(s): Christian Hildebrand

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Two links shared from Christian Hildebrand for the UI working group:

https://docs.google.com/document/d/1-aOlsj91RXcECiWnaJ1YQr3z42CZOtmKiz5pP6z0qrQ/edit

https://join.slack.com/t/diduxworkspace/shared_invite/zt-dxi5f6t1-J9aixWCPSsmEH4ZTW_ngRA

Supporting Sovereign Insurgencies - Secure Communities For Social Change - Putting Out Fires When It Is Illegal To Do So

Wednesday 16B
Convener: Eric Welton
Notes-taker(s): Juan Caballero (Spherity GmbH, Dortmund, Germany)

Tags for the session - technology discussed/ideas considered:
censorship resistance, communications, encryption, infrastructure, alternative trust frameworks

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Technology projects that came up in the discussion:

- https://ssbc.github.io/scuttlebutt-protocol-guide/
- https://en.wikipedia.org/wiki/Secure_Scuttlebutt
- https://gotenna.com/
- https://www.gotoky.com/

Reference materials

- Accountable anoncreds paper (Dec 2018) - https://link.springer.com/content/pdf/10.1007%2F978-981-13-1483-4_3.pdf
- https://www.goodreads.com/book/show/22107280-blueprint-for-revolution
- https://en.wikipedia.org/wiki/L%C3%A8se-majest%C3%A9
- better biometrics/ continuous authentication http://www.mirlabs.org/jias/secured/Volume6-Issue2/Paper17.pdf

Strategic discussions

- Reputation systems (without consent) as ultimate state monopoly on violence
    - Holochain's "warrants" - a red card that boots someone from the network for crimes against the commons
    - Revocable anonymity (coming from fintech/crypto eKYC discussions) - each pseudonym anchored to a liable party held in escrow until crimes are done
- [Moral] imperative to publish (even if anonymously and on, say, arvix) this work for the common good - it might be urgent in many places to build alternate tech/trust networks
- Alternative trust frameworks → how does that change the architecture?
    - gossip messaging rather than hierarchical messaging systems
    - credentials for access to subset of messages?
    - skeptical counterpoint: insurgents tend to burn all their notes after reading, why risk infiltration with any extra structure?
    - built-in obsolescence, time-bound messaging…
        - what's the UX needed for that
- Local webs of trust (f/CCI/Sovrin conversations)
    - early
- All roads seem to lead back to tradecraft

Low-Tech Solutions – QR Code Wallets

Session: 16(C)
Convener: Lohan Spies
Notes-taker(s): Lohan Spies

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

We are developing a low-tech version of SSI using QR code wallets for end-users. The problem in Africa is that most people lack access to technology or the internet and furthermore we required a solution that doesn't depend on any technology. We ended up creating QR code wallets for users that act as their SSI wallet. COVID status updates are issued as credentials to the QR code wallet that can be verified through a custom-developed SSI Verifier Mobile application. The QR code is then used to access services such as transport, restaurants and many others where verifies can ascertain the COVID status of an individual. Most importantly though is that we need a mechanism to allow economic activity to be stimulated and our solution provides individuals with a low-tech solution while corporates only need to download a mobile application. Restarting the economy requires digital verifiable proof of one's COVID status to ensure the health and wellbeing of all others. Lastly, our solution provides track and trace capabilities that are not possible with any other solution.

For more information please visit www.coviid.me.

Portable Reputation Using SSI

Session: 16E
Convener: Mike Richardson & Geomina Richardson
Notes-taker(s): Geomina Richardson

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Mike Richardson, CTO; together with Geomina Richardson CEO, presented EuroLedger's commercial SSI solution for reputation portability, CAPENA.

They presented the CAPENA pitch-deck and explained the solution, which include a proxy issuer DELEGA@CAPENA, a dapp PORTA@CAPENA and a plug-in, APPIA@CAPENA.

The proxy issuer acts as a notarizer to issue credentials on behalf of upstream platforms, such as eBay or Uber, by interacting with those platforms' public APIs to retrieve user credentials and issue them to the holder, via an Aries agent.

The dapp allows online sellers and buyers to monitor how the ecosystem of digital marketplaces perceives them, in addition to presenting (ie transferring) verifiable credentials based on public ratings between marketplaces.

The plugin is a generic library based on the Aries framework which allow marketplaces who wish to accept ratings from upstream platforms to conduct rating verification requests on demand from users and receive reputation credentials, all with user permission. The plugin will be integrated with downstream platforms allowing them to use credentials in their system.
The system works by issuing credentials (via a proxy or notarizer) to replace the actual upstream issuer: the holder then approves those credentials (which means the keys and other identifiers get written to the ledger in the form of Decentralized Identifiers – DIDs).

Downstream platforms then request a "proof", which is a verification of a user's credentials. It does this by establishing a point to point connection with the user; once established the credentials are presented via the ledger.

Christian Hildebrand shared his previous experience with Personal Management Information Systems and raised specific points on the business model – highlighting the need to work closer with the issuer. Christian proposed an approach related with the concept of trusted store, by which DELEGA@CAPENA, our proxy issuer could provide a recognised seal of trust on reputation portability transactions.

Mark O. Scott was very favourable to the idea and provided potential contacts in the business area.
The participants considered the technology setting and approach was ideal for the use case.

Would you be interested to consult the pitch-deck and find out more about the project, please contact Euroledger at: geominat@gmail.com

Open Discussion on Email, Messaging, & SSI/DID

Wednesday 17A
Convener: Ryo Kajiwara
Notes-taker(s): Ryo Kajiwara

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slides: https://speakerdeck.com/sylph01/did

Comments:

- There is a similar solution that is PGP, but nobody has figured out how to use it
    - There is a DIDComm app that does something close along these lines, but through the use of this app, there were no mentions of "long numbers" by the users of this app
    - We need to have a streamlined user experience, otherwise it would lead to "corporate capture" (as mentioned in the "Fundamental Problems of Decentralized Systems" session)

        - Email might be already under corporate capture; we need to please the great email providers to make them accept a new extension/alternative to email
- There are two different problems/use cases mentioned:
    - Encryption and privacy -> Applies more to person-to-person use case
    - Veracity of the sender -> Applies more to unsolicited communication
- How much cannot be done with existing solutions?
    - Need to dig down on this, but PGP and S/MIME partially solve the issue
- How could we layer this using the existing infrastructure?
    - Using a header extension to carry VC/DID associated information in the current mail headers can be a transitional solution moving forward
- In the personal messaging space, encryption is more important, but in the case of advertising and notification, it gets less important
- The use case where you know each other (-> use case with "pre-established trust") is easy; where we use email today is to send email to a completely unknown person. Can we do that with SSI/DIDs? Are these identifiers stable enough or understandable enough?
    - We might need a (partially) centralized directory to find "addresses" of someone
- Using VCs/DIDs to identify the sender can be thought of as replacing "pre-established trust" with a trust mechanism that can be globally used

Hyperledger Aries – How To Send Messages To An Unknown Receiver – The Out-of-Band Protocol

Wednesday 17B
Convener: Stephen Curran & Christopher Hempel
Notes-taker(s): Christopher Hempel

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slides:
https://docs.google.com/presentation/d/11a633q-90A-TwMWVVb3t93IcuagiQ0uZVt7lfOloZqw/edit?usp=sharing

Notes:
Since there is no existing standard for handling messages without an existing or known connection, there are currently several different implementations.
However, for interoperability it is essential to have a standardized solution.
The Aries RFC 0434: Out-of-Band Protocols is an approach to solve this problem.

RFC Link:
https://github.com/hyperledger/aries-rfcs/tree/master/features/0434-outofband

Identity For All – Universal Declaration of Digital Identity

Wednesday 17C
Convener: Jeff Aresty, Kristina Yasuda, Nicky Hickman, Joyce Searls, Doc Searls
Notes-taker(s): Kristina Yasuda & Nicky Hickman

Tags for the session - technology discussed/ideas considered:
#IdentityforAll #UniversalDeclarationofDigitalIdentity

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Draft Declaration: https://docs.google.com/document/d/1rqf_2Pas8beYXsEmk_kATuWr4gX-J4aa/edit

Presentation Deck:
https://docs.google.com/presentation/d/1mEKNGmAfMhygkf93-6nxPGPdx3mXlyHwU0FYzBFpMO4/edit#slide=id.g846c5da290_0_10

George Fletcher:

- do we have digital identifiers, or do we have digital identities. Importance of identity as a function of context.
- There are things that are 'natively me' but I don't 'own' the attribute, e.g. if there are a group of people who reasonably assert I am a good landscape gardener and they give me a credential, then it still isn't something I 'own'.

Doc:

- Trust is the key word, and the key point of control / decision-making for assertion of specific identity attributes in specific contexts
- Very few will manage our identities directly ourselves - we will use agents, might shift from a federated ID provider to an agent provider
- Portability rights are important underscores the point of control & VC's make this easier than current form of identity management
- Doc: Here is Devon's explanation of Self-sovereign identity, in 2016: https://www.moxytongue.com/2016/02/self-sovereign-identity.html

Nicky: Referenced other ethnographies with a concept of 'dividual' rather than 'individual identities'.
"*On this conceptualisation, we do not have a single coherent person performing different roles as demanded by a changing context, but rather a different person differently constituted in each of his or her interactions with others.*" Smith, Karl (2012) *From dividual and individual selves to porous subjects*, The Australian Journal of Anthropology 23, 54
(see her anthropology homework here: Dividual & Individual Identity)

Kaliya:

- Can't use the same language and as the WB or UN - what IIW mean by identity and what WB & UN to be 'legal identification'.
    - Eric: Important distinction
- In SE Asia Malaysian focus on digital rights, not Chinese way or western way but the Malaysian model, could help resistance to corporate and state surveillance

Eric: SE Asian experience, not clear on the differences between simple useful systems and the hyper connected world's focus on privacy. Balance between privacy and the value of digital services.

Nicky commented on the balance and tension between privacy and value on the one hand & privacy & security on the other. Cryptography alone will not help when people are involved.

Jeff encouraged everyone to add to, and comment on the document.

Discussion re Article 8 - Doc: Human Centric rather than Machine-centric, Eric - right not to be judged by a machine v important,

Will: https://wip-abramson.dev/facebook-erased-me
Eric: should have right to recourse, but no hurdles as with GDPR's right to erasure

Jeff & Kristina: Perhaps in some of world justice groups could familiarise and then try and move out from IIW as a bottom up declaration vs state run top-down. See if ID2020 can take to a broader adoption

Joyce: Feels top down, but a great start for the principle.

Eric: Have we considered the right to lie? Concern that SSI & Credentialing makes falsifying identity very difficult. Use case of escape routes for asylum seekers. Doc commented this is the right to pseudonymity.

Joyce gave the example of construction industry making airtight houses that leads to mould, you need some air in the system. Humanity is messy, the individuals need to be able to work it for their own purposes.

Doc:

- The difference between the natural world and the real world is vast. We are designed to forget specifics after a few seconds. Difference between tacit knowledge (natural world) and explicit knowledge (world of machines).
- Asserting rights is a good way of changing the balance between man and machine.
- Introduce the fudge of the everyday world, eg am I Doc or David? We have to build respect for the tacit into the digital, explicit world.

Eric: = Reclusivity rights
Kristina: Importance of human rights, and the right to choose what you share.

ZOOM CHAT TRANSCRIPT:

14:41:12 From Kristina : If someone wants to start looking at the draft
14:41:13 From Kristina : https://docs.google.com/document/d/1rqf_2Pas8beYXsEmk_kATuWr4gX-J4aa/edit
14:53:24 From Nicky Hickman : Instead of his/her for gender diversity suggest using 'their'
14:54:12 From Nicky Hickman : Is there a guardianship clause? or is that Right to Access
14:54:27 From Eric Welton (Korsimoro) : Article 9?
14:54:32 From Eric Welton (Korsimoro) : I'm intrigued by Article 8
14:54:40 From Nicky Hickman : ooh have they shared the link?
14:55:11 From Jeffrey Aresty : f someone wants to start looking at the draft https://docs.google.com/document/d/1rqf_2Pas8beYXsEmk_kATuWr4gX-J4aa/edit
14:55:29 From Nicky Hickman : Apart from article 1, are there any other 'duties' or responsibilities?

14:55:43 From dsearls : Someone taking notes?
14:56:01 From Kristina : no
14:56:06 From Kristina : any volunteers?
14:57:52 From Eric Welton (Korsimoro) : what are these expected to "kick in" - is there an "age of majority" with respect to digital identity rights?
14:57:59 From Nicky Hickman : I will do it
14:58:15 From Jeffrey Aresty : only in the chat
14:58:23 From Kristina : thank you Nicky
14:58:35 From Jeffrey Aresty : thank you Nicky
14:58:54 From dsearls : Kim Cameron, who wrote the seven laws of identity, calls himself, with his many identifiers, "a committee of the whole." Whitman speaks of "a knit of identity," and how "I contain multitudes."
14:59:13 From Kristina : why would there be 'age of majority' in digital identity rights
14:59:16 From Kristina : ?
14:59:24 From Kristina : because there is article on guardianship?
15:00:19 From dsearls : Devon Loffreto, who coined "self sovereign identity," says the identity that most matters is the first name our parents or tribe give us.
15:00:22 From Eric Welton (Korsimoro) : a newborn might have difficulty exercising duties, or participating in their political society, expressing self-determination, etc. - although many modern sapiens being digital life pre-natal
15:00:41 From Eric Welton (Korsimoro) : ^begin
15:02:53 From dsearls : The comedian Tom Bodett said he favored a Native American convention of naming a kid the first thing he or see saw, until their first child came, and the name was about to be "Nissan that won't start," and then "Slick spot on Main Street."
15:03:46 From Eric Welton (Korsimoro) : i think it was Katryna Dow's plenary at MyData 2019 that gave me that 'pre-natal' thought - there was a slide indicating the average age of digital tracks for pre-borns.... so mostly wondering about the transition of the digital self - no concerns in the 'sweet spot of normalcy' - with guardianship/delegation.... (which there is an article about)
15:04:09 From Eric Welton (Korsimoro) : but children famously do not have a choice of parents ;)
15:04:50 From dsearls : Michael Ventura says sanity is nothing more than the ability to manage "the myth of the mono-personality" when in fact we are all many people organized behind first person singular pronouns: I, me, him, her.
15:05:34 From Eric Welton (Korsimoro) : +1 love that! 555
15:07:19 From Wip : @Nicky you got a link to that? Is it a book or paper or something
15:07:36 From Kristina : +1 Nicky
15:08:31 From Nicky Hickman : @ Will - Smith, Karl (2012) From dividual and individual selves to porous subjects, The Australian Journal of Anthropology 23, 50–64.
15:08:44 From Wip : Ta :)
15:09:16 From George Fletcher : Maybe we could add a glossary with definitions to help elucidate the ideas being presented. It is unclear to me exactly what is meant by "digital identity".
15:09:23 From dsearls : Devon Loffreto's original distinction was between self-sovereign and administrative identity. The latter is what Kaliya calls "a database record," assigned by an administrative system to individuals for the system's convenience.
15:09:31 From Wip : +1 George
15:10:04 From Kristina : defining digital identity has usually been self-limiting
15:10:50 From George Fletcher : Kristina - I agree... but using a term with multiple meanings may cause the document to be interpreted in ways not intended
15:11:04 From dsearls : Here is Devon's explanation of Self-sovereign identity, in 2016: https://www.moxytongue.com/2016/02/self-sovereign-identity.html

15:11:24 From Nicky Hickman : +1 Kaliya there is a difference between legal identification and a functioning digital identity
15:13:10 From dsearls : I think we could say citizens or residents of a nation have a right to a state-issued identifier, without calling that identifier an "identity."
From George Fletcher : Doc - is the right really for an identifier? or a verifiable credential? or both?
15:16:14 From George Fletcher : I very much like the thought to NOT call it an identity!
15:17:51 From dsearls : George - I think it's a right to what the state calls an identifier and the individual calls — and uses — as a verifiable credential. So, yes, both. And not an "identity."
15:20:08 From George Fletcher : Got it... I guess I think of the identifier as just another claim. e.g. my passport has a "passport number claim" amongst other claims.
15:21:36 From dsearls : We will have succeeded when at some checkpoint the official says "Let me see a credential," rather than "Let me sed your ID."
15:22:40 From George Fletcher : :) Unfortunately my Dad has no clue what a "credential" is. Had to work through that when he got some instructions from his email provider to update his "credential" :)
15:23:10 From windley : What kind of judgment are we talking about here? Seems like it depends on the consequence. Does this mean a CAPTCHA is not allowed?
15:24:1 From Josh Verbarg (State Farm) : The point of CAPTCHA is to prove there is human interaction.
15:24:26 From windley : But it's a judgement by a machine
15:24:37 From Wip : https://wip-abramson.dev/facebook-erased-me
15:25:54 From Jsearls : CAPTCHA has 2 purposes. prove it's a human and train the machine.
15:26:46 From Jsearls : *prove there is a human…
15:27:24 From windley : So, is it allowed under Article 8 or not?
15:28:14 From JFQueralt : Could you share the link again? I arrived late. Thx.
15:28:24 From dsearls : I'm bothered at how lousy the CAPTCHA machine seems to be at learning what's a bus, a crosswalk and a traffic light.
15:28:40 From Jeffrey Aresty : If someone wants to start looking at the draft
https://docs.google.com/document/d/1rqf_2Pas8beYXsEmk_kATuWr4gX-J4aa/edit
15:29:02 From George Fletcher : Doc - lol
15:30:04 From Jsearls : CAPTCHA is exactly an open question for this type of thing.
15:30:13 From dsearls : I'm always surprised to learn how so many people's clueless and tech non-savvy parents or grandparents are younger than I am. :-)
15:30:17 From Nicky Hickman to Kaliya Identity Woman(Privately) : didn't you do a huge review of lots of different 'declarations of rights' ages ago... are we repeat preaching here?
15:33:27 From dsearls : If we don't have a note-taker, somebody should save off the chat. Just click on the file or ••• button.
15:35:14 From Kristina : saving :)
15:35:39 From dsearls : For identity purposes, I think there is a right to use a pseudonym.
15:35:40 From JFQueralt : Pepperidge farm remembers.
15:35:59 From Jeffrey Aresty : I think Nicky may be taking notes
15:36:07 From Nicky Hickman to Kaliya Identity Woman(Privately) : agree @ Doc
15:37:09 From dsearls : We should have a right to be anonymous (literally, nameless), and pseudonymous as well. Digital systems don't like either. The natural world is mostly fine with both.
15:37:28 From Nicky Hickman : agree @ Doc and yes taking notes
15:37:37 From JFQueralt : How about "the ability of lie" is only necessary when there are negative consequences inherent to interacting with others?
If you get rid of those consequences, is it problematic to "remove lying"?
15:37:56 From Josh Verbarg (State Farm) : How would that effect government sponsored spys?
15:38:10 From Kristina : also after a point a lie is not a lie anymore if everyone starts accepting that lie..
15:38:25 From Kristina : spies are already in trouble with all-going digital..

15:38:36 From Kristina : remember researchon this somewhere..
15:41:33 From Eric Welton (Korsimoro) : i've been playing with the term "reclusivity rights"
From Kristina : https://docs.google.com/document/d/1rqf_2Pas8beYXsEmk_kATuWr4gX-J4aa/edit#
15:43:41 From dsearls : Right, Kristina. It's interesting how many lies are widely taken as truth, even when they're disproven. Most belief systems depend on them. Even science is full of lies that work until they don't. World-is-flat, for example.
15:44:01 From Eric Welton (Korsimoro) : https://surveillancevalley.com/ had an interesting take on ToR, Signal, and espionage
15:45:08 From dsearls : Edward Snowden's book is good on that stuff too.
15:45:52 From Kristina : let us be humans in a digital world

Next steps: Finish the draft and start amplifying
How the document could be used: a declaration to help us "keep being human in this digital era"; a way to explain common goals of IIW community to get wider understanding

A sample project to start implementing this declaration and build a movement around it:
https://docs.google.com/presentation/u/2/d/13oox9jf7_WFDTWZGBM8Y7O7K147UoEscfgtMzcXbnTg/edit?usp=drive_web&ouid=113776052568350431907

Open Source Product Strategy

Session: 17E
Convener: Richard Esplin
Notes-taker(s): Richard Esplin

Tags for the session - technology discussed/ideas considered:

Technology Products, Open Source, Business Strategy, Licensing, Community Governance

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slides to provide context for the discussion:
https://speakerdeck.com/resplin/open-source-product-strategy

Additional points:
* Origin of Free Software movement.
* Origin of Open Source.
* What are the reasons for a business to pursue an open strategy.
* How commercial open source differs from community open source, pros and cons.
* Challenges with aligning sales teams and investors around the strategy.
* How a source available approach can get some of the benefits of an open source approach.
* Why are there no commercial open source mobile wallets today?
* We should have an additional session specific to SSI products.

Closing / Opening Day 3 Agenda Creation

Hyperledger AMA

Thursday 18A
Convener: Marta Geater-Piekarska, Dave Huseby, & Ry Jones
Notes-taker(s): Marta Geater-Piekarska

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

During Hyperledger AMA session the Hyperledger staff, David Huseby, Ry Jones and Marta Geater-Piekarska answered questions from participants all around Hyperledger and the Linux Foundation. These ranged from basic ones, like what does Hyperledger do and differences between projects we host, through some requests to dive deeper in specific projects all the way to very detailed discussion on contribution pathways.

Some key takeaways:

- Hyperlegder is an Open Source project within the Linux Foundation. Hyperledger is an open source community focused on developing a suite of stable frameworks, tools and libraries for enterprise-grade blockchain deployments. It is a global collaboration, hosted by The Linux Foundation, and includes leaders in finance, banking, Internet of Things, supply chains, manufacturing and Technology. Built under technical governance and open collaboration, individual developers, service and solution providers, government associations, corporate members and end users are all invited to participate in the development and promotion of these game-changing technologies.

  Similar to The Linux Foundation, Hyperledger has a modular approach to hosting projects. The Hyperledger greenhouse hosts developing business blockchain projects from Hyperledger Labs (seed) to stable code ready for production (fruition). All are invited to contribute to the greenhouse; collectively advancing industry goals of distributed ledger and smart contracts.

- There are many ways to contribute - you can look through contribution guides to work to help with the code, as well as helping with documentation, translations, and participating in Special Interest and working groups.

Some of the helpful links that we shared:

- Take a look at our Blockchain Showcase and if you are interested in being listed, please submit your solution for consideration
- Review our sector Special Interest Groups (SIGs), these are great forums to share your ideas and work and to get feedback from the community. Jump into these SIGs and start participating and please reach out to the SIG chairs if you are interested in presenting
- Global Meetups- Join and participate in over 170+ global developer meetups, our global community is always looking for builders to present their solutions, in person and virtually as well
- Hyperledger developer community events- regular gatherings for developers working on different projects. If you are able, signup to mentor new developers into our community!

- Sign up for the Hyperledger Monthly newsletter for the latest updates across the community.
- Make sure to follow our regular webinar series: https://www.hyperledger.org/resources/webinars and https://www.hyperledger.org/resources/video-library

Please contact marta@linuxfoundation.org and dhuseby@linuxfoundation.org if you would like an offline AMA:)

Verifiable Credentials For Global Supply Chains

Thursday 18B
Convener: Margo Johnson & Karyl Fowler
Notes-taker(s): Karyl Fowler & Margo Johnson

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Zoom Session Video Link (Provided by Karyl Fowler):
https://youtu.be/FoIS_sWxeho

Agenda:
-Global Supply Chain challenges and opportunities
-Transmute's approach
-Group discussion

Blockchain
Paper credential into digital credential evolution
Only talk about blockchain where we think it is helpful
Verifiable credentials is all that really matters
Everything else is just how it works
Why blockchain? Instead of more traditional database with cryptographic signatures
You don't have to use a blockchain.
In some cases it can be useful as shared source of trust with time stamp, not governed by a single actor
Decentralized Identifier
CU Ledger example: Domain name
Depends on the industry
Human terms - the way you have been given your name is decentralized
An identifier is just a name
No one cares if using an emerging technology
Just an identifier is helpful

Marketing order of operations
Trying not to lead with blockchain when possible
Overcoming existing market ideas

Opening pitch between chain of custody and e-signature solution

Verifiable credential - Trusted certificate or data
Digital version of a known asset

When does the lightbulb go off?
Reducing inefficiencies and liability
Competitive edge
Vendor reputation
Customer assurance

What's the "lightbulb" moment?
When a customer realizes that this tech can provably connect the product (and assc. metadata/reputation info) to the vendor - which currently live in silo'd systems.

Different supply chains are at different levels of maturity
Sharing data - moving away from physical paper
Transmute: "Trusted trade documents for the future of global trade"

Business Value - emphasize w/ customers:
Data Integrity
Data Access Confidence
Data Insights & Analytics

Reviewed Customer Case Study: Steel Import Chain-of-Custody

Who would be the issuer of a document like the Steel Mill Certificate?
While we like the idea of a 3rd party issuer, it is not always possible for some use cases. Specifically for the steel mill certificate, the manufacturer themselves is the issuer of the credential often with customs brokers as the ones presenting the VC to the regulatory authorities [acting as the verifier].
Primary customer today *is* the verifier or the regulatory authority.

What is public and not public about the transactions?
The second value prop of "data access confidence" is a big selling point. Customers want to selectively disclose data to a variety of ecosystem parties without compromising their IP. Encrypted data storage integrated w/ existing storage solutions is how we enable the ability to securely share data.

If the information is encrypted, who can see the blob of encrypted data?
Since Transmute uses encrypted data vaults and integrates w/ customers existing storage provider, the data remains where it was already stored - behind the firewall of the customer. The DID is the only thing publically available to view, and what a party can see when they try to resolve the DID depends on their role and access permissions.

Interest in the digital twin; is there particular technology that we are applying there?
Ref to https://www.riddleandcode.com/ as a company who can support digital twins?

Also reference: https://www.gleif.org/en

The LEI identifies them as a legal entity, and there are other identifiers that can then be issued and associated with the entities that can facilitate easier trade/add value to their supply chains.

GLIVE could also be used as a registry for public DIDs that represent legal entities.

It seems like we need a standard for ensuring that a DID from a different system can be known/resolved/understood in this one. It seems like associating with a unique url as an ID might be more useful; but then how do you sign things? You need a public key.

There are different privacy concerns for DIDs for individual persons vs. entities.

How do we solve for the human problems? Humans are not predictable and often fraud in an organization goes all the way to the top.

Zoom Chat Notes:

From Cam Geer to Everyone: (11:56 AM) product marketing 101!

From Stephen Curran to Everyone: (11:57 AM) Agree with never talking about it except when it adds to the education.

From Darrell to Everyone: (12:10 PM) I think we're seeing the wrong monitor (seeing notes not slides)

From Nicky Hickman to Everyone: (12:12 PM) Have you tried to address specific use cases where decentralization is essential in order to trade. In UK we have the challenge of Brexit and the hot red land border in Ireland. Another example where decentralization is essential is where there are oligopolies, Tony Rose from knowyourcow.com explained that in the cattle markets there are basically 3 big players that dominate the market. With a decentralized model you can promote competition and fairness for smaller farmers and more niche markets e.g. halal or kosher

From Catherine-Finema to Everyone: (12:28 PM) Hi, is this presentation available for download? Very Interesting.

From Arjun Govind to Everyone: (12:28 PM)+1

From Me to Everyone: (12:30 PM) We can make it available as a google doc and include it in the session notes later today!

From Arjun Govind to Everyone: (12:31 PM) Thanks Karyl!

From Me to Everyone: (12:32 PM) Great notes/inputs Nicky! The fact that supply chains are inherently distributed across a variety of players and systems is part of why we believe it's a space ripe for adoption. However, we as a company haven't yet focused on targeting areas who would use the tech to drive more competition - rather we haven't found that to be a selling point…yet.

From Nicky Hickman to Everyone: (12:33 PM) I understand. Ref what Margo is saying now, at least partially I think that the permissions are very clearly laid out in the relevant INCOTERM.

Guardianship & SSI

Thursday 18C
Convener: Sterre den Breeijen
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Zoom Chat Transcript:
From Paul Dunphy to Everyone: 06:34 PM Sounds is good
From Jody to Everyone: 07:05 PM Guardianship Authority would work well for me
From Line Kofoed to Everyone: 07:06 PM Guardianship authority
From Daniel Burnett to Everyone: 07:06 PM Guardianship Authority
From Alan Karp to Everyone: 07:08 PM I like the idea of presenting this in terms of a household because it avoids a lot of the legal discussion that isn't relevant to the key idea.
From Daniel Burnett to Everyone: 07:09 PM Drummond often talks about transactional identity, and it's appropriate here as well. In an ideal world, performing an action as a guardian should require only the authority to do so, and not necessarily a revelation of what your relationship is that allows you to take that action
From Paul Dunphy to Everyone: 07:10 PM I think the powers of attorney discussion is one step beyond the type of flexible and spontaneous delegation that a credential might enable.
From Tom Jones to Everyone: 07:11 PM Authority is often based on relationship
From Daniel Burnett to Everyone: 07:12 PM Digital credential delegation is a technical capability
Yes Tom, but that does not mean that the relationship has to be revealed as long as (in a VC world) a trusted issuer (e.g. a government authority) claims the individual has the right
From Daniel Burnett to Everyone: 07:18 PM I need to go. Thank you Sterre!
From Me to Everyone: 07:19 PM
https://blockchain.tno.nl/blog/four-lessons-on-guardianship-with-self-sovereign-identity/
From Jeffrey Aresty to Everyone: 07:21 PM I appreciate your effort to clarify the area. This is an important area for SSI, especially for adoption.
From Paul Dunphy to Everyone: 07:22 PM There are quite some human-centred issues with designing technology for delegation. e.g. the person that needs help doesn't want to expose themselves to additional risk by sharing resources. Plus the "helper" doesn't want to be accused of misusing the resources they are provided access to (or they won't help again). The "service providers" don't want extra hassle to faclilitate that delegation arrangement. etc.
From Jeffrey Aresty to Everyone: I also have to leave. Thanks for a great presentation and discussion.
From Wayne Chang to Everyone: 07:30 PM Sorry I realized we're using the blue hands
From Me to Everyone: 07:30 PM some are, some aren't ;)
From Alan Karp to Everyone: 07:39 PMJohnny, Are you an astronomer? (I am.)Actually, I was.
From johnnyfromcanada to Everyone: 07:44 PM To help model complex / wicked domains, consider modelling via Domain Driven Design (DDD) techniques: Strategic & Tactical levels, Bounded Contexts, Ubiquitous Language, Event Storming. No an astronomer, but always been enamored about space, the universe, space, space travel, physics,… (love Star Trek). For those not in the know, my background is an actual picture (composite), the Hubble Extreme Deep Field. Essentially, every dot is a _gallaxy_.
"Sorry about the turkeys"
From Me to Everyone: 07:48 PM
https://blockchain.tno.nl/blog/four-lessons-on-guardianship-with-self-sovereign-identity/
From Line Kofoed to Everyone: 07:48 PM Thanks, Sterre!

PhD Positions At Identity Lab Based In Edinburgh – Come Ask Me Anything

Thursday 18 Changpuh Park – China Garden
Convener: Will Abramson
Notes-taker(s): Will Abramson

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

I am 18 months into a PhD position at the Blockpass Identity Lab, Edinburgh Napier University researching privacy-preserving cryptography and identity. I have thoroughly enjoyed the experience and recommend a PhD to anyone who wishes to gain a deep understanding of a subject without the distraction of having to work on financially viable projects. You are accountable to yourself and you set the agenda and focus of your work, which can be tough at times but is also very empowering.

Our lab is new, opening it's doors in 2018. It is primarily a technology lab focused on developing privacy-preserving tools for a more trusted citizen-centric future. This includes privacy-preserving machine learning, cryptography, digital identity and distributed ledger technology. It is exciting to be a part of such a new lab because you get to help shape it's research agenda and future direction.

We currently have two fully-funded PhD positions and expect to get another 7 before October. If you are reading this and think it is something of interest or want to find out more please reach do reach out to me, we would love to have you.

Current proposals are:

- https://www.findaphd.com/phds/project/privacy-preserving-and-trusted-threat-information-sharing-using-distributed-ledgers/?p121028
- https://www.findaphd.com/phds/project/privacy-preserving-systems-around-trust-and-identity-within-smart-phones/?p120788

If there is a project idea that you think would fit with our lab then I believe we are open to suggestions, certainly for the new places when they are announced.

Cheers, I hope to hear from some of you.

Your Trustee & Ethics in a Pandemic – What Your Community Can Do To Prepare

Thursday 18D
Convener: Adrian Gropper
Notes-taker(s): Stew Whitman

Tags for the session - technology discussed/ideas considered:

Try to read this first https://bit.ly/Trustee-Ethics
COVID-19 Immunity-Credentials Decentralized-Governance SSI Authorization Server

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Introduction of Adrian's Blog post https://blog.petrieflom.law.harvard.edu/2020/04/29/covid19-privacy-surveillance-community-organizations/

There are various contact tracing and immunity passport applications being developed

Does there have to be a zero sum game between public health information and privacy

When it comes to using technology for these applications …..

Many of the things we are talking about do not need a network effect at the national level that can be effective at the local level.

The technology may be better applied locally and where there are specific applications of local community needs.

Physicians and local public health are trusted entities…..

Felt that the final hypothesis from yesterday would stop the community from designing these applications. There are too many ethics and issues that are unresolved.

Creates paralysis of action.

https://www.youtube.com/watch?v=3q6ZDtCayh8&feature=youtu.be

Stew: Comparisons of to the paper based vaccination "yellow card"

Aidrian: Creating a trustee for the future preparedness to truly decentralize

Who are you sharing your information with, which information is being shared, the role of the trustee allow to sign

Differential privacy and differential aggregation at the community level, you can strip out the PII to provide contribution to public health data.

Complications of the ontology of the symptomatic descriptors are not public domain.

From scottmace to Everyone: 12:59 PM Adrian, the AMA owns the CPT codes, not the ICD-10 codes

Anil: Separate Contact tracing from Immunity Passports, conflating these leads to problematic decision

Need to look at each application in terms of use and abuse vectors.

Anil's view is not on the contact tracing more on the immunity passport, it is not to do with technology, in the current cycle of the pandemic, disenfranchised communities are asymmetrically impacted by COVID. Those populations don't have the luxury of WAH so the immunity passport needs to be focused on this population.

Stew: Do we need to design solutions for those populations?

Anil: Anything that goes into pilot, in an emergency, will get deployed and that is worrying because the ethics have not been fully thought out.

Adrian: if the half baked solutions go to market are we creating an ethical situation

Adhar, Govt. of India forcing populations into biometric identity programs. Within the context of Adhar the system of ??india Stack?? as a way to store documents wrt health documents.

Anil: My 90 yr old mom has paper Adhar card, and if it needs to be used, Anil's nephew goes and presents it on her behalf.

@Adrian. Read your paper - TU. Trust is so important in public health. One of my clients are interfaith congregations and they serve the most oppressed. We have changed public policy on homelessness and sanctuary for immigrants and refugees in WA state. As a former gubernatorial appointee in environment and public health, I serve on multiple committees advising governors in WA and NY. - on COVID-19 response

Adrian: If we give people meaningful choices around their community and their trustee, not state coercion, in the form of, church, charity, civic organization.

Stew: Pvt sector companies designing solutions, those who can (e.g. privileged) are able to opt in, this creates an ethical divide from the marginalized populations.

Neil: Canadian perspective, Community servant, have many elderly and "marginalized" populations. BC Gov is pursuing digital identity aggressively. We are not spending the resource to find an advocate for digital consent and act on their behalf in a controlled manner. Need the concept of an SSI notary. Then we need the physical token that is not a digital device, eg smart card that encodes the key information. There is the concept of the last mile. People have trust in their local community organizations (the "last mile" of volunteer service delivery), even as Canada and BC govt are creating root DID. It can be like census data, DMA ZIP aggregating. Option of consent for a local proxy.
Adrian: Even while we have a trustee as a model, we originally had the prescription use case, we needed VCs to be serial so that the Dr has VC, the patient does not need to have the ID VC, by only a place to store the Dr. VC for the prescription. So there has to be a bonded intermediary. Govt. issue credential to the expert, e.g Dr.

Scott: how does a digital notary get created?

Adrian: Digital notary was solved for within the Etherium specification ……
Adrian: Going back to Anil, you didn't want to touch contact tracing, but you're ok with immunity passports. I don't see those any differently.
Anil: We will have to agree to disagree. The rails that are being put into place with Google / Apple APis for contact tracing. Are you OK with Google or Apple being the gatekeeper to immunity or contact tracing. I need to look around the corner to put in compensating controls.
Stew: Clarifying comments on innovation from the sources of innovation between private and public sources
Anil: In the pandemic you are seeing the dependencies, greatness, and flaws of the public service. There is going to be market mass coming from Google / Apple……..
From Kaliya Identity Woman to Everyone: 01:34 PM http://www.appassay.org
Johannes is doing this The Government bonds labs as to competence in running test samples for results. Is there not the same bonding exercise needed in the contact tracing case?

Adrian: Apple & Google should not be the organization to self-certify their applications and the contact tracing process

Anil: The perceived problem with Apple/Google will extract a price for the service at some point in future. Only disagree on matter of timing

Neil: The reality of (current manual) contact tracing is decentralized, there is no reason that the technology cannot do the same.

Attaching the Zoom Chat:
From Grace Rachmany to Everyone: 12:45 PM I would like to take the time to read
From Adrian Gropper to Everyone: 12:46 PM
https://www.youtube.com/watch?v=3q6ZDtCayh8&feature=youtu.be
From Kaliya Identity Woman to Everyone: 12:59 PM so are you talking to the Overlays Architecture folks like Paul Knowles he is working on this in CovidCreds.com some how…
From scottmace to Everyone: 12:59 PM Adrian, the AMA owns the CPT codes, not the ICD-10 codes
From Karen Advocate to Everyone: 01:05 PM @Adrian. Read your paper - TU. Trust is so important in public health. One of my clients are interfaith congregations and they serve the most oppressed. We have changed public policy on homelessness and sanctuary for immigrants and refugees in WA state. As a former gubernatorial appointee in environment and public health, I serve on multiple committees advising governors in WA and NY. - on COVID-19 response
From Kaliya Identity Woman to Everyone: 01:30 PM what is the link Adrian?
From Adrian Gropper to Everyone: 01:31 PM https://bit.ly/Trustee-Ethics
From Kaliya Identity Woman to Everyone: 01:34 PM http://www.appassay.org Johannes is doing this
From Karen Advocate to Everyone: 01:40 PM Share your concerns Anil. Sadly in addition to concerns about Google or Apple, I don't trust our current federal government - way too politicized and many experts not listened to or removed.
From Stew Whitman to Everyone: 01:40 PM Hey can someone take over the notes. I need to take another call.
https://docs.google.com/document/d/1qoH3JFvrFsyMkNPlWoCU8QRGg3dv6SewjHtShB_x7ME/edit

KERI Implementation: What's Next DID:UNI Method (Ref Imp. DIF Project)

Thursday 18E
Convener: Sam Smith
Notes-taker(s): Sam Smith

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Links provided by Sam Smith:

The notes are here: https://hackmd.io/orhyiJkLT721v4PCPkvQiA?both

Also slide deck and white paper:

https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI2_Overview_IIW_2020_A.pdf

https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI_WP_2.x.web.pdf

Intro To The Me2B Alliance Testing Specification

Thursday 18F
Convener: Lisa LeVasseur
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Presentation here: https://me2ba.sharepoint.com/:b:/s/GoodCoPsWG/ERZT57fS-KlMsKHnQGCY-4IBeJIdzu_n5Dkg6i0yjHWEpg?e=Dc6aWe

Zoom Chat window:
From dsearls to Everyone: 09:43 AM A side thought: we can get this community more interested and involved if we say "Me" is SS (as in self-sovereign)

From Me to Everyone: 09:47 AM We have sovereignty, we aren't sovereign.

From Marc Davis to Everyone: 09:47 AM Classic tension in political identity theory: 1) Me-First: individuals are prior to society; 2) We-First: society is prior to individuals.

From Me to Everyone: 09:47 AM We2B

From Bill Wendel1 to Everyone: 09:47 AM YES, We2B

From Marc Davis to Everyone: 09:51 AM Me-First (Rousseau) vs. We-First (Foucault) +1 Doc "The personal is political and the political is personal."

From Timothy Ruff to Everyone: 09:52 AM FYI Huseby hates the terminology SSI too

From Marc Davis to Everyone: 09:53 AMI actually like it for many reasons That friction with corporations is because there is actually a real power struggle.

From Timothy Ruff to Everyone: 09:54 AM I like it for many reasons too, and dislike it for some bigger ones. :)

From mahod mah to Everyone: 09:54 AM notes in chat is good.. then we cut out from the file

From Marc Davis to Everyone: 09:55 AM Internal vs. external naming strategies: what we say to each other vs. what we say to oppositional parties we need to sell to.

From JeffO-StL to Everyone: 09:59 AM Discussed 5 Assurances of testing Leaned independent testing would be more credible. Interviewed 20 various non-technical types about the idea of the seal.

From Marc Davis to Everyone: 10:00 AM People surveyed did not initially realize what they were giving up in order to use a “free” service.
From JeffO-StL to Everyone: 10:01 AMFound that people e spoke to are not well versed in under the hood tech. Ex: "What are you giving for the 'Free Service?" revealed lack of top of mind sensibility of the value trade. Looking to give a Pass/Fail behavioral assessment.

From Marc Davis to Everyone: 10:01 AM The product or the company who sells it?

From JeffO-StL to Everyone: 10:03 AM Key question in the survey: What am I giving, what am I getting and is the product holding up their end of the deal? Should the language in the survey be from the context of the individual or the company inquiry aspect, More outward facing.

From Marc Davis to Everyone: 10:05 AM Probably similar for Instagram

From JeffO-StL to Everyone: 10:05 AM In general people perceive the relationship to be with the service and not the connected family. Love WhatsApp but hate Facebook.

From Marc Davis to Everyone: 10:06 AM People love Amazon for shopping vs. are mistrustful of Alexa-enabled devices.

From JeffO-StL to Everyone: 10:07 AM Down to the one simple assurance Give, Get, Respect of the deal.

From dsearls to Everyone: 10:08 AM Craig Burton: every large and successful company is "a thousand tornadoes"— many companies, many personalities, in one. Example: Amazon is in the advertising business and its Eero home wi-fi mesh router bothers users on its app constantly to block ads at the network level, to speed up performance.
There is also the verb "relate" and the noun "relationship." We might relate to a barista without having a relationship with the coffee shop.

From Marc Davis to Everyone: 10:10 AM Three Relationship States: None—reasonable expectation of anonymity; One-Off—performing a “typical transaction” without being remembered; Me2B Relationship—Remembered, Recognized, Responded To.

From JeffO-StL to Everyone: 10:10 AM States of a relationship. No relationship - anonymity; Typical Transaction State w/o being remembered - sign up to gain function of service with embedding a relationship, one off; being remembered, recognized, responded to.

From mahod mah to Everyone: 10:10 AM Can you put the link in the chat?

From JeffO-StL to Everyone: 10:12 AM Loyalty relationships as example of prior state. Working on surfacing Vectors of relationship. Working on surfacing vectors of relationships.

From Marc Davis to Everyone: 10:14 AM Joe Andrieu came up with functional identity concepts of: Remembered, Recognized, Responded To.
From mahod mah to Everyone: 10:15 AM http://blog.joeandrieu.com/category/functional-identity/

From Me to Everyone: 10:16 AM Johannes' session on CCPA/GDPR requesting data

From JeffO-StL to Everyone: 10:21 AM Influencer as a highly viewable threat to all.

From dsearls to Everyone: 10:26 AM An aside:
https://trends.google.com/trends/explore?date=all&geo=US&q=influencer
I've been called that, and don't like it. Just saying.

From mahod mah to Everyone: 10:27 AM i think it’s awful and an attempt to separate and make people ‘micro famous’ and that fame model is so negative on our systems and society
the conversational middle is where it’s at

From dsearls to Everyone: 10:27 AM David Weinberger: "In the future everyone will be famous for fifteen people."

From JeffO-StL to Everyone: 10:28 AM mahod: Agree Fame is a four letter word starting with "F". I told my daughter that we put caution tape around that word/concept.

From Marc Davis to Everyone: 10:32 AM Familiar with?: https://tosdr.org/

From Timothy Ruff to Everyone: 10:32 AM For clarity: platforms shouldn't have the power to separate an influencer from their audience (regardless of how I feel about that influencer). Influencers should have a direct relationship with (not ownership over) their audience, where either the influencer or the fan can choose to discontinue the relationship at any time, without either being beholden to any particular platform. It is the essence of user portability.

From dsearls to Everyone: 10:34 AM FWIW, in ProjectVRM we have a privacy manifesto that addresses Marc's points here. https://cyber.harvard.edu/projectvrm/Privacy_Manifesto

From Me to Everyone: 10:38 AM Nathan Kinch is doing good work on readable TOS progressive disclosure for TOS oops two separate thoughts there reminds me of the levels of JLINC SISA

From Iain Henderson to Everyone: 10:39 AM yup, that is the JLINC SISA logic

From Marc Davis to Everyone: 10:42 AM Progressive Disclosure of Standardized TOS:

1) 7 +/- 2 Human-Readable Bullet Points; 2) Expandable to a single Human-Readable Paragraph; 3) Expandable to multiple Lawyer-Readable Paragraphs; 4) All expressed in Machine-Readable form as well

From Cam Geer to Everyone: 10:46 AM SMBs are a key part of the fabric of a community
and they employment the most people in the US

From Bill Wendel1 to Everyone: 10:46 AM Real estate is an example of a multi=trillion dollar marketplace that is broken. To address Tim's comment about the usefulness and VALUE from a consumer's perspective. In real estate, there is a 4th level of a Me2B relationship (1) Being remembered, (2) Being recognised, (3) Being responded to, but the high value add doesn't occur from the consumer's perspective until (4) Being responded as a fiduciary. Me2B has the opportunity to extend the conversation about fiduciary duties in real estate beyond agency relationship in the buy/sell transaction to Information Fiducariary before, during, and AFTER the transaction as a homeowner.

From Iain Henderson to Everyone: 10:47 AM Marc, I need to drop off now but i'll send some screen shots of the JLINC standard information sharing agreement approach which has 'the two sentence version that drills to the 3 paragraph one, then the full machine readable one. I'll put them in the notes.

From Timothy Ruff to Everyone: 10:48 AM Check out community.com
It's a platform, but it's doing well because they're giving influencers a more direct relationship with their audience. Influencers crave it. We could find a way to ride that toward adoption of our principles.
Link to Nathan Kinch's work on usable Terms: https://www.youtube.com/watch?v=tS-BlGIIg30&feature=youtu.be

Credentials Should Be Treated Like Keys KMS discussion

Thursday 18G
Convener: Cam Parra & Mike Lodder
Notes-taker(s): Mike Lodder

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

We discussed this PR
https://github.com/hyperledger/aries-rfcs/pull/440

We also discussed various APIs surrounding hardware enclaves and building a common ecosystem around that.

Build An SSI Proof Of Concept On Sovrin

Thursday 18H
Convener: Riley Hughes & Streetcred ID Team
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:
self-sovereign identity, verifiable credentials, Sovrin, SSI, DID

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Instructions for Building a Proof of Concept Session

1. Get set up on Streetcred Developer Portal by following the directions here: https://www.notion.so/streetcred/Login-to-Streetcred-Portal-d81e04a7e07746e5af930c677b5cd6ce
2. If you want support from our team, join IIW Slack: https://join.slack.com/t/iiw/shared_invite/zt-e08ieit0-7~iZLzYJBIuaD6CG55YH7w
3. Once you're in Slack, add yourself to the channel #proof-of-concept

Then, begin working on your proof of concept!

1. Consider your use case
    a. Is there something you're working on for your current company?
    b. Do you have a startup idea you'd like to prototype?
    c. Do you want to just do a demo or tutorial to understand how it works? (if so, use this link: https://docs.streetcred.id/docs/tutorial
2. Identify the actors
    a. Who is the verifier?
    b. Who are the issuers?
    c. Who is the holder?
3. Build out the flow using the Streetcred Developer Portal
    a. Set up organizations for the issuers and verifiers
    b. Set up Credential Templates for the issuers
    c. Set up Verification Policies for the verifiers
4. Determine next steps
    a. Use the API to integrate into a demo application
    b. Build a business case
    c. Validate ideas with stakeholders

Ensuring Transparency in Law Enforcement Exceptional Access

Session: 18J
Convener: Dan DuBeau & Alex Rosen
Notes-taker(s): Dan DuBeau

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link from Dan DuBeau for slides provided at the session:
https://barlea.org/wp-content/uploads/2020/05/IIW-Exceptional-Access-20200509.pdf

Summary:
The current methods of exceptional access are untenable. Solutions such as back doors and key escrow create more problems than they solve, and there is a flourishing gray market for hacking smart devices. There are approximately 500,000 to one million exceptional access requests each year, yet there is no standard for whose data is accessed, under what conditions, and how much of the data—no standards for governments, no standards for manufacturers. We propose a method of exceptional access that ensures 100% transparency, as well as a consortium of manufacturers, privacy and advocacy organizations, and law enforcement agencies to ensure complete global transparency is assured.

101 Session: Verifiable Credential Handler (CHAPI) & DIDComm

Thursday 19A
Convener: Manu Sporny, Orie Steele, Sam Curran
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Video Recording:
https://vimeo.com/413742210
PW: weCOULDN'TchangeTHEname (note the apostrophe)

Slides: https://docs.google.com/presentation/d/1qPbwx9IXwPlgsZgS2XPXeGgstxrixnC8n0E2I4cxVc8/edit

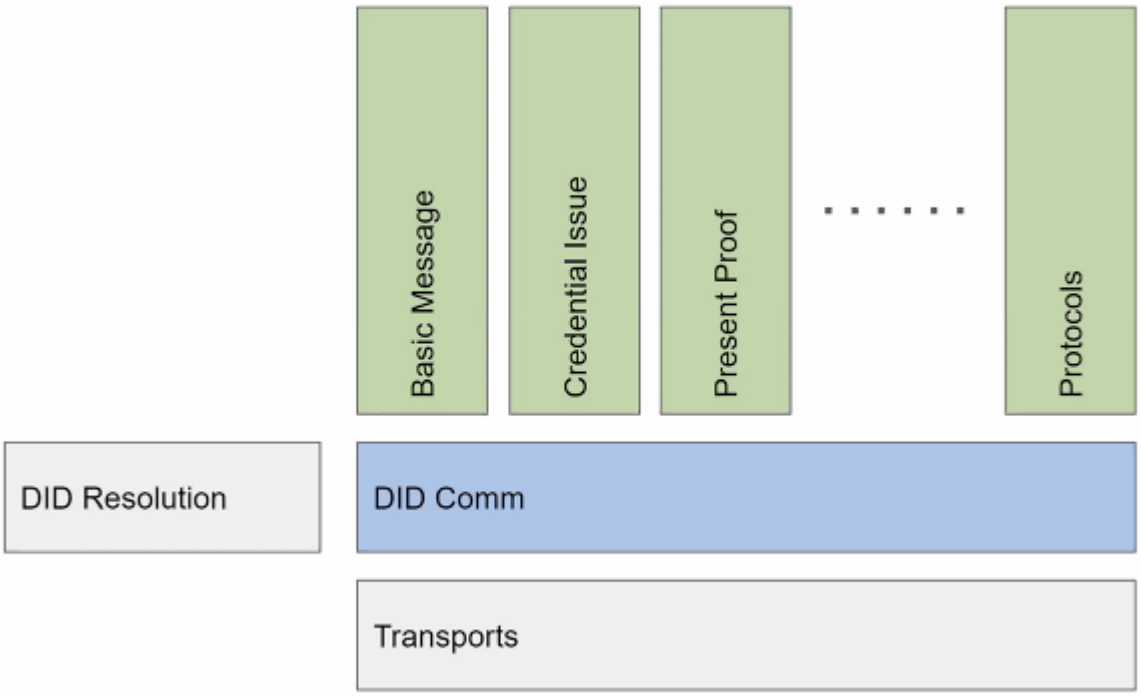
CHAPI and DID Comm 101 presentations were first

CHAPI 101
- General: Connectivity between issuer, holder, and verifier
- CHAPI
    - "Dumb pipe", open the communication channel
    - CHAPI solves for the browser security model
        - Problem statement
            - How do you enable communication between App and web browser?

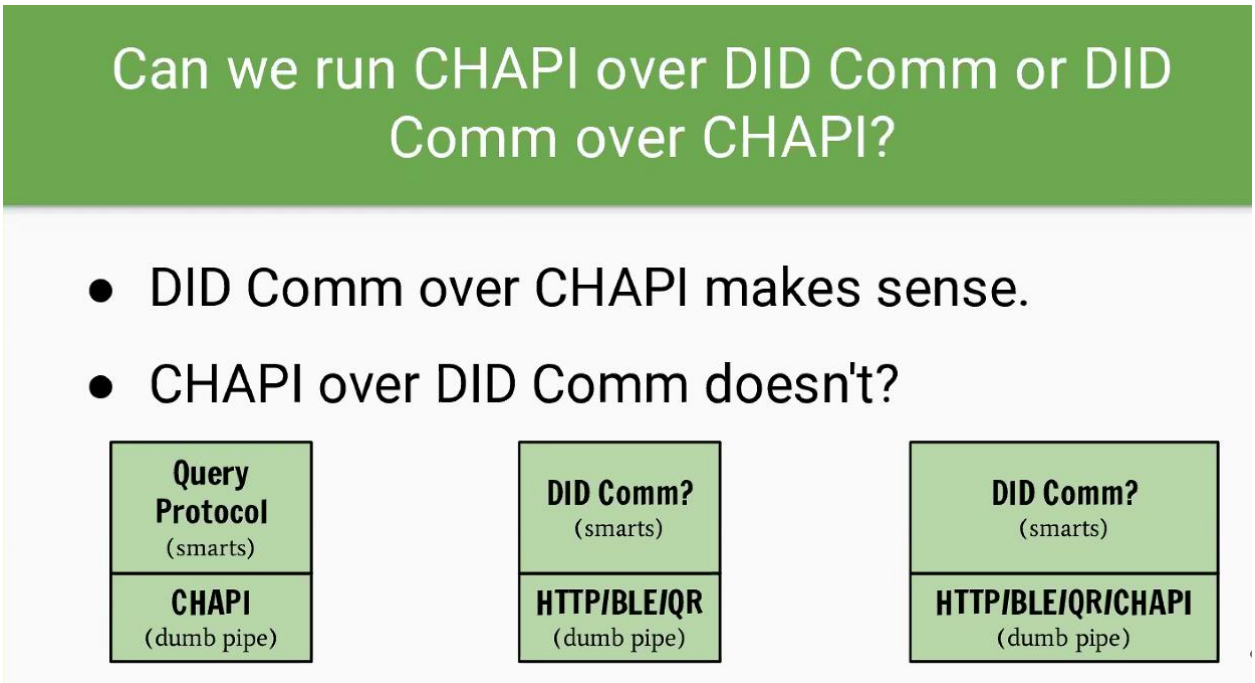
        - How do you enable communication between different tabs in a web browser?
    - Solution
        - Enable two websites to communicate between each other in a web browser
        - Browser can create real time pipeline between two browser tabs (client to client edge communication)
        - CHAPI allows to move data between two websites without leaving the machine
        - CHAPI doesn't care about the content of the pipes
    - Has a path that can grow into "WRAPI"—Web Request API—that lets any two websites talk privately via the browser
- Question about REST API - there is not one in CHAPI by itself
    - But in the DHS (US Department of Homeland Security) intro project the HTTP APIs and CHAPI APIs are both in use and therefore may seem intertwined

DIDCOMM 101

- Q&A - Some requests for more explicit definitions:
    - From the charter of the DIDComm WG at DIF: "Produce one or more high-quality specs that embody a method ("DIDComm") for secure, private and (where applicable) authenticated message-based communication, where trust is rooted in DIDs and depends on the messages themselves, not on the external properties of the transport(s) used. The method must be usable over many means of transport, including those that are asynchronous and simplex, and ones that do not necessarily use the internet. It must support routing and relay through untrusted intermediaries, not just point-to-point delivery. In addition to the communication and protocols described above, the protocols for exchanging DIDs/keys to bootstrap such communication are within scope. These protocols can be the foundation of higher-level protocols such as credential exchange and higher-level authentication protocols."
    - DIDComm in layman's terms: https://www.windley.com/archives/2019/06/did_messaging_a_batphone_for_everyone.shtml
    - From Geovane Fedrecheski and Oliver Terbu, in the chat: "DIDComm is a standard way to exchange DID-aware encrypted messages, regardless of transport (e.g., unlike TLS, which is limited to TCP) - a set of subprotocols and related messages, such as those used for credentials exchange"
- Other Q&A
    - Sam Curren: explicit ACKs allowed (but not forced at this level), threading (see RFC)



Deep-dive
Manu presented this slide:



- The fact that CHAPI is named CHAPI is misleading, because its not just about VC exchange

- Manu explained that the name Credential Handler API is so called because the browser vendors called their API the “Credential API”.

Highlights from Zoom CHAT during Deep Dive

- From Dmitri Zagidulin to Everyone: 08:58 PM
- (quick reminder) CHAPI the protocol and the presentation queries used over chapi are separate - https://digitalbazaar.github.io/vp-request-spec/
- From Michael Jones to Everyone: 08:57 PM
- Are you wanting to standardize any additional JWS and/or JWE algorithms?
    - Orie: @MikeJones AFAIK they want to reserve terms like JWT did but for messages, thats why JWM is a thing.
- Distinction b/w CHAPI and presentation-request spec?
    - https://digitalbazaar.github.io/vp-request-spec/
    - Orie Steele: https://github.com/decentralized-identity/presentation-exchange is not used by CHAPI… but could be used by DIDComm and CHAPI ; Correct… but I attend [to?] both and try to keep them in sync.
    - Dmitri Zangadulin: the Peer to Peer section of the spec even mentions DIDComm; we’d love suggestions of how the two could work together
- Commentary on Browser-vendor relations and W3C group (Wendell Baker’s backstory)
    - Wendell: Here is the G thinking https://github.com/samuelgoto/WebID
    - Tobias Looker: Yeap this ^ is essentially native support for the OIDC flow

Chat log PLEASE NOTE: POOR CHRISTOPH MENZER HAD HIS IDENTITY STOLEN by the “log in as host” button. all slanderous and reckless comments attributed to him in the log were actually made by notorious identity thief Juan Caballero

Transaction Tokens: Optimizing Authorization Across “Domains”

Thursday 19C
Convener: George Fletcher
Notes-taker(s): George Fletcher

Tags for the session - technology discussed/ideas considered:
Authorization, OAuth2, JWT

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link to slides provided by George Fletcher:
Slides: https://drive.google.com/file/d/18AhIjhPjkKx8GqbrUsHt-ZlXXO9rOeX7/view?usp=sharing

The Future Ain't What It Used To Be – How to approach the next few years (COVID, Climate, Economic Depression…)

Thursday 19E
Convener: Johannes Ernst & Grace Rachmany
Notes-taker(s): Johannes Ernst, Grace Rachmany, & Group

Tags for the session - technology discussed/ideas considered:
What are you doing on a personal level differently? What about professionally? In the following areas:

- Food and water security versus money security.
- Information sovereignty
- Community cohesion
- Influence in Government
- Health and wellness
- Federal money, hyperinflation, transactional money
- Violence: governmental, political unrest, survival-based
  Social rejection

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Attendees: about 25-31
Agreement for the session is that things are nameless/geolocationless. Anonymized notes below.

What do you do personally to get prepared?

- bicycling
- gardening and home food production
- modeling behavior for neighbors
- move into more survivable areas (within the country, to a different country)
- group economy, coops
- new kinds of technology
- outreach to new communities
- communicate / teach friends and communities
- attending remote conferences more
- feeling my own hypocrisy
- not playing music to be considerate of neighbors
- teaching neighbors to do sustainable home growing of food
- hospicing relatives
- blogging
- voter registration
- joining groups helping with Covid tracking

Organizations in the area of creating technology solutions
Digital Life Cooperative
http://open.coop/

P2P Foundation
Ceptyr /Metacurrency project/ Holochain
Lifescope.io
Daostack / Aragon / Colony.io
dGov.foundation
80 different interest-based groups https://www.presencing.org/community/hubs
Freedom Box Foundation
Bill Wendel, realestatecafe@gmail.com / http://Twitter.com/RealEstateCafe
reddit The Collapse Community
RebelWisdom.com
https://en.wikipedia.org/wiki/Stigmergy
https://youthclimateaction.com
Extinction Rebellion
www.project-springtime.org

If you want to explore what you might do after this session, there are sill about 8 more weekly sessions follow #GAIAjourney on Twitter. Here's a sample of the energy they create in their Global zoom sessions https://twitter.com/MITxULab/status/1255748188478283776?s=20
--

Following are the anonymized notes:

20:01:06 : May I record the session? Anyone not OK with that?:::
20:01:15 : No recording please:::
20:01:21 : Roger:::
20:03:15 : I've got my tin foil hat:::
20:03:44 : Good news for you, if you're looking for others eager to engage this conversation. An MIT related organization, the Presenting Institute, is convening a global conversation — 14 week long, with Hubs — organized by area or interest group, see https://www.presencing.org/gaia::
20:04:36 : Does this statement by Bill Gates ("We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten.") still hold true when we have a massively disruptive global event lasting 2+ years?:::
20:05:35 : There already is a mental health crisis:::
20:05:54 : i know 2 people, unrelated, that in the last week have both cracked, ended up in the hospital:::
20:06:02 : +1
20:06:33 : both in SF:::
20:07:10 : can you repost the slide ie LIst:::
20:08:59 : on current shifts in work: 1/3 working from home; 1/3 laid off; 1/3 essential workers.::
20:09:02 : To repeat the question: What are you personally doing to change your own life and / or contribute to the community differently.::
20:11:03 : I believe 15%-30% of workforce will stay in place and displacement will continue to grow thereafter.:::
20:11:30 : "Think globally, act locally" ;-):::
20:11:50 : And also collectively act globally.:::
20:12:06 : Apologies for tardiness. Roommate set off the fire alarm. All ok. :::
20:12:38 : ++:::
20:13:14 : We are also working hard on local policy up and down the west coast on moves that an lower carbons in each of our cities.. so San Diego to Vancouver:::

20:13:32 : New joiners, we are speaking from a personal perspective where we talk about what we are doing differently and also professionally in the current situation.:::
20:13:45 : The rules of the group are confidentiality if you are taking notes. :::
20:14:12 : projectspringtime ?::: <- https://project-springtime.org/
20:14:47 : The contact tracing site is contrace.org:::
20:14:54 : Devils' advocate: What are people's thoughts on the positive data/evidence given by folks like Hans Rosling, Steven Pinker?::
20:15:28 : (That's the topic of my next talk,.... new forms of money):::
20:15:33 : can you give a link? I'm not familiar with those guys::
20:15:36 : Resource-Based Economy ?:::
20:16:15 : q+:::
20:16:56 : yes.. that's hard -- not knowing people.. it took us a year or so to get up to speed in :::
20:16:59 : Another potential avenew: Global Parliament of Mayors::
20:17:01 : its hard, moving:::
20:17:19 : https://globalparliamentofmayors.org::
20:17:31 :, you're channeling the Otto Scharmer, the MIT professional convening the 14 week FREE program. His assumptions are 1. Our current system is not sustainable & collapse is currently under way. 2. I want to be a part of a new story of the future. 3. I don't know how. #gaiajourney gathers in this massive Zoom call to help birth this new future.:::
20:17:50 : I moved to from and still struggle with the culture in :::
20:18:34 : Nitpick Distinction: At the timescales (human reproductive time) that we are discussing, we are adapting (not evolving).::
20:18:52 : +1:::
20:19:24 : https://www.ted.com/speakers/hans_rosling::
20:20:11 : Links I've been collecting on new forms of money.
https://docs.google.com/document/d/1M3ooTulljGehOJ9lzcT0QSH1OcRmcAPbO-E8ej_DJuY/edit#::
20:20:43 : https://www.ted.com/speakers/steven_pinker::
20:22:28 : New joiners, we are speaking from a personal perspective where we talk about what we are doing differently and also professionally in the current situation.
·The rules of the group are do not use names and precise geolocations of speakers if you are taking notes :::
20:25:56 : Exponential Growth: Great explanations by Ray Kurzweil (Singularity)::
20:26:27 : only about 10% of the pop is able to deeply conceptualize:::
20:27:02 : Agreed. I think for that reason we as technologists and people who see this have an added responsibility to those 90% to create solutions that will allow people to transition and stay safe and healthy:::
20:27:37 : Instead of taking mic, will respond here. No problem disclosing my name or location as I'm convening one of the interest Hubs for #GAIA. Eager to connect in coming weeks w/ others who recognize current real estate ecosystem is not sustainable & the magnitude of housing inequality is being exposed::: 1 in 3 unable to pay rent, April 1st. Changes in the real estate ecosystem are already presenting opportunities for innovators in VRM/Me2B/IIW community. Getting some preliminary reactions from an intergenerational, even international group of concerned citizen's who want to help transform this moment into a better future. See / share tweet thread:
https://twitter.com/RealEstateCafe/status/1248629997612515329?s=20::::

20:27:46 : https://www.goodreads.com/book/show/417181.One_Grain_of_Rice::
20:28:06 : Great book to help explain exponential growth in prior message.:::
20:29:10 : New joiners, we are speaking from a personal perspective where we talk about what we are doing differently and also professionally in the current situation.

·The rules of the group are do not use names and precise geolocations of speakers if you are taking notes. :::
20:29:26 : Let's have a Plan: www.letshaveaplan.blog Started blogging when COVID-19 began in Seattle. Trained as a scientist and attorney; worked in environment and public health 30+ years. Hopsiced both parents. Twitter: My plan:
·(1) Organize and create relationships of trust.
·(2) Vision what you want your community to feel like.
·(3) Harness a crisis to create the opportunity to install new systems. (Systems which are resilient, sustainable and equitable for all.)
·(4) Hospice old systems.
·(5) Thrive.::::::
20:29:53 : +1 Bravo, tune into what @DrRevBarber is doing with the Poor People's Campaign. Virtual march on Washington, 6/20/20:::
20:30:21 : hhahahahaah you go!:::
20:30:53 : re: bezos::
20:31:44 : The future is already here, it's just not very evenly distributed.:::
20:32:31 : That's the extinction rebellion argument: 1-3% need to act to change this.. and we have 6y::
20:32:45 : Wow that is shocking:::
20:34:45 : water isn't free:::
20:35:02 : … but it should be and probably food and healthcare should be as well.:::
20:35:14 : its quite pricey for residential.. but for industry it is, effectively:::
20:35:35 : well.. the pricing is there to encourage conservation by individuals:::
20:35:51 : and i don't disagree with that.. water in CA is 1/4 the price per CCF as it is in seattle.. :::
20:36:03 : Corrected Twitter handle for Rev. Dr. William J. Barber II: @RevDrBarber::
20:36:04 : and how many water their lawns in seattle? too pricy so they dont:::
20:36:39 : Yes I know DrRevBarber from hospicing my dad in NC. Poor People's Campaign is in Seattle with a few people, but not much participation in the 5th whitest city in America. :::
20:36:48 : also people in WA state do a lot of water collection of rainwater.. because it makes sense economically:::
20:40:45 : ++ Extinction Rebellion is very good org:::
20:41:18 : def encourage people join their local chapter:::
20:42:44 : Bravo ….! thx for the correction, and glad to hear you're engaging faith communities, check out "New Economy" Summit the Pope had planned in Assisi before the pandemic canceled it. Covid has exposed what's wrong with the current economic model and so much more. One way to respond is via the interfaith New Economy movement is now using Slack to work in subgroups http://FrancescoEconomy.org::
20:42:51 : Brava!:::
20:44:09 : I'm very impressed that everyone are talking about their actions to the community, even in this hard situation. I'm barely adapting my own situations, and I feel like a terrible person not having the mental resources to care about my community...:::
20:44:19 : Thank you ... for talking from your heart. WE have to make the changes together. As the Hopi tribe says, We are the Ones we are Waiting For." Disruption is good. http://letshaveaplan.blog/2020/03/06/not-all-workers-can-stay-home-workers-need-safe-workplaces-paid-sick-leave/::
20:44:35 : ..., thanks for sharing.:::
20:45:18 :, please do not "should all over yourself". Everyone is different and has different resources. We are all doing our best and we all feel motivated at different times and in different ways. Don't underestimate the contribution you are making just by being considerate enough not to play your instrument.:::
20:45:23 : Go easy on yourself as you go and I can say that you contemplation is a GREAT start.:::

20:45:35 : Thanks! I'm happy to share <3:::
20:45:41 : It's a lot of work to be responsible and less carbon making.. so a change is: asking yourself what is worth your time and not having my our old views as marketers have told us we should do, ie making everything convenient.::
20:46:31 : Convenience is often a cue to a large offloading of environmental damage for that conveniece:::
20:46:41 :. Be gentle with yourself. Part of the process is getting re-connected within. :::
20:47:19 : Humans were evolved to feel good by helping one another. We are hairless animals with no claws or wings. our only defense is having one another and working in groups--- our "altruism" is a survival mechanism built into our DNA:::
20:47:50 : +1:::
20:47:50 : Yes, humans are social animals.:::
20:48:25 : Thanks for your kind comments. I personally think it's very difficult to express how I am thinking/feeling even in my native language, and that's making me think negatively:::
20:48:40 : Would like to share my experience that if you want to create change in your community you need to own the property and land that your activity is placed in/on, because otherwise you will loose against the property-owners. Software is not going to help, because the above is a root problem.:::
20:48:47 : Love the competition vs cooperation angle - if that's how you said it!:::
20:49:37 : Wow.. that's a background. Winter / snow is such a luxury.:::
20:50:06 : And there it is melting and floating away.:::
20:50:09 : Yes, "competition vs cooperation", I was thinking of that for building a study group:::
20:50:37 : Indeed, the Feudalism remains alive and well (just in better disguise):::
20:50:43 : As a disrupter....who after working 20 years....went to law school and studied law in the ...to understand how women were chattel in the US Constitution...we need a new legal system NOT based on property ownership. :::
20:50:59 : +1 to those comments:::
20:51:15 : +1:::
20:51:21 : My next session will be about Money & Mechanism Design, which addresses a lot of these structural issues.:::
20:51:50 : Yes- disrupting education! This is a great time to support groups who offer true education as opposed to Texas textbook based learning!:::
20:52:36 : _Level_ of government matters.:::
20:52:38 : I expect the US will break up into bio regions and the federal government will disappear. :::
20:53:08 : We need Liquid Democracy:::
20:53:17 : - that is my ray of hop:::
20:53:22 : hope:::
20:53:35 : Hi! Its been awhile. :::
20:53:41 : Cascadia:::
20:54:08 : https://en.wikipedia.org/wiki/Cascadia_(independence_movement)::
20:54:21 : We need to vision based on values not based on existing systems. :::
20:56:17 : I love when people disagree with me!:::
20:57:16 - What's the book you mentioned? George Lay...:::
20:57:39 : I AGREE. That is why we need to be LED by the most oppressed -disenranchised, people of color, poor, immigrants, disabled etc. :::
20:58:00 : also women, LGTBQ etc.:::
20:58:58 : Do you mean George Lakoff?:::
20:59:28 : Digital Life Collective:::
20:59:35 ::::
20:59:36 : Freedom Box Foundation:::
20:59:39 : ceptyr:::

20:59:54 : If you're looking for a community to join or want to start one of your own, here's the roster so far for #GAIA — 80 different interest-based groups https://www.presencing.org/community/hubs::
21:00:05 : Michael Moore's movie "Where to Invade Next…" arrived (IMO) at an interesting conclusion (which I also happen to believe): Women should run the world (at least for awhile).::
21:00:45 : The countries who have minimized the impact of covid19 deaths are all women led.:::
21:01:06 : isn't that fascinating..:::
21:01:21 : Lifescope.io:::
21:01:30 : and also.. that 2/3 of the deaths are men from C19 and they seem to care the least:::
21:01:34 : ironic:::
21:02:45 : Stigmergy is a great concept:::
21:02:45 : If people are willing to share emails, I'd appreciate being able to follow up with many of you. Mine is
21:03:18 : https://en.wikipedia.org/wiki/Stigmergy::
21:03:31 : Showing up for Racial Justice, SURG:::
21:03:58 : Help us as coders and maintainers on the self-sovereign technology project https://bit.ly/Trustee-Summary::
21:04:14 : CELDF for Rights of Nature as possible basis for a legal system...has been done in 2 other countries todate.:::
21:04:31 : For white folks wanting to disrupt our own impact, SURJ does great work.:::
21:04:38 : You can also send email through the list of participants.:::
21:05:03 : https://youthclimateaction.com::
21:05:08 : Thank you all! <3:::
21:05:42 : I think this session points to the society wide anxiety that has been building over the last two decades and really exploded during COVID.:::
21:05:45 : Thanks for convening!:::
21:06:01 : George Lakoff: https://en.wikipedia.org/wiki/Moral_Politics_(book):
21:06:06 : indieweb:::
21:06:19 : And: https://georgelakoff.com/books/:
21:06:42 : :::
21:06:51 : Extinction Rebellion also :::
21:07:29 : The Crash Course, by Chris Martenson will help you understand all of the infrastructure in the economy.:::
21:07:34 : I want to repeat my request that we don't try and reinvent the wheel, look locally to work with organizations that are grounded in centering the most impacted folks. BLM, aged out fostor youth, LGBTQ+ youth homeless, and for climate change look for the Indigenous people who have been leading change, many youth who need amplifying of their voices (is great and we need to listen beyond her voice):::
21:07:40 : If you want to explore what you might do after this session, there are sill about 8 more weekly sessions follow #GAIAjourney on Twitter. Here's a sample of the energy they create in their Global zoom sessions https://twitter.com/MITxULab/status/1255748188478283776?s=20::
21:08:49 : This work needs to be HEART led, not MIND led. :::
21:09:17 : Yes, IMO, city level is better… Global Parliament of Mayors:::
21:09:39 : Yes. And cities need to be much smaller, not millions.:::
21:09:46 : California is now a "nation-state" according to Gov. Newsom:::

SSI & Payments Continued

Wednesday 19G
Convener: Cam Geer, Timothy Ruff
Notes-taker(s): Cam Geer

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Discussion on how SSI technologies (DIDs / VCs) can be used to counter significant fraud problems in the exchange of value that exist to without upsetting the economics of the current payments landscape.

Kaitlin Asrow

- Fintech Policy Advisor at the Federal Reserve Bank of San Francisco, specializes in:
  - data portability
  - data privacy
  - artificial intelligence
- confirmed for the groups assumption that in most cases today, money DOES NOT actually move.
  - The Fed flips bits in the ledgers between two member banks to "move money" at the time of settlement
- offered to connect us to her Fed colleagues to further investigate SSI & Payments

Nick Thomas

- Payments relative to COVID

Brent Zundel

- designed sovereign token

Venu Reddy

- building payments rails & integrating SSI

Timothy mentioned the book as an influence

- Identity is the New Money by David Birch
- https://www.amazon.com/Identity-Money-Perspectives-David-Birch-ebook/dp/B00K86O66A/ref=tmm_kin_swatch_0?_encoding=UTF8&qid=&sr=

Timothy also touched on:

- Travel rule
- current system requires a lot of PII needing to go with transaction details and are written in to the permanent record
- Would be great to get ZKP on payment rails to get away from PII being exposed in the transaction record
- US RTGS
  - real-time gross settlement system
- TCH — bank of banks

Dave Huseby mentioned:

- Transparent systems in Seattle

Timothy identified the current problems in:

- Counter Party Risk & Surveillance
    - Dave mentioned this is Ripple's business model in the crypto world

Venu Reddy

- settlement is where the risk is

Timothy described a current market problem:

- APP fraud
- $600 million pounds in UK
- Authorized Push Payment (sender)
- described as a spear fishing attack
    - fraudster gets in between the two parties in a transaction because there is not a secure messaging connection

Other areas / opportunities:

- real estate
- escrow companies
- tax fraud
- no set of best practices in financial institution or market segments
- Kaitlin also mention
    - pull payments where fraud is significant as an area to explore

Potential Solution

- open protocol based on verifiable credentials (vc's)
- Timothy proposed the name:
    - OCTP
        - open counter party trust protocol
        - an end-to-end encrypted messaging layer
        - mutual authenticated by the counter parties
            - could be two or more
- the group agreed this is likely the basis to create best practices

- key issue to investigate
    - what are examiners going to demand for KYC / AML rules
    - how does it connect back to payment systems KYC processes
    - $$ people be confident to meet needs of regulators

Alex Blom asked:

- How will this keep people safe?
    - —when to introduce this in the relationship?
    - — needs discovery
    - — hypothesis — unique to context / industry
    - Mike Lauder / Dave Huseby will think about this
    - assumption / security of private key

Liam asked

- Anyone familiar with RCS?

- verified sender in protocol

the opportunity was described as :

- "DID Comm for Payments"
  - KYC regulation
  - multi party default
  - need to know basis

Will the protocol have pre-defined credentials?

- what's in them
- what's acceptable?
- governance
- transport

Kaitlin mentioned:

- Fed / banks take a risk based approach for KYC
- it's highly contextual
  - for examples immigrants
    - ID challenges

Tim summarized:

- email and phone calls are the real competitors
- move from what you know to what you have
- can involve 3rd party providers
- insure credentials
- Payee has all risk

Dave Haseby offered:

- prime broker service
  - unchained capital — Utah
  - Christopher allen
  - AML
  - CFT
  - OFAC checks

Tim mention another topic:

- micro ledger
- two parties log of all exchange
- fully auditable

Richard added:

- Z-Cash comments

Organizational Wallet

Thursday 19H
Convener: Chris Buchanan (MITRE)
Notes-taker(s): Neil Thomson (QueryVision)

Tags for the session - technology discussed/ideas considered:
Guardianship / Organization / Dependent Wallets

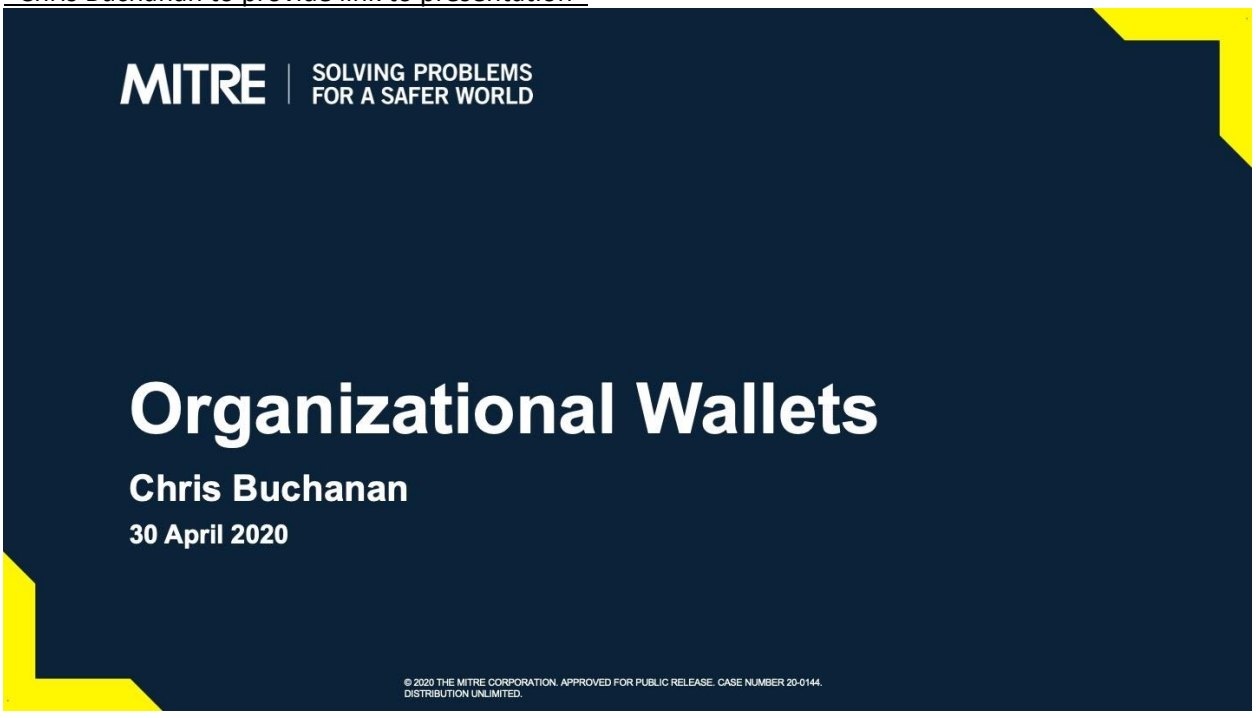
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Organizations are another form of dependent identity. Solving for dependent identity necessary for transition from federation to decentralization. MITRE is working on the model for organizational wallets with intent to transition that capability to government sponsors and would like the SSI community's input on the solution.

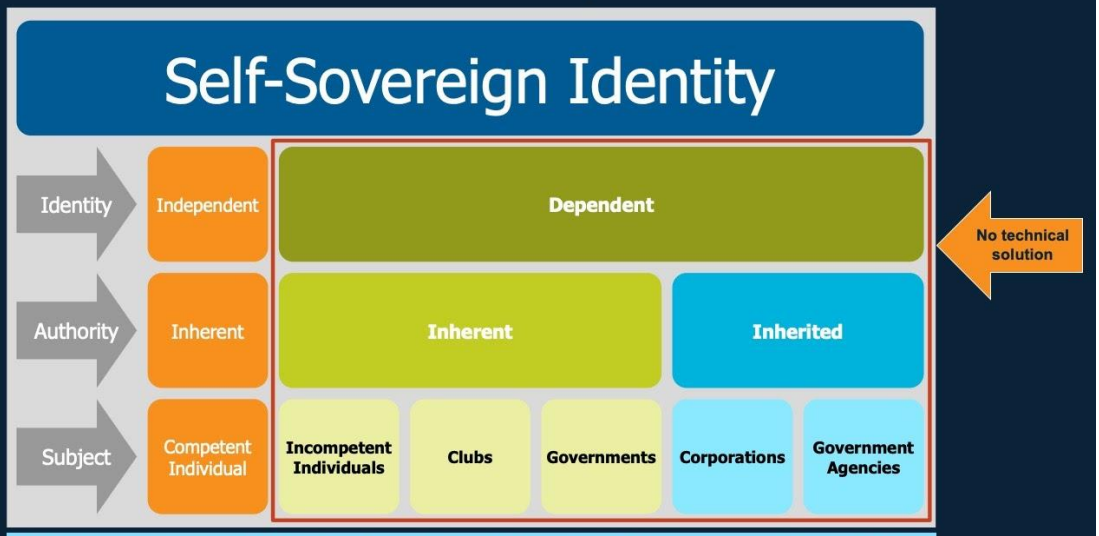
Key conclusions of MITRE's research to date:

- Organization/Individual delegation responsibility and relationships (vs. talking about wallets).
- Need a framework for delegation.
- No definition of a Decentralized Identity, which is clearly NOT self sovereign.
- What other identities are not "self" sovereign?

<Chris Buchanan to provide link to presentation>



Problem 1 – A hole in the SSI ecosystem



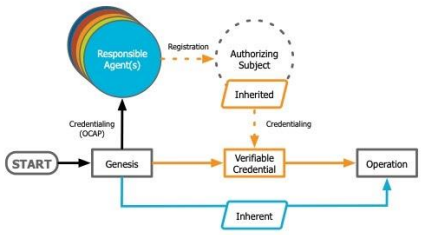
MITRE

Having the mechanism to delegate a dependent subject's authority to one or more independent subjects is *critical to the transition* of digital identity from being federated to decentralized.

Establish and Use Dependent ID

Problem 2: Genesis

How is the initial authority to delegate created?



Problem 3: Actuation

Is the mechanism for the governance of *delegation*, usage, and revocation of authorities embodied in a system or a metasystem?

In other words, is it software or protocols?

MITRE

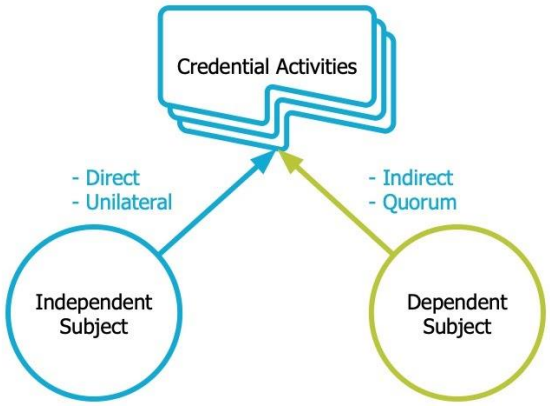
3

Differential Analysis

Independent vs. Dependent Wallets

Activity	Independent	Dependent
Accept verifiable credentials issued to the subject	Must	Must
Store verifiable credentials issued to the subject	Must	Must
Generate verifiable presentations with the subject's credentials	Must	Must
Verify presentations made to the subject	May	Must
Issue verifiable credentials signed by the dependent identity	May	Must
Revoke verifiable credentials issued by the dependent identity	May	Must

Dependent Wallet or Agent?



MITRE

Assumptions

Intent

A dependent identity is formed from the intent of one or more preexisting subjects.

This assumption leaves open the door for one dependent subject to create others, but also creates a recursive loop that necessitates origination with one or more independent subjects.

Inheritance

A dependent subject's authority must be intentionally delegated to authorized subjects.

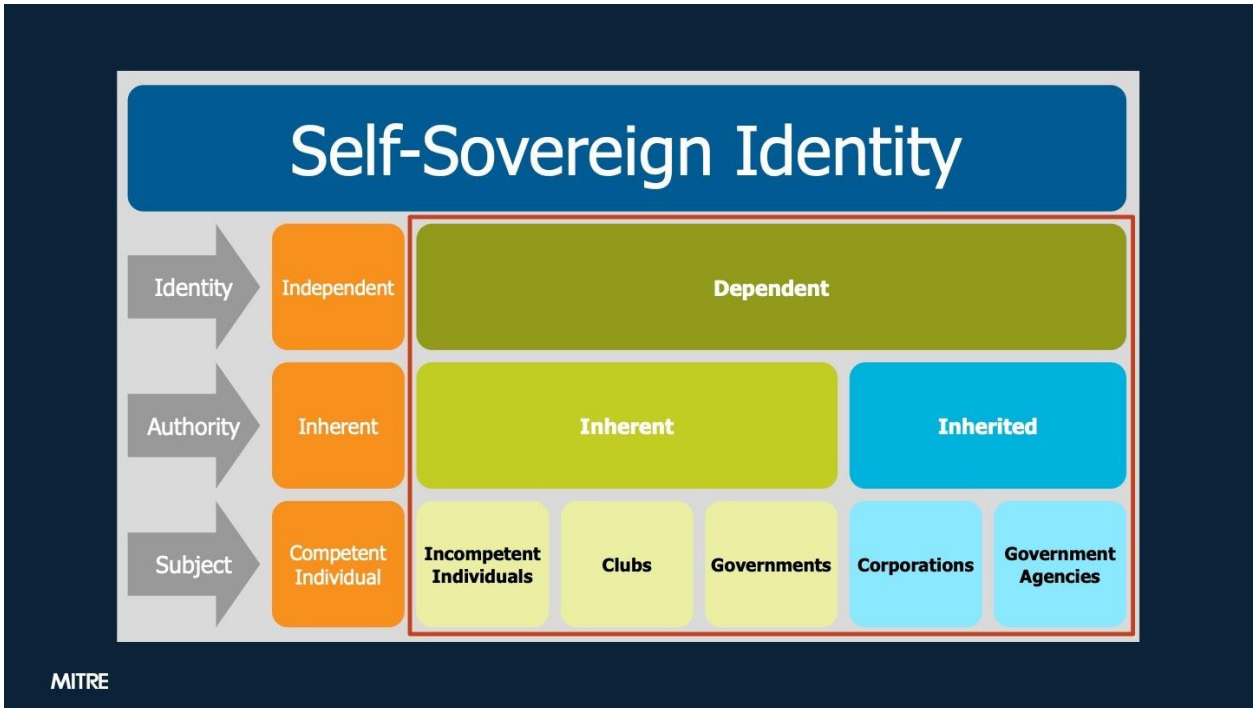
This assumption, when combined with the preceding assumption, ensures that an authorized independent subject must be present in all activities (albeit not directly).

Responsibility

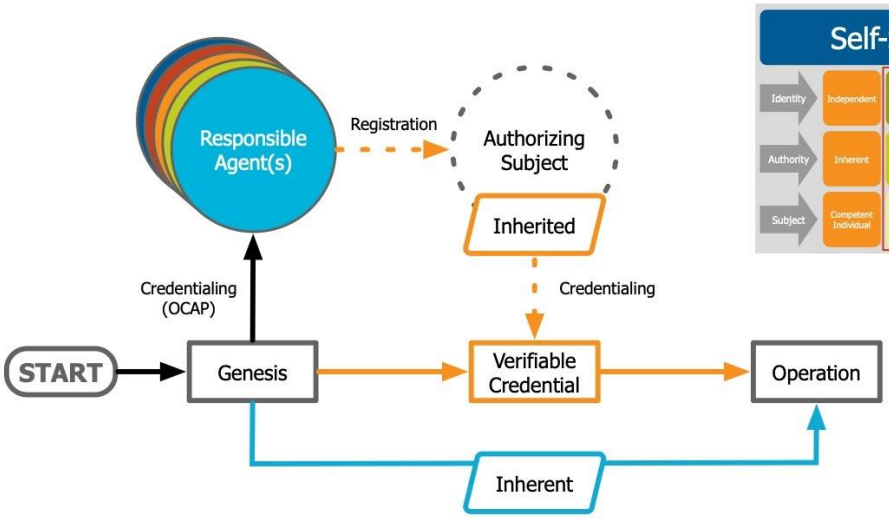
All activities by a dependent subject must be auditable with traceability back to the authorizing subject(s).

Since the authority to act must eventually reside with an independent subject, it is assumed that the traceability of that fact is necessary to proper function. There may be edge cases where this is untrue.

MITRE



Model of Genesis for Authority Types



Responsible for DID from the perspective on how you appear online

Organizational wallet work on hold due to identity (due to COVID-19)

Dependent identity - (incompetent individual - child)

Government Agencies inherit authority from the government

Looked at difference between inherent to inherited authority, in reality it does not actually exist

Mitre cannot get rid of Active Directory, because it cannot be in charge of itself - so cannot self sovereign identity itself

So that was a driving use case for an organizational wallet

Problem 2 - How does a dependent person, where does the authority come from to self-identify? Organization is liek a dependent

Problem 3 - actuation - (see slide 2)

Differential Analysis
- [Dependent] wallet and agent blur

An Independent entity has to prove it has authority over a Dependent Ideentity and which scope.

Starts to look like the Active Directory model

Assumptions
- dependent identity doesn't appear out of nowhere (child). Independent creates the dependent
- Dependent chain of delegation traceable to an Independent Identity
- Dependent actions/operations must be traceable to the related Independent [authority] source
-

Model of Genesis
- starts with a human interacting with software (responsible agent(s))
- DMV inherits from the Governors office

Responsible agent - people with fiduciary responsibility over the dependent (advocate)

Additional Ecosystem Roles required

- Trusted Agent (e.g. NIST SP 800-63A)
- (access) Role Manager (e.g. AWS Identity Access Manager)

Darrel: CIOs do not want to hand over control to SSI system. CIOs will now get locus of control they did not have, but should have had. When I sign off on SSI for the organization. Organizations will want traceability, where SSI permits non-traceable.

Actual privacy will change - in a different way - you will not be unknown. Goverments will be able to pierce the anonymity.

Chris: defining the specifications/behavior of the Trust Agent and Role Manager - which mentally maps to the AWS IAM

Paul: One wallet for the whole organization (including individuals)? is this there to verify relationships?

Chris: Organization has a wallet, but individuals have individual wallets. Organization will allocate credentials to the individual wallets

Paul: Pan Canadian Identity model in Canada. Org representative ability to act on behalf of the organization (wallet) - someone with "signing authority". Delegated to present organization credentials? and Act on behalf of the organzation (in a role)

Chris:
- DMV model with license issue. individual wants state of Virginia to "Sign" the license, not the person behind the counter. Direct signaturs from the state. Sally has a credential to ask the organizational wallet to sign the license (issue the credential) fpr the driver
- If you are an officer within the DMV is that you (in that role) to generated the credential directly vs. via the organizational wallet

Paul: Governance - Busines registry has authority to issue and verify credentials.

Chris: Not talking about just an agent or wallet, but a combined endity

Paul: organization does need the ability to delegate authority

Chris: Drummon Reid and I have talked about this combined function (needs a new role/name) - it's really a organizational identity system

Chris: recognize that need use cases and interaction diagrams. Will clarrify the distinction

Richard: ARES, Glossary E covers some of these issues. Some wallets follow the model of being a bucket of credentials. Others, split up the accountabiltiy across multiple individuals, where the individuals have a wallet, but not the organization or hybrid

Chris - we are using a hybrid - both Org/Individual wallets with delegated relationships.

Will Groah: Where is this going? See this merging with Marla Ozarowski
on Grants Management

Chris: working with State of Maryland - use case licensing of charities. Transition path do a reference implementation within the State. It's a complex system (not just state and charity)

Will: Grant Management/Org wallet overlap, will converge? Both have mutual problems to solve (even)

Margo: Session on Glossary session on working definitions (later today). Vocabulary needed to differentiate these terms. How a could an organization communicate what roles/permissions to other organzations on how external organizations work with it.

Chris: Current use case does not involve working with other SSI systems. How do we move away from federated identity. To do so you need an organzation "wallet/agent". Otherwise you are in limbo (neither federated or decentralized)

Margo: Transition will be difficult (my house, my rules) from Federated to decentralized. Don't want to share need to know information outside the organization

Chris: lots of people thinking about it. Competing ideas/implementations. Happy to contribute a base for a reference architecture.

Paul: How would model work for individuals who representative of multiple organizations (PAD or insurance agent)? Combined wallet or wallet per organizations.

Chris: Wallet could handle credentials from multiple organizations. Charities must agent to collect funds. With non-trivial set of interactions (multiple organization and individual wallets/agents). Lots of inter-credentialling. State <-> Charity <-> Agent (and back to State)

Paul: PAD (Patent Agent) agent example - rep for 10 companies. Need credentials for each company. Wallet for each or Wallet with sub-wallets.

Chris: one app on the phone. Credential is an independent item that can be presented from a single wallet.

Chris: Identity is transactional within a context. If you are being asked for verifiable presentation. The Patent office has to spec that corporations issue a specific patent office credential to PA.

Paul: so could have diffent "folders"/containers for each company credential sets that you representation. The service says here is the type of credential, which the wallet presents and the individual picks which instance of the credential to present

What will make sense to the business user (the human agent)

Chris: not much demand for this from a UX for this (back end). For the human selecting in the wallet, this is a simple selection process. Implementation issue for Wallet. Mitre in the business of the back end reference architecture

Chris: want to have organizational signatures. Dependent (corp or child). When to use the identity in a transation, you want that to be actual entity is the dependent entities signature. Have role based access to control to make that happen (acting on behalf of the depedent for the dependent to "sign"). Could be via a Quorum mechanism. Family custody may dictate may be several appointed family members (e.g parents die, god parent authenticated to act). Don't want to limit the wallet functionality, but cover the 6 key functions outlined in the presentation

The key piece is the Gensis of the Dependent/Independent roles/permissions.

Such as vehicle where the owner can delegate to the mechanic to do certain operations on the vehicle (which is the dependent)

Chris: How we deal with dependent/independent relationships in a corporate setting is the key aspect.

Mouse Head Model (MHM): A Global Solution For Safe & Secure Data Sharing

Thursday 19I
Convener: Paul Knowles
Notes-taker(s): Paul Knowles

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

In a harmonious Decentralised Data Economy (DDE), SSI technology has given rise to the most compelling component of assurance, a Verifiable Credential (VC) – a digital representation of a physical credential but more tamper-evident and more trustworthy than their physical counterparts. VC characteristics are compelling for human-to-human communication. This resides in the Credential space.

However, to enable a safe and secure data sharing economy, the female side of the model takes the lead. A phrase coined by Philippe Page, President of The Human Colossus Foundation, for decentralized data capture components is Decentralized Semantics. In the schema side of the model, the Overlays Capture Architecture (OCA) facilitates a unified data language so that harmonized data can be pooled into multi-source data lakes for improved data science, statistics, analytics and other meaningful services.

It is in the synergistic combination of the assurance characteristics of a VC and the immutable, yet interoperable, components contained in OCA schema that privacy compliant data sharing can be facilitated in a DDE.

In the Mouse Head Model (MHM), the left “ear” contains purpose-based services (PBS) - entities that issue schema for initial data capture into a DDE. The right “ear” contains meaningful service providers (MSP) – entities that enrich data by combining criteria searched data from harmonized data lakes. Consent is always obtained by the subject before data portability is actioned. VCs provide the mechanics to verify that the data flow stems from an assured source. At the heart of MHM is the OCA transformation tool required for data harmonization prior to data porting. In this single sector use case, the processing for consented data capture and associated credential exchange is treated as a separate process to the equivalent data sharing flows. In the case of an emergency response situation, such as the COVID-19 pandemic, those two processes are combined to speed up urgent data portability to any specialised agencies responsible for national and international public health

Video link from the session provided by Paul Knowles ...
https://drive.google.com/file/d/1TbUtUMjl_dbGQSlU0CMph2cFXhxMCD_p/view?usp=sharing

Overview of VC / DID / JSON-LD Interoperability Plug Fest

Thursday 20A
Convener: Anil John
Notes-taker(s): Melanie Nuce

Tags for the session - technology discussed/ideas considered:
multi-vendor interoperability, DIDs, VCs, standards

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- US Department of Homeland Security Silicon Valley Innovation Program (SVIP)
    - https://lists.w3.org/Archives/Public/public-credentials/2020Apr/0198.html
    - Not an R&D program; goal is to incubate projects that will eventually be implemented by Government Agencies in production
- Solutions to prevent forgery and counterfeiting of certificates and licenses
- Goal is to move paper-based processes to interoperable digital processes
- Focused on:
    - Issuance, validation and verification of certificates licenses and attestations
    - Storage and management of certificates, licenses and attestations
    - Consolidate decentralized and derived PIV credentials
- Security, privacy and interoperability: foundational principles; leveraging open APIs
- Projects to incorporate (as much as possible) the following components from W3C: DIDs, VCs, JSON-LD
- Product Focus Areas:
    - Raw Material Imports (Timber, Steel, Oil)
    - Permanent Resident Card (digital issuance)
- Why are DIDs important to this process: DIDs provide assertion of sameness (prove you are talking to the same person)
- All participants must prove interoperability across multiple implementations
- It is not enough to "talk about" interoperability; you have to DO IT
- Interoperability levels being assessed
    - Wallet
    - Issuer
    - Verifier
- Challenges to demonstrating interoperability
    - Tension between "interop" vs. one-way of doing something; the difference is whether multiple companies can utilize a set of tools vs. just one
    - For example, use of CHAPI (Credential Handler API) test plan, which has been extremely helpful
        - Test suite: https://github.com/w3c-ccg/vc-examples/tree/master/plugfest-2020
- Work going on to support Zero Knowledge Proofs across multiple implementations (Tobias and Kyle were mentioned)
- DHS looking for a competitive ecosystem of diverse solution providers
    - Critical to build on top of an interoperable framework, no matter what platform each company chooses

- Interoperability should not be underestimated
    - SVIP has been a great forcing function to drive the priority
- There is a potential to test interoperability between companies in the SVIP cohort and those that are outside. DHS to confer with cohort participants to determine feasibility

Group Identity Part 2

Wednesday 20B
Convener: Will Abramson
Notes-taker(s): Will Abramson

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This session was essentially a repeat of the first one held Day 1 - on Group identity.
This session posed two questions:

1. How do we model the identity of groups and our relationships to these groups and within these groups?

2. How the tools we are all building help us do this?

Link to additional notes provided by Will Abramson:
https://docs.google.com/document/d/1ENWEMiEB4xa-RbEwwlavw-iF72wkxVKqgKWT_uVMsQs/edit#

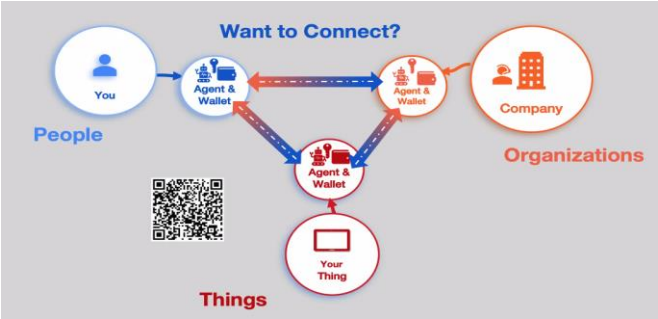
The Future of Telecommunications is DID Comm

Thursday 20D
Convener: Vic Cooper & Seth Back
Notes-taker(s): Bruce Conrad & Others

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Note: the session was recorded <**link here?**>
"DIDComm is your own private VPN"

On A couple of points from Seth's slide deck <**insert link to slide deck here**>
"Transport agnostic security"
"Strong identity guarantees"e diagram from Vic's slide deck <**insert link to slide deck here**>



Questions

Sam Curren. There is a DID for the conversation. Vic. the item, the bot, the live agent, the caller are all parts of the conversation. Sam: the management of a group. there is an agent which moderates. conversations which legally require auditing; the bot can do that, and store elements of the conversation. Is this what you're doing. Seth: yes, the conversation object was always very important.
Vic: from a telcom perspective, you are now choosing the channel first and then directing the conversation. here the conversation is created first; when an agent becomes available, you can choose the channel -- messaging, phone, etc. The conversation can span many interactions. It is more like a case. But the company isn't opening the case, you as the customer open the case and control it, without having to remember a case number. Sam: that's awesome

Marc Davis: multiple high fives. an abstraction of channel and device. an enormous opportunity. about presence and availability; is that built in? (see also conversation in chat). Vic: an organization could fit this into its web chat area; web chat with benefits. once established, can turn on audio, or Zoom conversation. Very difficult to spam because you don't have a public endpoint. If one of your channels is misused, you can just shut it down. Seth: you have to be added to the conversation before you can send messages about it.

Vic: case of a credit union where people are receiving calls that appear to come from its 800 number. How do you stop this? Now, you can't. The agent which represents you operates almost like a web site. When I call my bank, I have to go through a ritual to identify yourself. But how to identify the bank?

Andrew Whitehead: good work, this is cool, more work with DID Comm transports than I've seen before. With the payload inside of JSON, wonder if you could use a binary transport instead to reduce overhead.

Seth: we use protocol buffers a lot internally so it's quite a bit faster. I like binary protocols. We push our message stream through the nats that way.

Ryo Kajiwara: thank you for the talk. email lacking identity. This looks like the future of email and messaging going forward. Where can I look for information? Seth: we relied heavily on the Aries RFCs. What we're doing is a bit of a departure. There is a huge amount of information and it's like drinking from a firehose. Vic: for a couple of weeks I couldn't talk to Seth; he was busy understanding. Sam: working on DID Comm version 2, so there is information available. Vic: what is email exactly; is there a way it could go over the same kind of channel; definitely "yes."

Ben Weaver: saw the demo, an example of me as a customer reaching out. We talked about spam. my email address or phone number can be shared around; but it allows my friend to share my number. How can inbound be facilitated? Vic: you can do introductions over DID Comm. Seth: There are "introduction" RFCs in Aries. For our purposes the communication can add users to the conversation.

Vic: also how do you connect to a rep from a company. the initial connection is to the company and they add that person in. We have personas: my work persona, my friend persona, etc. The company has people representing them, but all conversations are routed through them.

Dave Sanford: having a fantasy about having “allow” lists. one problem are all of the aggregators using web beacons etc. then they direct content to you. I want to unpeel the onion and aggregate into my devices myself. DIDs inside of DIDs. Vic: When you connect to a company you start by connecting to the agent (now, generally a web site). Once you make the connection they can use that to send content intended only for you. You could go even further and know that all my interaction with the company is going through the (something like a) VPN. Dave: a good citizen will behave well, but everything becomes
a gateway and the company may want to pass content on to you that they get from someone else. Vic: were only scratching the surface

Ben: thinking again of spam; trying to connect this back to basic trust. How do I know I have the correct company? in the presence of all those phishers out there. [in the chat, people are saying, “Trust Frameworks!”] Vic: there’s an element of human trust, organizations that may certify the company.

Vic: the possibility of no more passwords or pins, no more waiting, should unlock faster better business processes, reduction of compliance costs, one-click customer support. The whole point of this is to reduce effort. What used to take ten steps (or a hundred) now just takes one. Goal is effortless communication.

Zoom Chat Content:

From swcurran to Everyone: (1:28 PM)Could someone ask the host if this can be recorded? I'd love to hear this session, but can't make it.
From Josh Verbarg (State Farm) to Everyone: (1:33 PM)You can set that yourself too.
From Sam Curren to Everyone: (1:33 PM)I have. :)still a help for new folks though.
From Josh Verbarg (State Farm) to Everyone: (1:33 PM)very true
From Andrew Whitehead to Everyone: (1:39 PM)Possibly four DIDs..
From Andrew Whitehead to Everyone: (2:03 PM)I think that comes from the model where the ‘wallet’ is the only storage.. I think gradually things are moving away from the term wallet towards multiple specialized backends
From Drummond Reed to Everyone: (2:03 PM)+1
From Geovane Fedrecheski to Everyone: (2:05 PM)@andrew Just to make sure I got it right: "app wallet" and "cloud backup service" would be examples of those specialized backends?
From Andrew Whitehead to Everyone: (2:06 PM)The current division is probably more like KMS (key store), credential storage, protocol state - Mike Lodder has an Aries RFC proposal with more details on the proposed storage architecture requirements
From Drummond Reed to Everyone: (2:06 PM)We definitely need the DIDComm spec to define one standard DID document service endpoint type for requesting a DID connection.queue?
From Nathan George to Everyone: (2:07 PM)The original though there was that the service endpoint was sufficient to specify that, but perhaps implementations haven’t fully implemented that?Drummond++Is whipped cream really whipped if it isn’t whipped with whips?
From Marc Davis to Everyone: (2:09 PM)I have some questions when at relevant point in presentation: 1) Do you have a model of “presence”/“availability” of communicating parties to enable communicating parties the way IM does? 2) Do you have a model of channels of communication (e.g., sms, email, IM, voice, etc.) and devices (phone, PC, etc.) to enable smart routing of messages and to most present/preferred channel+device?; 3) Can your architecture support better spam filtering of incoming communication requests, and if so how (Trusted connections? Reputation scores across multiple connections? etc.?)?
From Ryo Kajiwara to Everyone: (2:10 PM)+1 on spam filtering, would like to know about that

From Drummond Reed to Everyone: (2:10 PM)Who let Marc Davis in to ask all the graduate level questions?? ;-)
From Drummond Reed to Everyone: (2:11 PM)We're still in elementary school here :-)
From Andrew Whitehead to Everyone: (2:11 PM)I think didcomm+https:// or similar
From Marc Davis to Everyone: (2:11 PM)+1 Drummond ;-)
From Nathan George to Everyone: (2:11 PM)A few spam approaches: didcomm means mutual authentication and if you attach proofs for attributes you get signed/certified attributes that can't be spoofed, so you can request real legal names for orgs and people, next payment decorators can allow for staking like "if this call isn't worth it to you, you can collect my X dollars/cents" (spam insurance if you will).
From Nathan George to Everyone: (2:13 PM)I think the proofs on top of the connect protocol means that you can fully authenticate existing protocols, track where introductions come from because the intro comes in on a correctable channel and as a result you don't need the "connect stamps" stuff that never took off in email except for extreme cases
From Drummond Reed to Everyone: (2:13 PM) +1 to all of Nathan's points. IMHO one of the MOST important points about DIDComm is that it runs over DID-to-DID connections and so once you establish a secure, private connection, you KNOW that messages on that connection are authentic unless the other party's keys have been hacked.
From Nathan George to Everyone: (2:14 PM) I want all my caller ID data notarized by someone who collects money from you regularly. That way there is an appeals process for gross fraud.
From Drummond Reed to Everyone: (2:14 PM) While that's not a non-zero risk, it's SO much less of a risk that all the wide open vulnerabilities in non-secure messaging protocols today.
From Marc Davis to Everyone: (2:14 PM) I am imagining a spam filtering approach that uses trust across multiple parties in the network too create a reputation/trust score without sacrificing anonymity and that can be personalized to the querier based on a "transitive trust" assumption across your trusted connections and their trusted connections, but done anonymously.
From Marc Davis to Everyone: (2:14 PM) Typo: to create
From Drummond Reed to Everyone: (2:15 PM) I gotta run to another session, but I just want to say I LOVE the name of this session. DIDComm really IS the future of telecommunications (in fact nearly all digital network communications). It is THE protocol at the thin waist of the Trust over IP stack.
From Nathan George to Everyone: (2:15 PM) The think I love about HearRo's model is they then share common authentication across lots of channels so my caller id and my web chat and my email can all aggregate into a coherent dialog centered on a relationship
From Marc Davis to Everyone: (2:15 PM) +1 Nathan George. That is what I was hoping for, and then to use that to enable smart routing.
From Nathan George to Everyone: (2:16 PM)Cool. Signal if you have it, fall back to apple, fall back to ..
From Drummond Reed to Everyone: (2:17 PM)I'm in exactly the same camp as Vic. I don't accept calls from numbers I don't know.
From Ryo Kajiwara to Everyone:Some questions: (1) Is DIDComm able to do multi-party communication or encrypted group communication? (2) Are there technical resources I can look into to start? Are there "unopinionated" (not tied to a specific implementation such as Aries) specs for DIDComm itself?
From Josh Verbarg (State Farm) to Everyone: (2:18 PM)Phone system can spoof numbers though. So I just need to know what numbers you trust.
From Drummond Reed to Everyone: (2:18 PM)HeaRo is one of the first companies I know that's recognized the full power of DID-to-DID connections Vic, you just need to give big bucks to Joe's campaign and then politely ask them not to send any more emails ;-)
From Nathan George to Everyone: (2:18 PM)Group messaging is a hard problem. We have good thoughts there and the crypto is catching up. I would love a chance to take on that part of the problem in open source code, but no one has funded that work directly yet.
From Drummond Reed to Everyone: (2:19 PM)GET NATHAN SOME FUNDING!!!!!

From Me to Everyone: (2:19 PM)+1
From Andrew Whitehead to Everyone: (2:19 PM)MLS is another standardization effort for group messaging, still in the draft proposal stage
From Drummond Reed to Everyone: (2:19 PM)Gotta run to another session, but GO HEARO!
From Marc Davis to Everyone: (2:19 PM)In the Joe Biden example, would it be able to automatically work across all channels and devices a person uses? It is a form of universal “unsubscribe” which would be awesome.
From Sam Curren to Everyone: (2:19 PM) actually, HearRo might have done something here about group communication, in one form at least.
From Vic Cooper to Everyone: (2:20 PM)Yes, all channels. It’s connection first then channel
From Nathan George to Everyone: (2:20 PM)(Group signatures that ratchet on message delivery would force catchup and prevent those who left the channel from getting message delivery outside their time as a channel member — so it should let you do cool stuff — the crypto papers are there but the performance may not be, yet.)
From Ryo Kajiwara to Everyone: (2:20 PM)yeah, I wanted to know how MLS can tie into DIDComm. It looks like a good mechanism to use in combination with DIDComm
From Nathan George to Everyone: (2:20 PM)This ^^^MLS should be a good encryption format for group DIDComm messages, but AFAIK it isn’t far enough along.
From Andrew Whitehead to Everyone: (2:21 PM)I have issues with the MLS approach, because the trade-offs for a small group (<100) to a big group (10000) are very different
From Nathan George to Everyone: (2:21 PM)Probably a case of needing different approaches for broadcast vs private groups with peer messaging
From Andrew Whitehead to Everyone: (2:21 PM)Just attempting key management with that many parties seems silly
From Nathan George to Everyone: (2:21 PM)Once you have that many parties it helps to differentiate between speakers and listeners
From Andrew Whitehead to Everyone: (2:22 PM)Good point
From Sam Curren to Everyone: (2:22 PM)also, mediated groups vs peer groups.
From Ryo Kajiwara to Everyone: (2:22 PM)good point > differentiation between speakers and listeners
From Nathan George to Everyone: (2:22 PM)(If you love this type of discussion on MLS join the Hyperledger Ursa and Sovrin Crypto Calls, we would be happy to put folks to work integrating these ideas)
From Me to Everyone: (2:22 PM)love the GET SUPPORT button
From Sam Curren to Everyone: (2:22 PM)peer groups require no infrastructure. most large groups will need some style of 'management' that can help there.
From Marc Davis to Everyone: (2:22 PM)Do you have a model of how people, roles, teams, and organizations are related to support routing of messages to the relevant level?
From Ryo Kajiwara to Everyone: (2:23 PM)Thanks for the pointer, will look into those calls!
From Vic Cooper to Everyone: (2:23 PM)We use credentials to allow a representative to be a rep for a company and join a conversation
From Nathan George to Everyone: (2:23 PM)^^^ Revenge of the library sciences it is an ontology problem. Peer to peer private lets you model those aggregations with credentials
From Marc Davis to Everyone: (2:23 PM)Universal Unsubscribe is a killer feature.
From Sam Curren to Everyone: (2:23 PM)does the conversation itself have a DID and relationships?
From Vic Cooper to Everyone: (2:24 PM)Yes, the conversation has it’s own identity
From Nathan George to Everyone: (2:24 PM)Sending encrypted data to everyone that only some people can decrypt is a bad story (crypto eventually breaks)
From Andrew Whitehead to Everyone: (2:24 PM)Nevermind multiplying bandwidth by ’n’ for the sake of hiding who is talking to whom

From Nathan George to Everyone: (2:27 PM)Seth++
From Nathan George to Everyone: (2:28 PM)Drummond: Agents are now for people, organizations, things, and conversations ;)
From Geovane Fedrecheski to Everyone: (2:28 PM)A way to allow many to many, end to end encryption, is attribute based encryption (ABE). I don't know much about it but maybe credentials could be used as attribute sources for that.
From Nathan George to Everyone: (2:29 PM)Geovane if all the keys are pairwise you don't have to go that far, the derivation (if needed) is just an optimization, as you can associate the attributes with the new keys you roll when you initialize each new interaction
From Nathan George to Everyone: (2:35 PM)Andrew++ WebRTC as a communications channel is underrated
From Andrew Whitehead to Everyone: (2:38 PM)Although the layering of DTLS over SCTP over UDP or TCP hurts a little :)
From Sam Curren to Everyone: (2:42 PM)There is an Aries protocol for introducing alice to bob.
From Marc Davis to Everyone: (2:42 PM)Like LinkedIn Inmail perhaps?
From Andrew Whitehead to Everyone: (2:42 PM)The Tinder protocol Sorry I mean Introductions
From Sam Curren to Everyone: (2:42 PM)lol Andrew. For orgs, a public DID can bootstrap into a peer connection. the did:peer method is awesome for preventing spam.
From Marc Davis to Everyone: (2:44 PM)Excellent: Person vs. Role/Persona
From Nathan George to Everyone: (2:45 PM)You don't have to attenuate everything into capabilities when you have ZKPs credentials, you can associate capabilities directly with attribute values or combinations of attribute values and not disclose the irrelevant parts.
From Andrew Whitehead to Everyone: (2:50 PM)Trust frameworks!
From Sam Curren to Everyone: (2:50 PM)Trust Frameworks!
From Andrew Whitehead to Everyone: (2:50 PM)LOL
From Sam Curren to Everyone: (2:50 PM):)
From Marc Davis to Everyone: (2:50 PM)+1 Trust Frameworks!
From Nathan George to Everyone: (2:51 PM)This is where you need pivot points between different trust frameworks, you want a thin global interop type layer that just helps the different frameworks translate between each other.
From Sam Curren to Everyone: (2:51 PM)TOIP FTW
From Marc Davis to Everyone: (2:54 PM)@VicCooper and @SethBack: Fantastic session and opportunity! Thanks!
From Sam Curren to Everyone: (2:54 PM)Awesome work!
From Randy Warshaw to Everyone: (2:54 PM)Will there be a link to the recording?
From Ryo Kajiwara to Everyone: (2:54 PM)Again, thanks for the talk! It looks exciting, and I will definitely look into the tech side of this!
From Nathan George to Everyone: (2:55 PM)Excellent work guys, look forward to more protocol integrations across the open source stuff.

Magic Sandwiches

Thursday 20E
Convener: Justin Richer
Notes-taker(s): Neil Thomson

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Normative vs. non-normative
Normative (examples) - you have to pay atention to
non-normative (examples) - an illustration, example - not a specific requirement

The non-normative text can have unexpected consequences (and influence)

Despite the "musts", "shalls" in the specification

In DID working group - text referring to a separate document that implied it was normative. (e.g. requirements can be found in this other document)

Should have been - the other document was, for related details of interest (only)

"Sandwich" comes from DID <magic> DID Document, where magic is the "meat"

Working group was averse to specifying the magic. The consequence was that the community disagreed with where the boundaries were. Were arguing "stuff" had to be added to DID or DID Doc, where it should have been defined as contracts as to how to get from DID (input) to DID Doc (output)

Problem of where the abstraction lines are drawn are key to all the standards discussions.

If you don't specify enough about the implementation in the specification, you get problems.

Yet the implementation provides key context which changes how you achieve security, etc.

Do you put that in the contact requirements or in the implementation notes?

Because implementations are wildly different, what happens is separate groups with their own implementation guidelines.

Should be able to abstract that as to inputs, behavior and outputs (interface contract use cases)

Blog post (need link from Justin Richer) on Sandwich concept.

Any arguments on implementations were about the boundaries with the magic.

Pointed out that this applies in many areas, including UI/Interfaces.

But isn't this what Architecture (decisions) is all about.
Look @ OAuth - many ways to get tokens, use of them, refresh, etc. etc.

That it is opaque to the applications was the real abstraction, not that their can't be several different implementations (under the hood).

Different levels of abstraction are required (and possible)

Suggested - do you need both the abstractions for the contracts AND the implementation guidelines (need multiple inputs on how to think about the solution). More guidance is "considered helpful"

Usually hard to get agreement on the details (even given specific use cases). Consensus disagreement on where each perceives where the implementation needs to support variability (in the future).

"Too many cooks" problem where people want to be compliant with standards. But it is not mandatory to support/implement all the possible applicable standards.

Why use standards at all (interop). DID Com doesn't specify a transport layer. Utility to who. As you add more and more specification (away from the abstraction), you then can shut out some groups with needs that actually are compliant with the abstract/intent.

Standard example where over specifying killed it (as didn't actually fit any real world situation)..

SOAP as an example (incredible of detail) for many things. How to figure out how to do the few simple things that were actually useful was made very difficult.

Complex client, sending complex message over complex protocol to a complex server.

SOAP was hurt by that complexity for simple operations, which resulted in the much simpler REST which essentially replaced it

DID Resolvers are unspecified - can't possibly support all the details of all the DID methods.

Not specify how DID resolvers work, but the core interactions/interfaces (in/out). Push back is that it is both it is overspecified and underspecified.

Alan offers condolences for everyone working on standards. Disagreements based on different understandings of the facts and what they were trying to build.

Misunderstanding of specifying inputs/output/ interfaces vs. specifying network protocols

When writing specifications - treat it like programming. Normative statements are like lines of code that have to run on the most unreliable execution platform - which are software engineers

Overspecifying that a DID needs a private key.

There can be many different levels of interoperability.

DIDCom is not a protocol. It is a set of ideas that does not define boundaries. It's an abstract model of 10,000 foot behavior
DID operations are at multiple levels of abstraction. Variability (http, etc. for comm channels)).

Have a DID, I did a DID document, what if more information needs to be passed than the DID and more coming back than just the DID document. Implementations all work in their own space, and work, but they cannot agree on what they are specifying.

Like passing around an unspecified variable vs. a numeric variable

DID Document (byte stream) [Function] Resolve(DID, Options)

Where byte stream which includes metadata

If you are a resolver you must implement the above function. You can do other things, but that is the minimum.

If you can tell me how to send you the string that represents the DID and the map of string/string to map the input options to generate the DID Doc. The goal is a generic interface - only strings, not even JSON (could be XML).

Standards tend to act like something is not complete until there is nothing more to add. The goal really should be a standard is complete when there is nothing more to take away.

Link: to DID-Core specs https://github.com/w3c/did-core/pulls
Especially 253, which is now 262-265

A dereferencer is different from a resovler in that it (potentially) different inputs and outputs (And behavior) even though the input and output (DID, DID document) are the same

There is metadata about the document. The metadata is data ABOUT the document that is separate from data IN the document.

Response Headers are one area of contention.

Example DID vs DID URL

What is a matrix parameter - different form of query specification - turns out to have been a bad idea.

The idea behind the contracts discussion that could map to http or other mechanisms (uses a map of strings could be http headers). Exactly how you do this is up to your implementation.

People are biased in thinking about their implementation vs. the abstraction.

This is also about architecture and design partitioning, with the example of partitioning interfaces

The goal of abstraction (of interfaces) is able to call a function, without consideration for the underlying implementation

What is the part we want variability on and what are the limits on variability. Some level of input, output and behavior is required.
OAuth for device flow (for set top boxes). Two implementations. Assumption made on the optionality on the field (optional) on the time between multiple requests. One implementation put in default of (time=0),

which swamped the system that assumed not specifying the time between would result in something reasonable, not that 0 would be a reasonable.

This effectively is a bug in the spec - it wasn't specific enough (e.g. if not specified, cannot be 0, with default is <non-zero default behavior>. In order to have a sensible default on both sides (client/server).

We're good at behavior when specifying mandatory values with specific ranges, with optional values which leave ambiguous as to what to do if not specified (e.g. default value).

Clarity for humans is vitally important.

Need to explain it for humans, but specs should use formal language to specify (and be unambiguous).

Are there people on the standards committee who have the skills to do formal analysis.

[Standards] People tend to be one of two extremes - too abstract (with no understanding of implementation) or too (specific) implementation centric (with no understanding of abstraction)

Standards can be created too soon - before there is sufficient practice to create a pragmatic standard.

The RUST core in the standard is very small with everything as an external library, which are then pulled into the core as it is proven. However, this approach allows different competing libraries, where one wins and is pulled into the core, which breaks apps built on the other equivalent libraries.

There is tension in both directions over vs. under-standardize.

The reality is iterative and incremental - get it as right as possible right now and then fix as used.

Get a complete set of use cases - with the core set of high use cases drive initial implementation with a strong set of edge cases to think about the breadth of the standard that have to be solved at some later level.

Proving Security for Web Protocols

Thursday 20F
Convener: Daniel Fett
Notes-taker(s): Daniel Fett

Tags for the session - technology discussed/ideas considered:
OAuth 2, Formal Analysis, Security

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

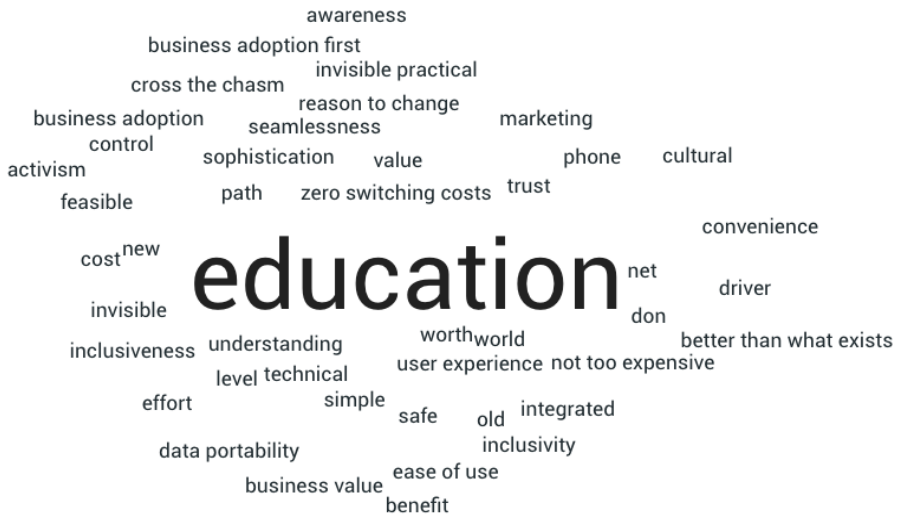
https://danielfett.de/publications/2018-10-19-an-expressive-formal-web-model/

Defining The Growth Factors of SSI

Thursday 20G
Convener: Adrian Doerk
Notes-taker(s): Adrian Doerk

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Word maps:
user-adoption: Education, Zero switching costs, etc.
comments: We think too technology focused - focus on the user,



governance framework:
regional aspects need to be considered, granularity of credentials, trust is build over time, decentralized governance via e.g hedera hashgraph, tyranny of the majority, no harm principles,

business:
clear responsibilities of stakeholders,
who are the users?

Government usage:
willingness of data sharing with gov. can vary in different jurisdictions
Abstract government structures complicate things, localization is favourt

SSI: When I Should Start Charging My Cutomers?

Thursday 20H
Convener: Robert Mitwicki
Notes-taker(s): Robert Mitwicki

Tags for the session - technology discussed/ideas considered:

SSI, Business model, monetization, value chain

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

KYC is not cheap and SSI and VC can reduce the costs by far.
One of the most popular assumptions is that the verifier is the one who will pay and should pay as this is an additional value for him. But in the current model this does not necessarily hold. If you show your passport in some foreigin country they are not paying to see that credential.

The value is not in data but in the data flow. Data is like electricity it has value when it flows.
Seems like monetization of the VC could harm the adoption. Especially that a lot of analog credentials are "kind of free".

How often do you get new credentials? In many cases is not the thing which flows through the system.
Variable source of data has a value but more value comes with data flows itself.
SSI brings identity to the next level - makes the PKI simpler and cheaper but that is not what we are after.

Users not necessarily would like to take the responsibility for their identity, so they probably would not want to pay for it either e.g. paying for wallets. The costs would have to be pushed to the companies or organizations who benefit from letting people use digital credentials because this reduces their costs.

SSI is an enabler and unlocks new ways of building businesses with a more consent driven way and allows data to flow. Seems the biggest value is behind the hill called VC. VC is just a key to unlock new stuff and this new stuff will bring the biggest value.

Zoom Session Chat:

21:43:28 From Paul Dunphy : @sebastian - did Commerzbank make any conclusions about SSI?
21:44:19 From Sebastian Bickerle : Still exploring the space via lissi.id
21:44:58 From Paul Dunphy : Thx
21:48:06 From Eric Weber : build a smart contract that pays issuer when verifier does verification
21:50:29 From Gabe Cohen : That isn't necessarily privacy preserving for the holder
21:51:01 From Eric Weber : could you make it anonymous?
21:51:03 From Benedikt Olek : ...or the issuer and verifiers
21:51:23 From Gabe Cohen : Not without significant data volume

21:52:19 From Rory Martin : Verification occurs over two different steps: retrieving the DID of the issuer, and checking any revocation status. It seems difficult to charge during the DID resolution, so you could build the entire payment into the revocation check. This may drive verifiers to avoid checking the revocation status.

21:54:08 From Rory Martin : The sovrin token white paper seems to suggest that the verifier pays the issuer with a blinded payment. Is anybody familiar with that model?

21:54:22 From Sebastian Bickerle : Binding the payment on the revocation is actually an interesting idea

21:55:24 From Rory Martin : https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

21:55:49 From Rory Martin : Page 34 shows the triangle of payment
21:56:18 From Sebastian Bickerle : I've seen that, but it does not really go into detail
22:06:22 From Paul Dunphy : Another big challenge in banking KYC and VC is pinpointing liability. If BankA KYCs a customer (badly) and BankB trusts that VC - can BankB evidence that they trusted a credential in good faith, and BankA should receive the "punishment".

22:07:04 From Eric Weber : In most countries you pay for your passport as a holder
22:16:23 From Richard Esplin : Sorry it took me a while to get back. I kicked a hornets nest and figured it would be impolite to leave. grin

22:19:16 From Andre Kudra : Good to have you, Richard. We are all interested on how Evernym sees SSI value propositions and selling Points to customers. :-)

22:23:33 From Eric Weber : understand who looses money in the use case today (fraud, theft...), then sell them guarantee

22:32:19 From pknowles : Correct
22:32:30 From Richard Esplin : That's a pretty good guess.
22:32:41 From Richard Esplin : Regarding YouTube premium. grin
22:36:15 From Paul Dunphy : I think some evidence of the future potential of people paying for VCs, can also be seen by who pays for FIDO U2F or FIDO2 devices.

22:36:38 From Paul Dunphy : (spoiler, it's the nerds :))
22:38:37 From Andre Kudra : Back in 3 minutes.
22:41:37 From Richard Esplin : Most of our adoption today are for "Issuer is Verifier" use cases. So they know exactly where the value is.

22:45:49 From Richard Esplin : Our experience is that users want control, but want to be able to contract with a vendor to ensure they can get out of any problems that arise with their data.

Diversity & Inclusion – What Are Your Experiences? We Are Designing An Offering For This Community & Want Input.

Thursday 20I
Convener: Kaliya Young & Shannon Casey
Notes-taker(s): Kaliya Young

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The session was thought of as a way to get input from people who are seeking to improve their cultural capacity and skill set around diversity and inclusion. It ended up attracting lots of women who had a deep conversation about their experiences generally and in the community. There were also several people of color.

If you are reading these notes we, Kaliya Young and Shannon Casey, are very interested in understanding more about your experiences with Diversity and Inclusion training so we can sculpt our offering for the community.

SURVEY ABOUT your diversity experiences https://docs.google.com/forms/d/e/1FAIpQLSeTuHVctbkaYXBEF_B3Wkvr0TMvyoySshAUk7U2r25OPwbXvA/viewform?usp=sf_link

EXPRESSION of interest to participate in a learning circle/study group https://docs.google.com/forms/d/e/1FAIpQLSdJRucPEk8Ec4S0qyvcdI-qCSWdZYJfHHi89WFdBBAawdu0Mw/viewform?usp=sf_link

Question on the table now - what brought to this topic?

- I'm here because yesterday we were going to have a 15 min session after the closing on the Harms Dict for Me2B and it ended up being a 3h discussion on inclusivity, listening, and how to appropriately make diversity
- wow. I was only able to attend one session yesterday cuz working on COVID-19.
- I'm here because I'm new to the identity and tech worlds. I'm coming from the world of social work and community based work which has been filled with very diverse groups collaborating together so I'm looking to find those spaces in these new worlds.
- survival
  alternative option - what do you want the community to know?
- +1 on proactive support of our sisters

Agree.. non-defaults are talking more .. i would never go back to the CHM again.. online is 100% better and when you talk, your face and your space is big.. it gives you parity for a period in a way it cannot in person
+1 mary

we are going to have a different conversation then the one I thought we would I think we should talk about women's leadership within the community
From Dee Platero to Everyone: (01:02 PM)

I was invited to share what brought me here. Truthfully, it was a stark realization that I by default passed over this session. Amazing that I didn't consider that this was a place for me at first blush. + to Riley for some helpful backchannel that helped me realize that.

i feel like the unconscious forces within us are the biggest problem. self awareness of our behavior and communication habits that inhibit inclusivity.

The role of invitation is going to be key to creating a learning/study group of white men in the community who "want things to be different"

Maybe I should clarify about babies: being the center of the universe means your parents feed you and care for you.. but maybe that is white.. but the framing of 'center of the universe' is how psychologists see and study child hood development that at 1y old you cannot comprehend 'sharing'

I likely will leave if Drummond starts pontificating.

@Infominer I'm not sure if this is helpful - but an invitation goes a long way. I personally struggle with imposter syndrome and as a developer I'm frequently intimidated by the older white intelligent men I work with. Even though I've been hired to work it feels better to be invited to the conversation.

I think that many diverse people want to be involved but don't feel like they have any space to speak.

Should we do some type of conference to proactively reach out to women and people of color to increase knowledge/awareness the identity tech stuff...
Yes. Absolutely yes. And I would love to help any way I can.
^ yes. I'm happy to help how I can too.
Interested in thinking out that concept with y'all too, Kaliya.
+1 to the proposal on a conference in awareness

Its now time for us to vision, build new society/economy and return to the governance of Atlantis and hospice white male patriarchy capitalism, so that it collapses with love.

@Infominer I really liked how you said this conversation is uncomfortable. I agree! So, thanks for sharing your thoughts - that takes courage.
@Infominer. I encourage you to participate in and listen in more uncomfortable conversations.
Infominer: hurrah for uncomfortable conversations

it's not evil, it's mental habits it's not evil. it's communication habits.

SURVEY ABOUT your diversity experiences
https://docs.google.com/forms/d/e/1FAIpQLSeTuHVctbkaYXBEF_B3Wkvr0TMvyoySshAUk7U2r25OPwbXvA/viewform?usp=sf_link

EXPRESSION of interest to participate in a learning circle/study group
https://docs.google.com/forms/d/e/1FAIpQLSdJRucPEk8Ec4S0qyvcdI-qCSWdZYJfHHi89WFdBBAawdu0Mw/viewform?usp=sf_link
I wish I could have been here for the beginning of this, as this was my most excited session. Had to deal with some home issues, though. So thank you for having this space and welcoming me.

Condensed/Repeat Sovereignty Principles + Practice = Opportunity

Thursday 20J
Convener: Dave Huseby
Notes-taker(s): NH

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- DH trying to condense 3 talks, responding to challenges 'If you were in charge of the Internet how would your values change the way the Internet works?'
- User Sovereignty is a spectrum not an absolute 'a user controls what, when, where and how of an interaction'. e.g. FB @ one end, Sam Smith at the other, understand that any service fits somewhere on the spectrum
- Let's re-define decentralisation, as distinct from distributed (e.g. twitter), but because of little user sovereignty, they are not properly distributed
- Presents 6 principles of user sovereignty which describe the absolute extreme of user sovereignty on the spectrum
    - Absolute privacy by default
    - Absolute correlation/zero correlation by default
    - What, not who (ie no identification and go straight to authorization)
    - Open and standard protocols / formats
    - Strong encryption
    - Balance of power
- From principle to practice
    - Users control the who, what, when, where, and how of their interaction
    - User access is fully anonymous & private
    - Users fully control their level of correlation
    - Users only use open protocols
    - ….
    - ….
- Nine problems: *Discovery,* **Introduction**, *Coherence,* Public Services, **Trust**, Privacy, Coordination, Membership, Persistent State
    - **Bold - have decentralised solutions in the main**
    - *Italics* - researching solutions (get slide)
    - Normal text - publically available & solved

- Showed research on Coherence (network analytics)
- User Sovereignty means better UX
- Spotting Economic Opportunity - IIW full of entrepreneurs!
    - Choice for companies to build distributed services at the edge vs walled gardens which threaten user autonomy
- Example of Git - failed to solve some of the 9 problems.
    - e.g. not coherent (doesn't accommodate asynchronous connections)
    - No easy way to connect with other users (Introduction)
    - Git's competitor Fossil, has solved the Membership

    - Github.com is the solution to the 9 problems - opportunity because of lack of decentralization of Git.
- Bitcoin is not truly decentralized
    - lacks discovery & coherence
    - privacy partly addressed by Coinjoin
    - solution is coinbase.com to fill these gaps
- Critique of other systems - the web analysed against 9 problems = economic opportunity in the order of billions of $
- Discussion re blogging protocols, impact of google who hated the decentralization (Doc) and killed blogging
- Dave hopes that people will use the 9 problems to analyse services because there's gold in the holes - great economic opportunity
- He's been harsh on the browser and we should redesign because it's an attack vector
- Apps are over-taking browsers so shifting focus away from web stack so looking to other protocols

5am project

- fully user sovereign, decentralized github

Link to slide deck, provided by Dave Huseby:
https://docs.google.com/presentation/d/1G4Quf96ZIts2KgOc9w8WFUpTuF5Bkgbun90jU0m9F2M/edit?usp=sharing

CCLang for Encoding Complex Crypto Constructs

Thursday 21A
Convener: Dave Huseby
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

CCLang is a new language, inspired by Bitcoin script, for serializing all cryptographic constructs as a series of data and command tokens that describe the use/application of the construct. For instance, a secret key would be serialized as an encrypted key with commands for unwrapping the key. Anybody wanting to access the secret key can execute the script and if they provide the proper inputs, the result will be the unwrapped key. This applies for all cryptographic constructs from simple constructs such as key storage up to the most complex such as multi-factor key rotation schemes.

This session covered material documented in link below which was used for the presentation because it has examples and diagrams. Link provided by Dave Huseby:
https://github.com/dhuseby/cclang/blob/master/README.md

SSI for IoT: What Are The Benefits & Challenges?

Thursday 21B
Convener: Geovane Fedrecheski

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Slides: https://docs.google.com/presentation/d/1UF-rWxJeM4jUWiQ-ZfRIVDVqs4r3l4ToxFRA8z9kmI8
ArXiv paper draft: https://arxiv.org/abs/2003.05106

HTTP/3, DIDs – Any New Developments Or Thoughts

Thursday 21D
Convener: Eric Welton
Notes-taker(s): Eric Welton

Tags for the session - technology discussed/ideas considered:
HTTP/3, DID, DIDComm, ClientCertificates,TLS, getting rid of Mr. Login
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- Review of HTTP->(HTTP/2,SPDY->QUIC)->HTTP/3
- What happened w/ DID + TLS
  - TLS says nothing about Certificate Authorities
  - openssl deeply codes ideas of CAs, hard to extend lib for pluggable certificate validation
  - client certificates are there, but never caught on
- DIDComm
  - Hear-ro is looking at WebRTC over DIDComm
  - Can DIDComm handle high volume/rates? Maybe no?
  - Gaming industry wants high volume/rates for example
  - Blending Layers - active exploration of pushing encryption down from the top towards the transport, transport pushes back, where does it balance - e.g. server + client certificates requires a huge ask of both sides for "registry lookup"
  - Do not Tunnel everything over DiDComm
- What is the pain point TLS/ w QUIC
- Do we need to encrypt everything
  - is there a role for HTTP
  - some content *needs* pairways encryption
  - some data can be encrypted from sender for all clients (all subscribers see the same, but not suitable for public)
- ultimately it is not clear how close HTTP/3 w/ pairwise encryption is to the DIDComm ideal
  - worth a little more investigation to understand exactly where it breaks down
  - likely breaks down with the cost of registry lookups
- CAs still do provide value

Glossary Results – Credentials, Wallets, Agents Defined + Next Steps

Thursday 21F
Convener: Kaliya Young, Drummond Reed, & Margo Johnson
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Here is the slide deck -
https://docs.google.com/presentation/d/1gIEPmbtLNVuaHxdawGBe6ZwFqP43m7iqmIEeUUm3sjI/edit?usp=sharing

Wallet can have qualifiers
One could be enterprise wallet

see the specific terms.
WAllet can be depended on
With SSI - holds my identity credentials.
Bank - Vault might be better for them.
Storage - is more generic and more broadly.
Talk about an agent - agent framework and controler.
Depending on person talking and listening they may understand different things.
When describing these things - what are the words that I should be using.

Opportunity to add descriptors or qualifiers to be clear in what contexts we are doing what functions. May be possible to get past those points of confusion.

Enterprise wallet and multi user are stretching it too much.
Agent - creates an expectation that the agent is doing something non-trivial.
Wallet doing direct manipulation.
Insurance agent and publishing agent.
Something more complicated.

Must We Call It "Self-Sovereign Identity?" (Hopefully Not)

Thursday 21G
Convener: Timothy Ruff
Notes-taker(s): Scott Mace

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Johannes: Sovereign is not a word people use.
Tim: This is about terminology, not concepts. If you have huge friction when the words escape your mouth, you start in a big hole.
Iain Henderson: IT management folks faces go blank when you say SSI.

Tim: Public evidence of that. Doc has used the phrase the baby got named. As if that term has been stamped. The reality is any word in any language just means what we all agree it means. A word like googol can come to mean a company. It would be okay if it really got named. It's my contention that the baby hasn't been named. Big organizations getting into this won't use the term. Microsoft. IBM was, no longer. Mastercard. You will not find the term SSI. The allergic reaction that corporate entities. They use decentralized identity. Gartner uses BYO identity. That's a mouthful.
pknowles: Decentralized consent, identity. When I explain it to people, it's a comm channel between two entities without anyone interfering with that channel.

Tim: One way to really throw people off is to start with identity.

Gabe Cohen: Something more marketing oriented, like privacy.

Marc Davis: Has the community ever done a standard branding exercise. We may think we all mean and want the same thing, but that may not be true. Good for surfacing shared assumptions.

Tim: Do we agree the name is problematic? How about a path forward?

Nathan George: I don't know if rebranding it is worthwhile.

Tim: Fair enough.

Doc Searls: I'll speak for the guy who came up with the term, Devin Lefreddo. I will put in the chat what we wrote about it in 2016. If the path forward starts on the corporate side and is limited to what corporations understand and agree to, we're going to lose a lot. The vector starts with the individual. This pen is my pen. It's not pen-as-a-service. If we give up because we need a word acceptable to people who can't understand why I have control over how I disclose my veriable credentials, we're going to
lose. I'm in favor of keeping the term SSI, but will be hard to replace. Usage matters.

Johannes: What is the "it" that is being named here? The technology and the ecosystem applied to a particular set of circumstances, but where the money is drags it in a particular direction, doesn't get taken up as much as it should. Therefore, what should the name stand for? Are individuals more important than the corporations? If market adoption is in a different place than intended, maybe these are two things.
Tim: Doc you said if we have to use a name acceptable to corporates --
Doc: Only to corporates.

Tim: To Johannes' point, it's what Doc said. I am carrying some things that I want you to accept. This is all about issuer holder verifier. Want orgs to be accepting of those.

Johannes: Corporate IT eliminates choice of IT. Whole idea of SSI among employees is the worst.

Joan Caballero: I deal a lot with the interface, work for a thing identity company that does B2B sales. Non-individual credential use cases. Data soverignity is a broader category. Data rights, data protection instead of privacy. I like those terms. If "it" is the tech stack, SSI stack.

Tim: There is data sovereignity. Let's constrain it to the issuer holder verifier model.

Juan: To me that's credentialing. Data-only use cases are still part of SSI but have no VCs.

Tim: Agree. Sam talking about KERI. Consistent attribution, the same key. All of that falls in this bucket. This is all going to stay academic until we get organizations to accept a new way of interacting with us. Get RPs to do things different than they do today.

pknowles: Entity instead of identity?

Josh Verbarg: Why are you so scared of the term SSI? A few years ago, the cloud was the naughty word. Now we have major corporations completely converted. Don't be too scared. It takes time.

Riley: I have been thinking that SSI is not the issuer holder verifier model. I think that is VCs. SSI is a superset of that which encapsulates tech other than VCs. VCs are the first thing to be standardized, digital wallets and DIDs. But there's a lot of other technologies that will work in conjunction. I would suggest either we decide what to call the entire big picture, I use SSI for that, otherwise, if talking about issuer holder verifier model, come up with a word just for that.

Tim: Great points Riley. In our hierarchy of values in our naming exercise, accuracy of the term is a little less important than palatability of the term. We're choosing among a selection of inaccurate terms. The lesser poison.

Marc Davis: We're having a scoping problem. SSI makes most sense when scoped as an ideological concept. Power relationships & control. When includes tech implementation strategies, it gets very confused. The term is being applied to specific tech strategies to implement a particular tech ideology. The "what" we're talking about is ambiguous.
Tim: No one bleeds SSI principles more red than I do, but the path to adoption of the thing that we love lies through organizations, government, public, private. We have to have something that doesn't immediately cause those entities to cringe.

Marc: You have a way of talking about things in the community. Rename based on your strategy for the people you're talking to. What language is needed for that? Different for true believer vs. corporate executive.

Tim: We need a public-facing term.
Hadil Elbitar: First heard about SSI in this conference. Been in identity space for 8 years now. I can't for the life of me figure out a coherent definition for it. Main thing I'm missing is what is the problem we're trying to solve. And how.

Kim Cameron: I have been resisting this whole use of the word sovereign, not that I'm ideologically opposed -- doesn't work in Europe -- but it's because it's not accurate. Because we're social beings, it includes statements by people other than ourselves. Would be better to have a more accurate one to express what's going on. I would propose, VCs are proofs under the control of the people who present them. You don't issue the proof, but you control its presentation. I suggest the idea of user-controlled proofs.

Doc: Kim, great to have you here! I like user-controlled proofs. It's a noun. Self-sovereign is an adjective. What would the adjectival form be? Just use personal. It's how we feel it, also going back to, it's going to work with everybody. We're at a moment now after 20 years on the identity front, may be not purely corporate. Like 1977 when personal computing came along and was scoffed at by IBM. When IBM invented the PC, it ceased to be ironic. I have proofs that I am Doc and that I'm David. Back in 2005 or 2006, as soon as they said identity provider, they bailed, never came back. Defined the way federated identity worked. I think personal does the job. I'm sure there are exceptions. Nathan brought up one in the chat.

Tim: So much in the chat.
Doc: 2 of Kim's original laws apply here. One is user control, a critical thing. Another is minimal disclosure. Justifiable parties.

Tim: A simple decision. As far as the general term we use to push and press releases, internally at IIW, use SSI all day long. But the external facing term, here's the conclusion I want to push forward. The term SSI has to go for those entities we need not to cause problems with. I've talked to more execs than anyone except maybe Drummond Reed. It's a problem. Get rid of the big booger we have in our nose when we walk in the room? Do we have general consensus?

Doc: The question is what are you going to substitute?

Kim: Doc is talking about the adjective. I don't know why we need an adjective. One reason we need the adjective is it always goes with the word identity. I did more than my share of getting that word used. The way identity has been approached so far is so far from grasping the problem of human identity, it's basically a tainted concept. It doesn't grasp anything other than the statements about who we are. It doesn't grasp the selfness of being me. We're still far away from that. We'll introduce wallets as ways to organize our whoness. But we're on the brink to have ways to recollect and assemble ourselves digitally. In the interim, we stop talking about digital identity, but say we have user-controlled proofs to get into web sites, and hospitals nowadays. We have to get concrete. Talk about proofs.

Tim: A wonderful attribute of the word proof, it's very elegant use as a verb and a noun. The zero-knowledge proof folks. It's interesting, you just put a fork in the word identity.

Rory Martin: Seems reminiscent of Agile Manifesto or Green New Deal. Those are principles. We need to separate the principles of SSI. VC term is problematic.
Tim: A big tradeoff with "personal"...it almost does sound like a product. Some friction associated with that.
Vic Cooper: These conversations come out of the context of the internet. When I think of it in terms of telecommunications, I start describe what we're building as identity-based communications. Adding identity into the mix is a real selling point, helps define it from most telecommunications which is defined by the channel (chat, phone call, etc.). We really need something that just talks about how this is real identity. Whereas before we had broken or shadow identity.

Marc Davis: A great conversation, but again, the scoping issue. Different comments hit the problem at different levels. Ideological, identifying the principles. That's where SSI comes out of. Second, tech implementations. Third, business value propositions. Trying to define one term that satisfies each of those scopes. Kim, the term user is good for systems, but not when talking about individuals and power relations. Personal is language is independent of any tech implementation. I don't think one term works across all three domains.

Kim: People have been objectified and they understand that they are using things. Everyone sees themselves as the user of an app.

Marc: Regulators?
Kim: They know who uses the apps.

Marc: Within the ideological political scoping, there is the concept of the individual before using any system. That's part of what SSI is getting that, this pre-user notion of selfhood.

Tim: Selfhood cuts out IoT, organizational identity. Let's say we've got a Trojan horse here. Call it portable digital identity, then we get self-sovereignity. But if we get religious about it, name it, plant a flag, then we defeat our efforts. How do we get the Trojan Horse into the city.

Carl Youngblood: When you look at scopes, it's always going to be mutually exclusive. What's most effective when introducing the concept?

Tim: Influential thinkers called analysts. They create & name the category. Those who want to understand the category buy info from the analysts. Will never call it SSI.

Vic Cooper: SSI sounds like a high-tech additive. My thing is powered by SSI. Needs to be super simple. Should make your life easier. Makes logging in simpler.
Scott Mace: The original Trojan horse was built by the Greeks as a trophy for the city of Troy. Think of this as a gift we're giving to corporations.

Cam Geer: How did the term evolve from feature phone to smart phones?

Lisa LaVasseur: We had feature and smart phone language since the 1990s. The product development leant itself easily to that language. We had the language for a long time. Gartner had projected smart phone adoption probably in 1995.

Tim: No one has spoken up for the favorable term for Microsoft, which is decentralized identity. I also wrote a blog about how everything we're doing with SSI is not decentralized, the literal definition of the term. We know some corporates like it?
Juan: … works with the Decentralized Identity Foundation. Decentralization is the end state. I would like to move in that direction.
Tim: I playfully disagree. The basic premise is with our identity in a bunch of places, it's actually decentralized today. The more I bring control to myself with a reasonable set of credentials, keys, identifier, I'm centralizing that.

Kim: You want to centralize the control of the individual. Decentralization is the technical end goal. Centralized systems are easily attackable. They're not going to scale or sustain or the militarization of the internet which is currently underway. We're living on borrowed time. It's a very technical term. Scoping, we

can talk about when we have a bunch of engineers in the room, but we can't talk to the people who are going to use it. You need something really simple, has to be convey what the benefit will be to them. Under my control, and it can prove stuff. Some way to convey that. Why this is a good and important thing. Then, when talking to business and government, you leverage the fact it underlines what's useful to the individual person. A way of talking about what is useful for the individual and the rest of the system. Does away with privacy problems that will become harder and harder. You eliminate all those privacy problems.

Tim: Would love to convey in the term that kind of individual control. That's what SSI conveys that triggers the allergic reaction in the U.S.
Kim: In Europe, different.

Graybeal: Unfederated identity or credentials? Challenge is, presents different benefits to different people.

Tim: I like the term portable digital identity. Don't like the word identity. But analysts could get behind it and is better than the current term, IAM.

Balazs Nemethi: I haven't used SSI for a long time now. Brings up misunderstanding of how something can be self-sovereign. Decentralized digital identity. I do it because the tech is decentralized, but it explains it happens in the digital space. Not as it used to be. Can be explained much quicker than self sovereign.

Riley Hughes: Gartner and Forrester use DDID right now.
Josh Verbarg: DDI, makes sense to me. Now I'm trusting all these other possible identity providers to give me an assertion about somebody. From a person point of view, you're centralizing it. From a corporation's point of view, it's decentralized. A lot of these technologies are built on blockchain, and blockchain is about decentralizaiton. I understand where Microsoft and Gartner are coming from when they use that term.

Rory Martin: The term decentralized is more of a tech implementation term.
Tim: That's my feeling.

Rory: Doesn't connate value prop to laymen. Interoperability, I can have this ID, works across a multitude of systems, and rephrase SSI as independent ID. The other ones sound righteous.

Tim: I named Sovrin. I got to name it Indy when it got donated to Hyperledger. Indy stood for independent. I like portable digital identity. This is a hot topic

Carl: Interesting the words for independence, having learned Norweigan. unampengyskit?? (sp)

Vic: Couldn't we highlight connections? Connections are a lot of the secret sauce that makes SSIO special. That's what makes us sovereign.

Kim: Super simple identity. It could still be SSI.

Tim: Jonas made a great point. Aren't we underselling it by talking about identity? We're making trust digital. Are we having to kiss the ring of corporate world to make this happen? I don't want to say it that strongly. The way identity works today is dictated by the corporations. They have to change their system. Find a term that works for them.

Joyce: Super Simple Identity. It's like RSS [got different acronym]

Carl: Rather than disagree with them, insert a word that makes them want to know more.
Joyce: Just continue calling it SSI. It's super simple identity
Scott: It's Marketing 101.
Cam: It's worth testing.
Tim: It's just so wrong. My goodness, user names and passwords are far simpler.
Vic: It gets rid of effort. I'm not going to have to need that password before.
Tim: We need our UI to be done first.

Wip: It's SSI, people don't need to know what it is.

Vittorio Bertocci: Calling SSI super simple would be a self-defeating move. Talking with customers even deep into the identity space, SSI looks like an ivory tower effort. Been around for half a decade. Worked with Kim back in 2006. So far there is no mainstream. Naming is important, but I don't think it's the most important right now. Would not be true in a way that would expose you to more bad press.

Riley: I really like portable ID, PID. From federated to portable. Someone mentioned Trust over IP. That's really the value proposition. Can be done in different ways.

Tim: I like the word portable as well.

Marc: Super Simple / Self Sovereign is clever. The actual tech implementation, what is the core tech substrate. Ideological, value prop, and tech implementation.

Tim: I'll take that as a vote for SSI.

Cam: I'm a test and learn guy. Portable identity is one. DDID. See if they resonate in different industries and come back with some input.

Tim: I like it.

Doc: A vote for super simple identity.

Zoom Chat Transcript follows:

14:02:27 From Lisa LeVasseur : usability problems
14:05:10 From Juan Caballero : the baby has been branded :D
14:05:33 From Juan Caballero : yup those are the big 3
14:06:20 From Juan Caballero : I actually think BYOI means something slightly different that can overlap with SSI but not always
14:06:36 From Juan Caballero : although because Gartner is pushing it I don't want to use it :D
14:06:42 From Andre Kudra : For all I know we were using Bring Your Own Identity much before Gartner did… ;-)
14:07:01 From Juan Caballero : ^ I have the early records on vinyl ;)
14:07:28 From Nathan George : And some of the trouble like user-centric terms and similar have already been defined as different things
14:07:45 From Lisa LeVasseur : yeah there's a kind of myopia about it
14:08:46 From Lisa LeVasseur : do we agree the name is problematic?
14:09:25 From Lisa LeVasseur : do the problems warrant changing the name?
14:09:33 From Marc Davis : There are many aspects I like about the name as a "political" strategy.

14:09:48 From Gabe Cohen : Forget problems. Are there more benefits that could be had with a different name?
14:09:57 From Juan Caballero : ^ well put
14:10:06 From Marc Davis : +1000 Doc
14:10:14 From Andre Kudra : Our article "Bring Your Own Identity" published in June 2017. See page 6 of pdf: https://www.teletrust.de/fileadmin/images/publikationen/broschueren/ix/170522_TeleTrusT-Heise-Sonderbeilage_Sicherheit_und_Datenschutz_01_2017.pdf
14:10:30 From Andre Kudra : Don't know when Gartner started, though.
14:10:33 From Nathan George : Polarizing names can be more powerful, if they motivate the right people to opt-in and the wrong people to opt-out
14:10:52 From Juan Caballero : ^ Yeah, I remember last year
14:11:01 From Marc Davis : +1 NathanGeorge
14:11:03 From scottmace : Lime Bikes are bikes-as-a-service
14:11:11 From Juan Caballero : when Rouven said he had the hardest time selling SSI to emirates, and I was like... do we want Emirates funding this? hehehehe
14:11:17 From Lisa LeVasseur : ugh. that's what the world needs: more polarization
14:11:53 From Juan Caballero : (to Lisa's point, I mean that their money comes with strings and backdoors, not that they're bad or illegitimate people)
14:11:53 From Nathan George : It isn't about intentionally leaving people out, it is about convincing the most helpful people to actually help us.
14:12:58 From rileyhughes : Joined the meeting late, there's 7 hands up. Whoof, good conversation already I guess!
14:13:21 From Nathan George : Johannes++
14:14:02 From Celine Takatsuno : +1 to doc.who do we want to name this for? humans? corporations? governments?
14:14:35 From dsearls : Celine, all three. To me it's like the word "personal." All three of those entities knows what that means.
14:14:39 From Marc Davis : Useful to unpack both parts of the term: "Self" and "Sovereign". "Self" is the IMHO key as lowest level locus of control and agency. "Sovereign" is a political term which has its own issues, but as a radical restructuring of individual vs corporate or state power, I think it gets at the key disruptive aspect of the term. It embodies an ideology intentionally. Question here is if the change in terminology is a change in ideology, or merely a tactic as part of a larger ideological effort.

14:14:51 From Iain Henderson : self sovereign identity is not any more understandable to individuals than it is to corporate IT.
14:14:59 From Lisa LeVasseur : +1 Iain
14:15:03 From Juan Caballero : +100 Iain
14:15:32 From Celine Takatsuno : Thanks @Doc. That. Also, branding is hard ;)
14:15:46 From dsearls : here is Devon Loffreto on self-sovereign identity: https://www.moxytongue.com/2016/02/self-sovereign-identity.html
14:16:29 From Nathan George : The "shield against the dragon" type theme?
14:16:36 From Marc Davis : @doc I actually prefer the term "Personal" to Self"
14:16:42 From Jonas Jetschni : Isnt SSI fundamentally about trust that is shared?
14:17:38 From dsearls : Actually, "personal identity" might work. The moment we're at here, finally, may be where computing was in 1977, when "personal computing" first came up. The whole notion that computing could be personal and not just corporate or governmental was anathema to both of those types. "personal computing" to them was an oxymoron. And it remained so until IBM itself created the PC.

14:17:50 From Nathan George : It isn't just about the holder. Each role is important and the system has to be balanced between them, we focus on self because they were perhaps the most underrepresented previously
14:18:07 From Andre Kudra : Couple of thoughts:
Corporate IT has absorbed these terms:
14:18:19 From Nathan George : meh
14:18:19 From Andre Kudra : PKI - Public Key Infrastructure
14:18:20 From jimfenton : "Self sovereign" bothers me because it makes it sound like it's only what I have to say about myself that matters. That ignores identity as informing and being informed by our relationship with others.
14:18:27 From dsearls : See if it works. Substitute "personal identity" for "self-sovereign identity" and see if it works. I think it does.
14:18:29 From Nathan George : jimfenton++
14:18:35 From Andre Kudra : SSO - Single Sign-On
14:18:38 From Marc Davis : Need to distinguish ideology layer from technology layer. "Self-Sovereign Identity" is IMHO technology agnostic.
14:18:43 From pknowles : Self-sovereign entity
14:19:02 From Andre Kudra : Are these terms any better than SSI?
14:19:12 From Juan Caballero : @Marc did you see Karyl's slideshow from Tuesday?
14:19:17 From Juan Caballero : she did exactly that :D
14:19:19 From Marc Davis : I did not
14:19:22 From Marc Davis : :-)
14:19:27 From jimfenton : Any use of "sovereign" sounds too political IMO.
14:19:28 From Andre Kudra : When we are moving from SSO to SSI, we are just changing one letter. ;-)
14:19:36 From Juan Caballero : https://www.slideshare.net/KarylFowler/introduction-to-selfsovereign-identity
14:19:47 From Nathan George : Lots of what credentialing is used for in practice isn't private or "personal" at all, it is very public and about getting bits from A to B to C with the most integrity
14:19:55 From Juan Caballero : ^ YES
14:20:05 From Marc Davis : +1 NathanGeorge
14:20:11 From Juan Caballero : certainly everything Spherity has been able to get someone to pay us to do
14:20:29 From Marc Davis : This debate is in programming terms a "scoping" problem
14:20:54 From Nathan George : This is where John's Trust over IP came from, trustable data fluidity actually seems more important in many of these cases
14:20:57 From dsearls : Nathan, if this is all about moving credentials between what we used to call relying parties and identity providers, we've only re-invented federation. The individual needs agency in this thing.
14:21:02 From Juan Caballero : who's taking notes and where? in the google doc?
14:21:21 From dsearls : Scott is taking notes.
14:21:22 From Juan Caballero : can't let the perfect be the enemy of the good
14:21:27 From Juan Caballero : particularly when it comes to marketing :D
14:21:36 From Nathan George : Dsearls, agreed. Just trying to turn it over to see if something pops out from the other perspective
14:21:49 From riley : yes and that's what I'm getting at too
14:22:27 From Nathan George : Subject-centered federation doesn't quite capture it.
14:23:02 From Juan Caballero : ^ also sounds hard to explain
14:23:37 From Carl Youngblood : "User-controlled credentials"

14:24:21 From Todd Gehrke : Portable credentials
14:24:34 From Carl Youngblood : +1 Todd I like that
14:24:51 From Juan Caballero : I'm not getting this bicep "SSI" tattoo removed guys, it's for keeps
14:25:04 From Carl Youngblood : haha
14:25:10 From pknowles : Decentralized credential model
14:25:15 From Timothy Ruff : I've recently heard the simple "Portable Digital Identity" and I kinda like it
14:25:34 From Lisa LeVasseur : to me, the ethos <with which i do agree> transcends the iam domain.
14:25:36 From Iain Henderson : Yes, that's the best so far
14:25:39 From Celine Takatsuno : thanks for that @Hadil
14:26:03 From Timothy Ruff : @Iain Which?
14:26:16 From Iain Henderson : Portable Digital Identity
Juan Caballero : Philip Sherbourne's work with Akasha Foundation is along these lines
14:26:35 From Juan Caballero : He always insists "identity is always interpersonal"
14:26:37 From jer : User Centric
14:26:42 From Lisa LeVasseur : yes @Kim
14:26:45 From Gabe Cohen : Privacy preserving/user-centric ..?
14:26:47 From Nathan George : Don't do direct API integration anymore, give out signed statements and let others assert them on demand…
14:26:50 From Juan Caballero : and there's a lot of recent work on data unions and data guilds that even data ownership need not be so emphatically INDIVIDUAL
From Carl Youngblood : @Juan good point. Identity only makes sense in a social context.
14:27:14 From dsearls : @Kim "user controlled proofs"
14:27:18 From Lisa LeVasseur : @uan -- ownership and production
14:27:30 From Lisa LeVasseur : @Juan
Juan Caballero : @Lisa, you mean like, "seize the means of data production?" I've seen that graffitid on walls here in Berlin!
14:28:14 From Marc Davis : @Kim Given your points about social embeddness/construction of the self, is the "self" part inaccurate or the "sovereignty" part inaccurate, or both?
From Lisa LeVasseur : :) I mean data production also isn't solely individual. some is co-produced.
14:28:40 From Juan Caballero : toootaaallly
14:28:42 From Nathan George : @Marc probably both
14:28:54 From Paul Dunphy : The term "Trusted Identity" gets quite far with corporates. Is there an extension of that?
14:28:59 From Iain Henderson : As Doc has said before though, 'user' is only common to the tech industry and the drug trade
14:29:00From Nathan George : But together they sort of work, maybe, if your not in Europe, we guess.
14:29:05 From Juan Caballero : delegation thinking sometimes feels like shoehorning the collective into the individual
14:29:23 From Josh Verbarg (State Farm) : SSI is Identity Federation on Steroids from my point of view.
From Juan Caballero : Iain is right-- late capitalism atomizes and insists on the individual scope
14:29:31 From Iain Henderson : Personal Identity and Personal Proofs
From Juan Caballero : nothing more late capitalist than the pharma trade and the software racket
14:29:43 From Celine Takatsuno : +1 Iain
14:29:47 From Marc Davis : I have a big issue with the term "user" because it only exists in relationship to a "system". Need term which is prior to any individual's engagement with a system. I agree with @doc to use "personal" rather than "user".

14:30:01 From Juan Caballero : user smacks of server-client hierarchy :D
14:30:11 From Marc Davis : +1 Juan
14:30:14 From riley : personal proof system
14:30:35 From riley : if we all spit out as many permutations of the options as we can, we might eventually find one that we like :D
14:30:48 From Carl Youngblood : It's the only way some of us can participate!
14:32:53 From Juan Caballero : I feel like "User-controlled proofs" is a MUCH more precise name for the technology
From Juan Caballero : and "decentralized identity"is a MUCH more precise name for the business case
14:33:19 From Juan Caballero : (and/or decentralized credentialing/ credential infra)
14:33:35 From Nathan George : Every large organization tends to chafe at the term. Unless we _like_ that it makes them uncomfortable we should reconsider it. Sometimes doing something shocking is valuable, but you have to live with it.
14:33:48 From Lisa LeVasseur : there is a way to do a poll
14:33:56 From Juan Caballero : we all came! your title was "let's change the name" :D
14:33:58 From Gabe Cohen : Can vote with the yes/no next to "raise hand"
14:34:10 From Marc Davis : @Juan Need to separate terms used to express: ideology; technology; business value.
14:34:50 From Juan Caballero : @Marc - no one should ask me to weigh in on the ideology side, I am a pinko literature professor :D
14:35:18From Carl Youngblood : @Juan huge fan of pinko literature. Don't sell yourself short. ;-)
Juan Caballero : "DEFINING SELFHOOD WITH WALLETS" is the most American thing I've ever heard
14:36:11 From Nathan George : Is it about selfness though, I like to think of the most important part as the relationships and our right to choose within each of those contexts. Which is why I think Kim's concreteness helps.
Carl Youngblood : "User-controlled proofs" seems a bit underwhelming for a grand unifying moniker.
14:36:31 From Lisa LeVasseur : +1 digital identity is a meaningless phrase for everyday people.
14:37:19 From Juan Caballero : ^ I tend to concur
14:37:55 From Marc Davis : +1 @Rory
14:39:57 From Balazs Nemethi : "personal" is short when it comes to IoT
Lisa LeVasseur : +1 rory--separating the principles [which transcend the identity part of technology]
14:40:58 From Juan Caballero : On the issue of identity, Christian Kameir once told me something like (hope i'm not misquoting), "99% of the time people say 'identity' and mean 'profiles', as in 'racial profiling' and 'data profiles'. credentialing is only a consensual form of profiling."
14:44:23 From windley : The problem word in SSI isn't "sovereign" it's "identity"
14:44:55 From Lisa LeVasseur : for me, it's both @Phil
14:45:00 From Lisa LeVasseur : :)
14:45:04 From Cam Geer : +1 Timothy
14:45:25 From Cam Geer : Call Ulysses! ;-)
14:45:44 From Juan Caballero : the name that gets it built is the best name
windley : So, why not just talk about trustworthy digital credentials and forget identity and sovereignty
14:46:48 From windley : Then we "start with the wallet"
Nathan George : @windley That seems to +1 Kim's position about user controlled proofs
14:47:08 From Cam Geer : we're looking for the "invention is the mother of necessity" event which will be named by the market. We can keep floating them until it sticks or is coined
14:47:21 From Lisa LeVasseur : <btw, interesting anecdote maybe: most everyday people have no idea what SMS stands for.>
14:47:22 From Marc Davis : @Juan please do weigh in. I feel like I'm out on a limb here trying to separate the scoping of terms for ideology vs. for technology implementations.

Dan Marino : As mentioned earlier, I do think that the DID communication is very important. So in addition to “trustworthy digital credentials”, we have “ubiquitous authenticated communication” or something.
14:47:57 From Jsearls : +1 Lisa, ditto ATM
14:48:00 From Juan Caballero : ^ Haha, I was only halfkidding when I said I should recuse myself for the ideology portion :D. But yes, me and Karyl agreed with that separation of concerns!
14:48:12 From Juan Caballero : (@Marc)
14:48:31 From windley : STP!!
14:48:39 From Celine Takatsuno : +1 cam
14:48:41 From jimfenton : SO @Phil, if “identity” is the problem word what will we call IIW?
14:49:15 From Jsearls : IIW
14:49:16 From windley : Cause it’s endorsed by history, to take a phrase from Nathan. :)
14:49:24 From jimfenton : :)
14:49:45 From Lisa LeVasseur : Joyce :-)
14:50:06 From Cam Geer : an offering to Poseidon!
14:50:18 From Gabe Cohen : https://en.wikipedia.org/wiki/Timeo_Danaos_et_dona_ferentes
14:51:19 From Vic Cooper : “My hot rod of an application is powered by SSI” It sounds cool enough that I don’t even care what it means
14:52:04 From Marc Davis : @TimothyRuff your points about focusing on the language that gets adoption of a given technology seems to imply that the adoption of the current technology is equivalent to having the desired ideological change effect. I am skeptical of that personally because the ideological goals could have several possible technology implementations and I worry that the view of technology adoption necessarily driving ideological change, seems to me to imply a technodeterminist view of how social and political changes occur.
14:52:51 From Marc Davis : @Vic cool
14:52:53 From Jonas Jetschni : Do we need a terminology that fits into the evaluation of identity? Centralized ID, Federated ID, Social ID, ???
14:53:12 From Cam Geer : Digital Identity?
14:53:21 From windley : Internet Identity?
14:53:41 From Jonas Jetschni : +1 Internet Identity
14:53:44 From Lisa LeVasseur : I'm interested in collaborating on a paper or something on the ideological principles. Anyone?
14:53:50 From Vic Cooper : Short words and Acronyms are incredibly powerful. Think about TSA PreCheck. People know it’s a great thing without even knowing what TSA stands for
14:54:11 From Jsearls : +1 Vic
14:54:13 From Andre Kudra : That's more like chaotic identity. ;-)
14:54:20 From Marc Davis : “Decentralized” can refer to the loci and architecture of power and control vs. a given technology implementation, so it has promise as a term that can Trojan horse in interesting ways.
14:54:23 From Marc Davis : +1 Vic
14:54:47 From Marc Davis : +1 @Kim
14:55:41 From Paul Dunphy : In the spirit of making the conversation easier with executives - we internally we chose use the term “decentralised identity”. I don’t regret it…
14:55:44 From Marc Davis : But, “decentralized” is an opposite metaphor to the individual being the central locus of control.
windley : I like “decentralized” as describing the “architecture of power”. SSI allows anyone to issue, hold, or verify any credential. That’s a diffusion of power well past something like, say, Oauth
From Andre Kudra : Yes, Vic, indeed. Like PKI and SSO. See also my earlier posts here in Chat.
From Juan Caballero : In political terms, decentralization actually means local, bottoms-up power relations--- which is my endgoal on the IDEOLOGICAL side as well as the technical side :D

14:56:26 From Juan Caballero : @Windley +1
14:56:32 From Marc Davis : +1 @Juan ;-)
14:56:36 From Cam Geer : +1 Juan
14:57:10 From Jsearls : +1 Juan “Subsidiarity”
14:57:21 From windley : Some posts:
14:57:27 From windley : https://www.windley.com/archives/2018/10/decentralization_in_sovrin.shtml
14:57:49 From Vic Cooper : How about Effortless ID?
14:57:54 From Marc Davis : Preach @Kim! Love it!
14:58:03 From windley : https://www.windley.com/archives/2016/08/an_internet_for_identity.shtml
14:58:39 From windley : https://www.windley.com/archives/2017/09/is_sovrin_decentralized.shtml
14:58:41 From Jsearls : https://en.wikipedia.org/wiki/Subsidiarity
14:58:50 From Vic Cooper : Connected ID?
Celine Takatsuno : +1 to kim. this community and technologists and gov’t and corporates may all converge on a name at some point. the individuals out there will likely pick up the name of the first product that uses SSI that has true market adoption. (in branding exercises they’d use kleenex as the example here.
14:59:27 From Cam Geer : PDI?
14:59:30 From windley : https://www.windley.com/archives/2016/10/on_sovereignty.shtml
14:59:30 From Riley Hughes : Shorten it to “portable ID”
14:59:32 From Carl Youngblood : What about just Portable Identity
14:59:40 From Carl Youngblood : Do we have to have the digital in there?
14:59:57 From Christoph Menzer : Can we control our internet identity as humans!? Or can we, in best case, control our devices, which control our internet identity? With control over the key, self-sovereign begins.. DID is only an identifier, VCs are my identity, right?
15:00:09 From Jan Taylor : What about Mobile ID?
15:00:23 From windley : Sounds like something for a phone
15:00:46 From windley : +! Christoph
15:01:06 From Cam Geer : DDI / DDID/
15:01:14 From Juan Caballero : DDID:Docs
15:01:20 From Cam Geer : ddID
15:01:34 From Carl Youngblood : “Portable credentials”
15:01:54 From Vic Cooper : The secret sauce of SSI is the way it connects people, orgs & things. Why not highlight that in the name?
15:02:15 From Lisa LeVasseur : Is this an accurate separation of scopes and ergo names: (1) ideological / ethos, (2) enabling technology, and (3) consumer facing product names?
15:02:28 From Marc Davis : @Josh exactly!
15:02:30 From Riley Hughes : Vic, that’s the secret sauce for your use case. But there are lots of use cases that don’t need pairwise DID connections at all
15:02:31 From Cam Geer : “Hey, what’s your ddID?”
15:03:02 From Celine Takatsuno : great observation @josh
15:03:07 From Cam Geer : +1 Lisa
15:03:37 From Lisa LeVasseur : he became one with the sky
15:03:56 From Marc Davis : +1 @Rory
15:04:00 From Riley Hughes : +1
15:04:08 From Riley Hughes : And decentralization is a buzzword which turns some people off
15:04:17 From Timothy Ruff : +1 Rory, but I prefer "Portable" over "interoperable"
15:04:58 From Graybeal : portable universal identity

Vic Cooper : Good point @Riley but aren't connections is a huge part of most SSI use cases?
15:05:08 From Cam Geer : Indy ID
15:05:09 From dsearls : I like "independent identity"
15:05:48 From Timothy Ruff : Me too
15:06:01 From Timothy Ruff : kinda close to self-sovereign though
15:06:19 From Juan Caballero : Unabhaengigkeit
15:06:22 From Carl Youngblood : uavhengihet
15:06:37 From Juan Caballero : not-hanging-on-[anyone else]-ness
Jonas Jetschni : Arent we underselling us with identity? Isnt the topic much big as we bring trust to digital?
15:06:47 From Carl Youngblood : @Juan precisely!
15:07:02 From Todd Gehrke : Relational identity model
15:07:07 From Marc Davis : @Kim love it
15:07:18 From dsearls : "super simple identity" SSI +1 Kim!
15:07:37 From Hadil Elbitar : ^ lol :D
15:07:45 From dsearls : My vote is for that one, and I didn't expect to like any of them.
15:07:48 From Paul Dunphy : We should validate the usability before committing to that one :)
15:07:56 From Marc Davis : "Super Simple" is a great way to explain a value proposition.
15:08:10 From Gabe Cohen : It's super simple - you own it
15:08:10 From Jsearls : Super Simple Identity!
From Cam Geer : it's a practical move on the part of this community to drive adoption
15:08:15 From Vic Cooper : I like Super Simple!
15:08:22 From Hadil Elbitar : and no one would have to stop saying SSI
15:08:28 From Chris Eckl : super simple +1
15:08:48 From Balazs Nemethi : Super Sexy Identity? -- :)
15:08:52 From Lisa LeVasseur : i didn't expect to be saying this either, but the beauty of SSI is that it's open to multiple interpretations.
15:09:15 From Paul Dunphy : I think that's decentralised identity works for the same reasons
15:09:39 From Juan Caballero : PGP
15:09:41 From jimfenton : Asynchronous Transfer Mode ??
15:09:43 From Juan Caballero : it's pretty good!
15:09:50 From windley : +! Jim
15:09:57 From Micah McG : SSI is v2 to SI
15:09:59 From Gabe Cohen : Some secure identity, stupidly simple identity
15:10:02 From Marc Davis : SSI as global scope: ideology scope = "Self-Sovereign Identity"; value proposition = "Super Simple Identity"; what is the technology term for SSI?
15:10:24 From Juan Caballero : you can hit "NO" if you hate it
15:11:03 From Drummond Reed : Super Simple Identity, is that it?
15:11:15 From dsearls : Yes, Drummond.
15:11:19 From Jan Taylor : Simply Secure Identity
15:11:23 From Drummond Reed : I've been saying we should call it "SSI" for months now!
15:11:26 From Carl Youngblood : Usernames and passwords are not simpler. A brief glance at the number of records in my 1password app will attest to that.
15:11:29 From Juan Caballero : @Jan +1
15:12:48 From Marc Davis : +1 @Carl
15:12:53 From dsearls : I'm down to 800+ login/pw combinations. Simple!
15:13:04 From Marc Davis : @Doc ditto
15:13:04 From jimfenton : We need to remember that "identity" or whatever you call it goes way beyond authentication (e.g., username/password). Apples and oranges.
15:13:11 From Stephen Curran : +1 to Doc

15:13:15 From Timothy Ruff : My PW manager makes un/pw simple for me
15:13:39 From jimfenton : Timothy +1
15:13:53 From windley : Many people *hate* the word “trust”
15:14:03 From jimfenton : Yes I do
15:14:45 From Riley Hughes : Single sentralized identity
15:14:51 From Riley Hughes : Only problem is you have to spell centralized wrong :)
15:15:13 From Vic Cooper : That would be TOIP @Marc
15:15:17 From Jsearls : Super Secure Identity
15:15:37 From Vic Cooper : Super Simple Identity running on TOIP
15:15:43 From Juan Caballero : Test drive!
15:15:45 From Lisa LeVasseur : so to be clear, we're naming the technology, yes?
15:15:49 From Marc Davis : @Vic +1
15:15:56 From Andre Kudra : Vic +1
15:15:59 From Drummond Reed : +1 to SSI. It’s already become the term the majority of the market is using. Why would we try to move away from it now.
15:16:18 From Andre Kudra : SSI will not go away easily any more in the world.
15:16:18 From Riley Hughes : Agree with Drummond.
15:16:21 From Marc Davis : Thank you! 15:16:28From Jan Taylor : Thank you!
Cam Geer to Everyone: 03:17 PMthx! Juan Caballero PMThanks all! Sorry I spoke too much!
From Marc Davis to Everyone: 03:20 PM@Juan love your contributions!That was my scoping point
Timothy Ruff to Everyone: 03:20 PMThanks Juan. :) Juan Caballero: 03:21 PMgreat problem to have

Introduction to Marshall Rosenberg’s Nonviolent Communication (Perhaps Discussing Integration With Standards Processes)

Thursday 21H
Convener: Infominer & Shannon Casey
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Link provided by Infominer for additional notes to NVC:
https://docs.google.com/document/d/1dMq2LASFyOK26ALrzQ5pXQNO1Z6jyta9Fp5yYgxadfY/edit#

Shannon Casey https://shannoncasey.net/

NVC is a first step toward understanding the importance of relationality that is key to creating anything. When we step into awareness of communication and where we are not relational, we are not creating effective solutions or products that reach all the potential of the public.

The dialogue held during the session was a practice of relationality and opportunity to widen the scope of the lens of attendees who are newer to this work.

Shannons suggestions for learning NVC- Find a practice group or create a practice group of your peers, the neurobiology of this relational approach cannot be found in our own isolated thinking. We cannot unthink our way out of our learned inter-relating. My mentors are Roxy Manning, Mika Maniwa, Sarah Peyton, Miki Kashtan and Kristin Masters. All offer online access to their work and Sarahs book Empathy Brain is one of primary sources for the neurobiology of NVC.

Kimberle Crenshaw's & Patricia Hill Collins Intersectionality is a cornerstone of my navigating walking with awareness. Here is Kimberle Crenshaws TedTalk and please include both names when you say Intersectional Feminism.
https://www.ted.com/talks/kimberle_crenshaw_the_urgency_of_intersectionality?language=en

Article Shannon mentioned at the end of the session for white folks regarding unpacking impact of whiteness http://www.dismantlingracism.org/uploads/4/3/5/7/43579015/whitesupcul13.pdf

Money Is The Problem: Mechanism Design for Currency

Thursday 21I
Convener: Grace Rachmany
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

https://coala.global/

Main points of the talk:

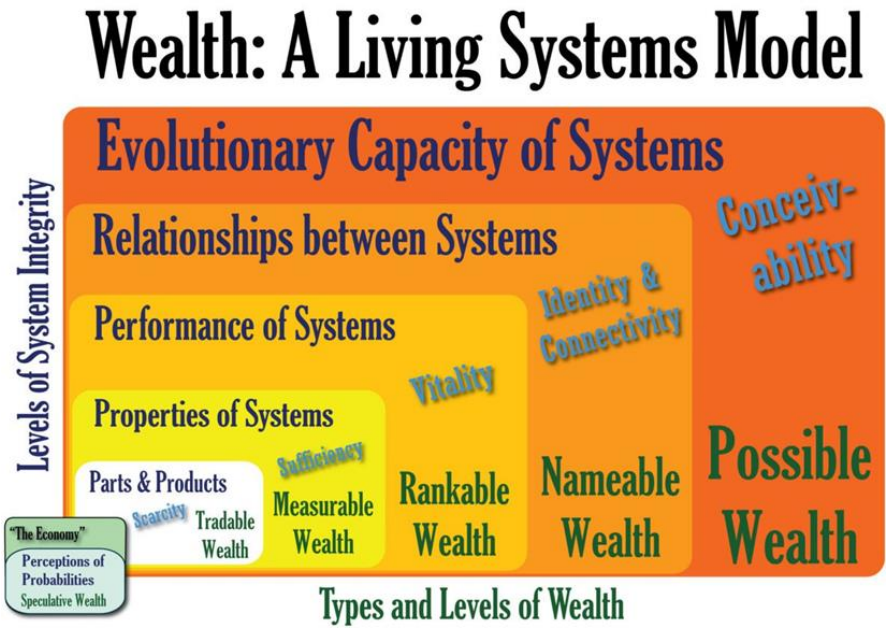
- Money is a mechanism we invented and it's a figment of our imagination. We have the opportunity to create anything we want. Now with cryptocurrency there is an opportunity to completely re-invent money but most tokens have not done that, they are the same kind of money than we already have.
- In this presentation I will attempt to represent the most extreme case to put into contrast with our existing beliefs. It's not necessarily my precise opinion but gives a perspective to shake up your assumptions.
- Money represents transactional value which is anti-human values. Anti-air, anti-relationship. Most money today represents EXTRACTIVE value that has collateral damage or "externalities" that are not accounted for.
- Extractive includes:
  Extracting resources from the earth

  Extracting labor from people
  Extracting food from living animals
  Extracting data from people

Polluting people's brains with disinformation (advertising/persuasion)

- Money today is created by debt. This is an arbitrary invention of our system. 97% of money is created as debt by banks, not by governments. Today we see governments taking out bonds and loans in order to print money… so it's not really even printed. It's created in the form of debt.
- The result of this invention of money by debt is that GROWTH is the main engine of the economy. Because governments, businesses and individuals are eternally trying to service this debt, we must have growth. You don't have to imagine the consequences because we see those consequences now-- everyone suddenly defaults on everything and the results are tragic because this debt is not serviceable and never was. It was a kind of a huge ponzi scheme and increasingly we were seeing how we could never get out of it..
- Other ways to create money include mutual credit, commodity backed, time banks. We probably don't know what is possible in this realm but we can start to think about it.
- Our current system brainwashes us to think money can solve problems. We have to re-adjust our minds to think about resources rather than money. When we think about resources and value rather than money, we are able to come up with creative solutions. The current system pushes that without money you will die--but money is just a means to get those resources and it doesn't have to be.
- Money as we use it today is transactional outside of membranes. Inside of membranes, you don't use money. In your family you don't pay for food. In IIW you don't pay for knowledge or speakers. That's the membrane agreement. In other conferences it could be difference -- the speakers could be paid or the speakers could be paying to shill to you. Whatever the terms for entering the membrane, once inside the membrane money is not used for transactions.
- In that sense, you NEED money to the extent to which your existing membranes don't meet your needs. You want money to the extent to which your membranes don't provide your wants.
- Rather than UBI, we could talk about food the same way we talk about healthcare, that is, it's a service and universal right. That way instead of distributing money to people in a membrane, we would have a way of distributing food. (shelter/education/whatever)
- What are those membranes? Right now it's nation-state, but any shape of membrane could be possible.
- Question: what about free riders? who will do the work to produce that food?
- Opinionated answer: The system we are in was designed in a scarcity economy where the scarcity was food. If you lived in a sustenance society, if one dude/dudette didn't help with the harvest, then someone went hungry. That's a free rider problem. You actually truly needed every able-bodied person to contribute to the survival of all. Today's reality is different. 10% of the workforce could create enough food for all. We would have to pay farmers and every society would decide for itself. In some communities maybe everyone would take turns. In other communities we might give them special awards in ceremonies. In most societies, we'd pay them and they would have money that would allow them to buy luxury goods.
- Q: who decides what a luxury good is?

- A: That will also vary from membrane to membrane. Every society will have different values. Maybe in some societies nobody pays for everything and they have some cool 3D printer that recycles everything and produces everything for zero nominal value, maybe everybody gets everything free and money is only used when you travel.
- Fungibility could also be in the form of different certificates. For example, it might be enough to show a credential that says you are in good standing in your community in order to get a hotel room in another community. Those communities might not exchange fungible money but just "in good standing" certificates, and give the hotel rooms based on a ranking basis during peak times… this would all be community interchange.
- Reputation may end up to be a more important form of exchange, particularly for goods that are digital. For example, a group of scientists might invent a cure and give the formulation to everyone except anti-vaxxer communities. These kinds of exchanges could be based on any type of currency.
- When thinking about new forms of exchange and reputation and currency, we should be thinking in terms of biodiversity rather than having the right answers. Societies and membranes have their own values and will have different ways of exchanging value and signalling values.
- Regarding free riders, if survival is not a problem, free riders are not a problem. The guy sitting under the palm tree playing the ukelele isn't bothering anyone and if he has no extra cash, he isn't burning up fuel by travelling or buying plastic toys. He's just bumming around consuming less than the hard worker.
- Some (many) people will want to work not just to buy stuff but because they like to.
- The following is by Arthur Brock of Ceptyr/ Metacurrency/ Holochain.
- Please see this for an explanation https://finnern.com/2014/07/06/wealth-a-living-systems-model/



New currencies can think about all these different types of wealth in designing different types of currency flows and measures for their communities. We have a richness of opportunity now and we need to try many things to find out what works. The first step is realizing how stuck we are in our thinking about money, and this talk has been a first step in breaking those thoughts and allowing us to let in some new ideas. It's probably unimaginable what money will be in the future -- this is only a start.

Zoom Chat Transcript:

23:03:22 From Kalin : I am in europe, late night and kids sleeping;
23:04:04 From Kalin : I am here for the great topic - little known on MONEY
23:13:54 From Elias Strehle : Central banks are not "the government", and they are the ones responsible for monetary policy.
23:19:11 From Nicky Hickman : Has anyone read Dave Birch's book 'Identity is the new money'
23:19:59 From Nicky Hickman : And also Nigel Dodd's 'The Social Life of Money'
23:20:37 From Kalin : Dave Birch has consolidated 5 years of forum exchanges and ideas, often times not his, and signed his name on it; also - half-baked IMHO
From Kalin : DEBT - the first 5,000 years is a good departure point of current monetary system
23:21:42 From Nicky Hickman : Thanks will check it out
23:21:58 From Kalin : https://en.wikipedia.org/wiki/Debt:_The_First_5000_Years
From Nicky Hickman : I have just finished some anthropology studies and Grace just touched on the difference between perceived social value (as part of gift exchange) and the difference between that and economic exchange. Actually they are closely related rather than being in opposition to each other I think
23:29:26 From Kalin : if we address Maslow's Pyramid, then inevitably we end up in a situation of supply and demand, which is econ101, and back to WHO WORKS, while others rest and benefit; human nature will kick in to quickly wean off the free riders…
23:29:54 From Kalin : sorry, cannot use audio
23:31:49 From Nicky Hickman : Check out https://en.wikipedia.org/wiki/Kula_ring for a completely different way of looking at gift exchange, trade and wealth creation
23:32:04 From Nicky Hickman : or even value creation
23:33:36 From Kalin : Thank you, Nicky!
23:39:39 From Kalin : Society is just an oversized membrane, so there must be some record-keeping of how wealth, food and housing is distributed… One may argue that societies/nations have outgrown the reasonable, which might explain why we are swinging away from globalization to local-first… truth is, MONEY is such a vast network of rabbit-holes, as deep as culture, habits and deep-rooted inertia that unpacking it is vastly more difficult from "lets just build a better one"
23:40:02 From Kalin : Amen to FUNGIBLE, @Nicky
23:41:09 From Elias Strehle : +1
23:42:20 From Nicky Hickman : This is the RSA stuff https://www.thersa.org/action-and-research/rsa-projects/economy-enterprise-manufacturing-folder/the-future-of-work
23:43:24 From ChristianHildebrand3000 : I am here in the IIW (as well as this session) to learn how to forward the vision that we are developing around the acti
23:43:30 From ChristianHildebrand3000 : vity
23:43:47 From ChristianHildebrand3000 : valueinstrument.orgFrom Karen Advocate : Has more to do with how we define "success" individually. In capitalism having more money and stuff is most important. Whereas you cannot eat money or stuff, redefining success as the most oppressed member of a community thriving is a different values-based definition of success.
23:44:29 From Kalin : separating humans from subjectivity @Elias? Great one
23:44:30 From ChristianHildebrand3000 : this project aims to allow anyone, any group and network to experiment with new forms of money
23:45:49 From Elias Strehle : Who decides what is enough? Who defines what is a luxury item?

23:47:56 From Nicky Hickman : your project sounds really interesting would love to experiment on a project for homeworkers in India making PPE!
23:50:37 From ChristianHildebrand3000 : cool, lets figure it out!
23:53:09 From Kalin : on the topic of reputation as money, I suggest you watch the NOSEDIVE episode of Black Mirror = https://en.wikipedia.org/wiki/Nosedive_(Black_Mirror)
23:54:41 From Kalin : in summary - the crowd is the worst Central Bank you can imagine (and there are some awful examples to benchmark agains)
23:55:28 From Nicky Hickman : I was trying to be deliberately provocative - in fact one person walked out because they said I was 'a bloody communist'
23:55:42 From Kalin : HAHAHAHAHAHAHAHA
23:55:52 From Kalin : if this is what communism looks like, sign me up
23:56:12 From Nicky Hickman : your little red book is on its way
23:56:27 From Karen Advocate : Money is a TOOL - not a measure of success. Would be interesting for 6 figure working from home folks to change employment, housing, pc/phone, access to healthcare benefits and internet with minimum wage grocery store and building cleaning workers surviving pay check to paycheck for a few months? In WA state, . one of my clients is the faith community who advocates for people experiencing homelessness and holds poverty immersion workshops to get people to understand that people do not choose homelessness. https://www.councilforthehomeless.org/poverty-immersion/
23:57:37 From Kalin : if we keep crossing each other so often in so many different places, we might just spin our very own rebellion @Nicky
23:58:26 From Karen Advocate : Argue that Congress subsidizes fossil fuel, industrialized agriculture, essentially corporate socialism, which the US is built upon.
00:14:25 From Elias Strehle : An excellent book: "The Politics of Bitcoin" by David Golumbia
00:22:55 From Grace Rachmany : COALA
00:24:41 From Grace Rachmany : https://coala.global/

What Is BC Gov Doing? Why Should I Care About Digital Trust? Why Is A Government Investing In This? Ask Me Anything…Can't Promise The Answer Will Make Sense!

Thursday 21J
Convener: John Jordan (BC Digital Trust Service)
Notes-taker(s): John Jordan

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

We didn't take real time notes so this is my reflection on the discussion.

We had a wide ranging discussion that spanned from the importance of gov participation in issuing foundational credentials (person, organization, land, relationships between these entities). to trust in society and the need to have verifiable origins of words (fake news), and emissions (manage our planetary carbon balance).

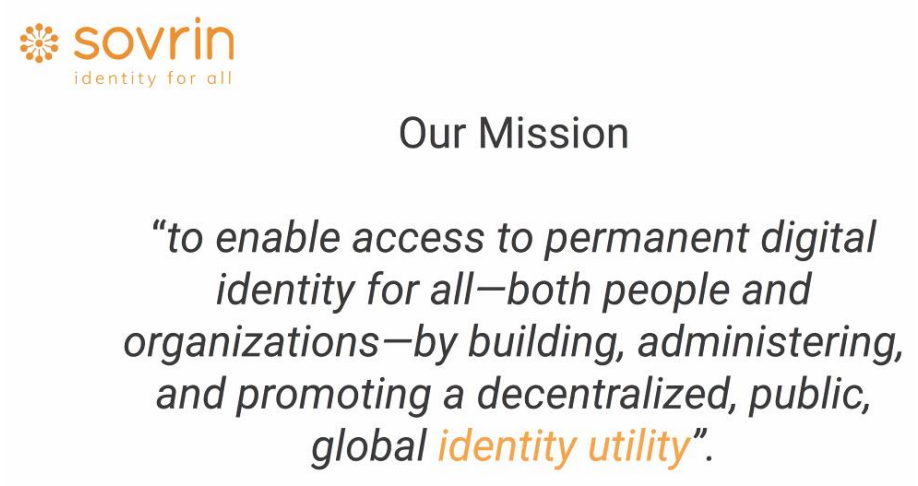
Appreciate the thoughtful questions and the time people took to listen.

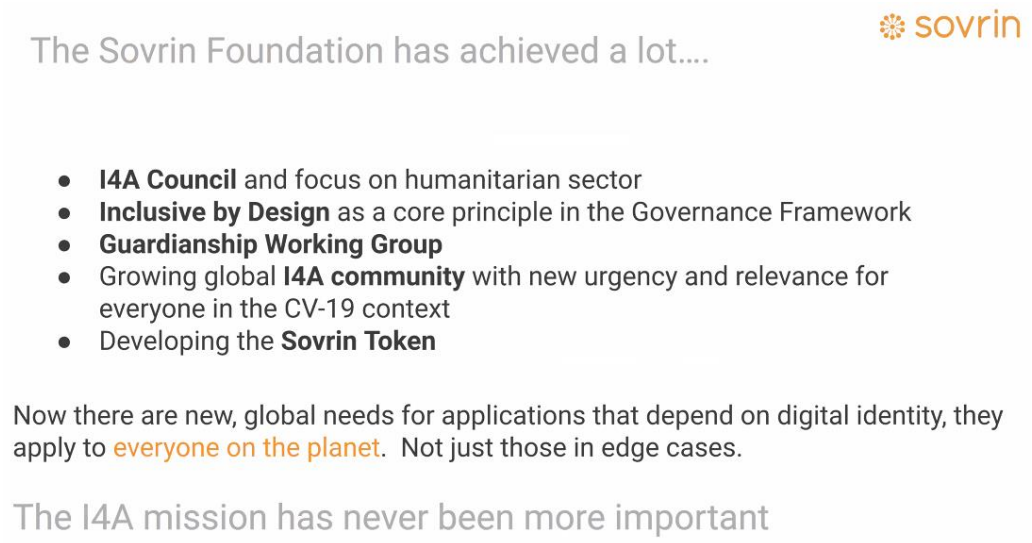
Can You Have Universal ID for All Without A Token?

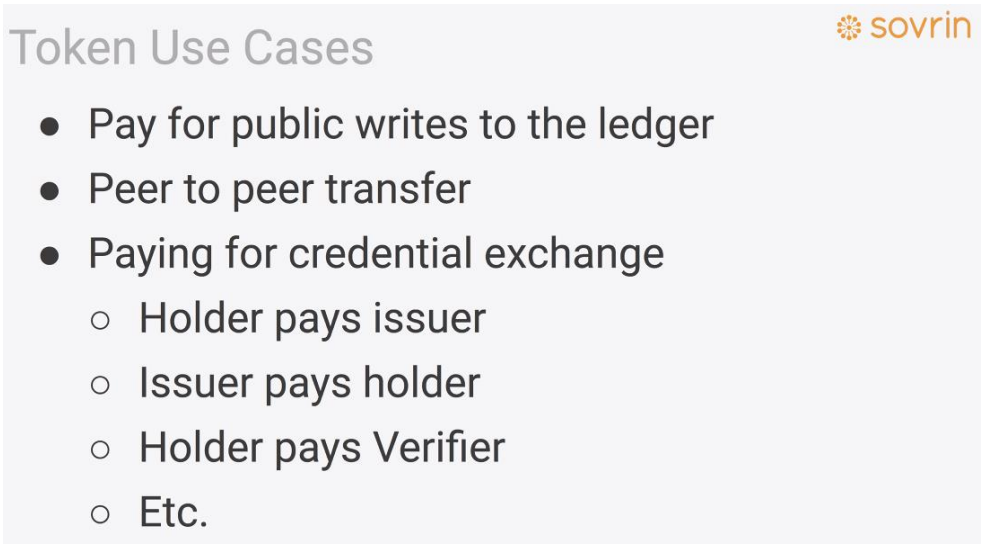
Thursday 22A
Convener: Jeff Aresty, Nicky Hickman, & Phil Windley
Notes-taker(s): Phil Windley, Jeff Aresty, & Nicky Hickman

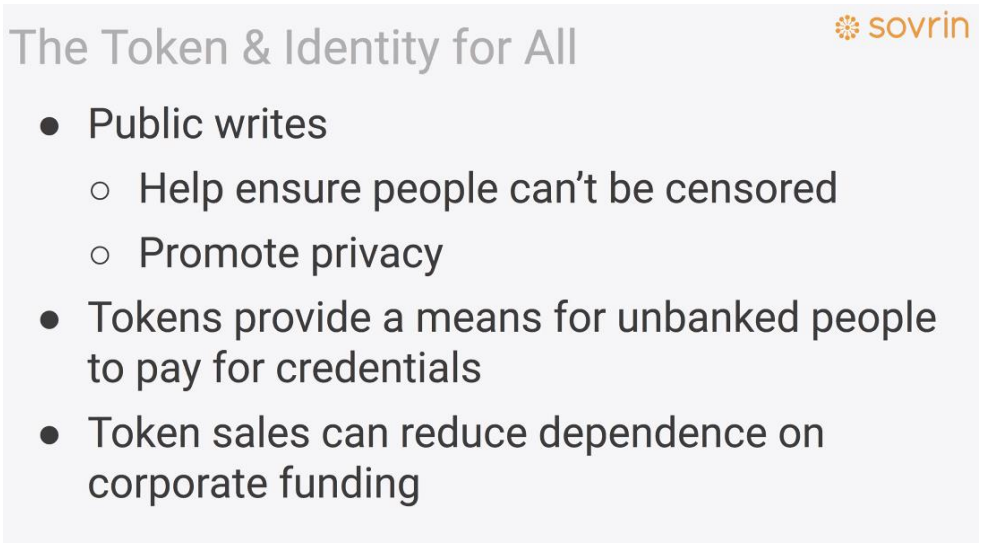
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

1 Phil started with these slides:









Grace Rachmany: "That kind of token (an anti-spam token) would have to be integrated with a reputation. So if you are identified as a spammer, you'd have to pay me a lot of token to get my attention whereas if you are a reputable expert, I might have to pay you in order to get your messages[SEP]The problem with pure attention tokens is that they go to the higher bidder -- and then you just end up with The New Google."

2 The next slides were from Jeff Aresty.

Application Example:

sovrin

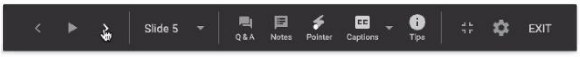
Bee1 World from Jeff

Project Description ~ during Covid-19

During this period of time the hope isn't lost - we are adapting by taking the project online and organizing online filming courses.

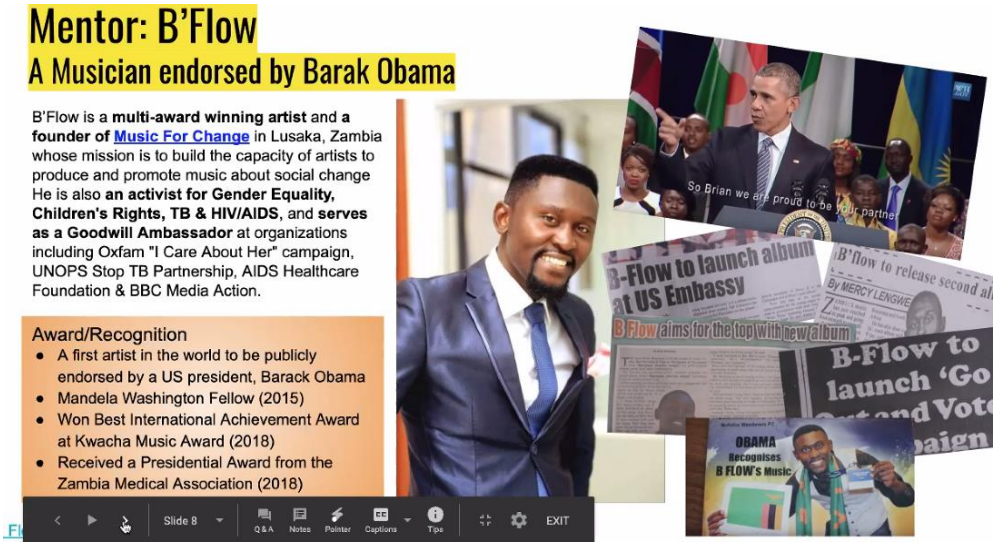
Students are asked to film videos that would help prevent spreading of COVID-19 in African continent - a geography much more vulnerable than European, Asian and American countries affected right now. For example, videos that explain how to protect yourself and your loved ones even without owning a mask and gloves.

We are all in self isolation but we can be a voice to the world while being at home!

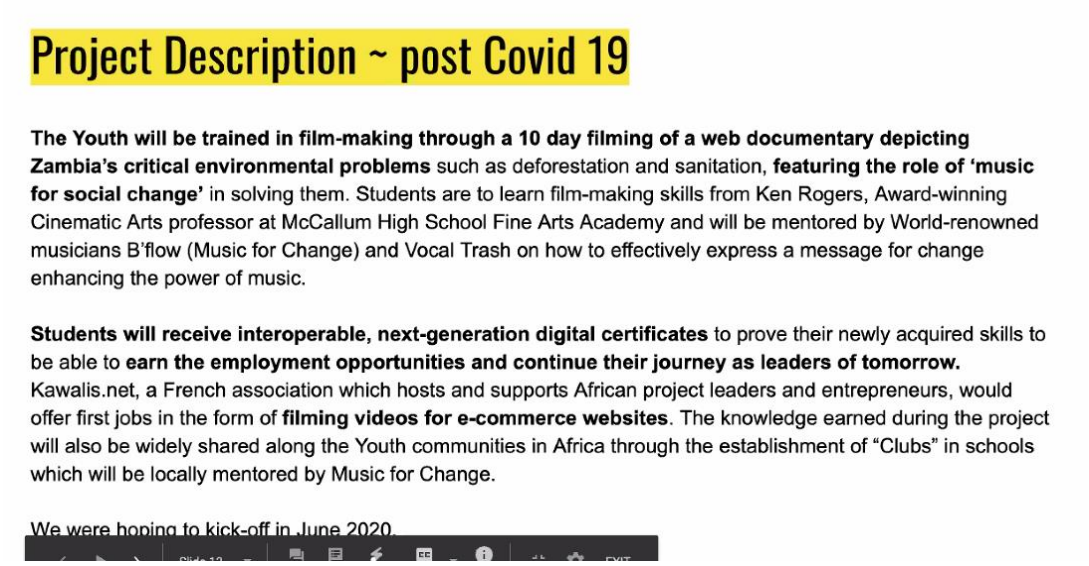


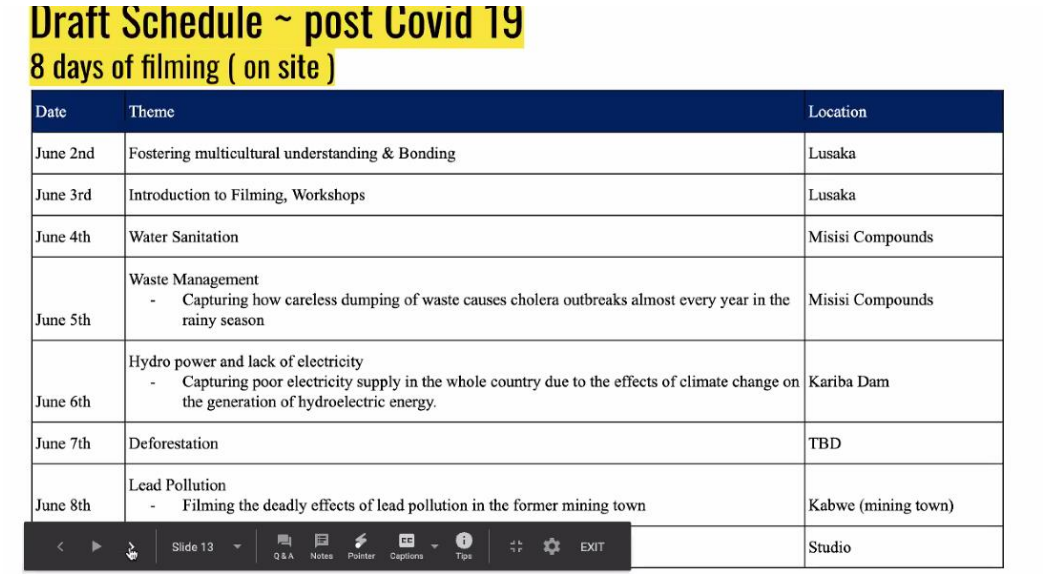
Schedule ~ during Covid-19

Date	Theme	Location
April 2020	Training courses with Ken Rogers	Online (30 min/session)
May 2020	Training courses with Ken Rogers	Online (30 min/session)
June 2020	Hopefully physical training program begins (detailed schedule on the next page)	Lusaka



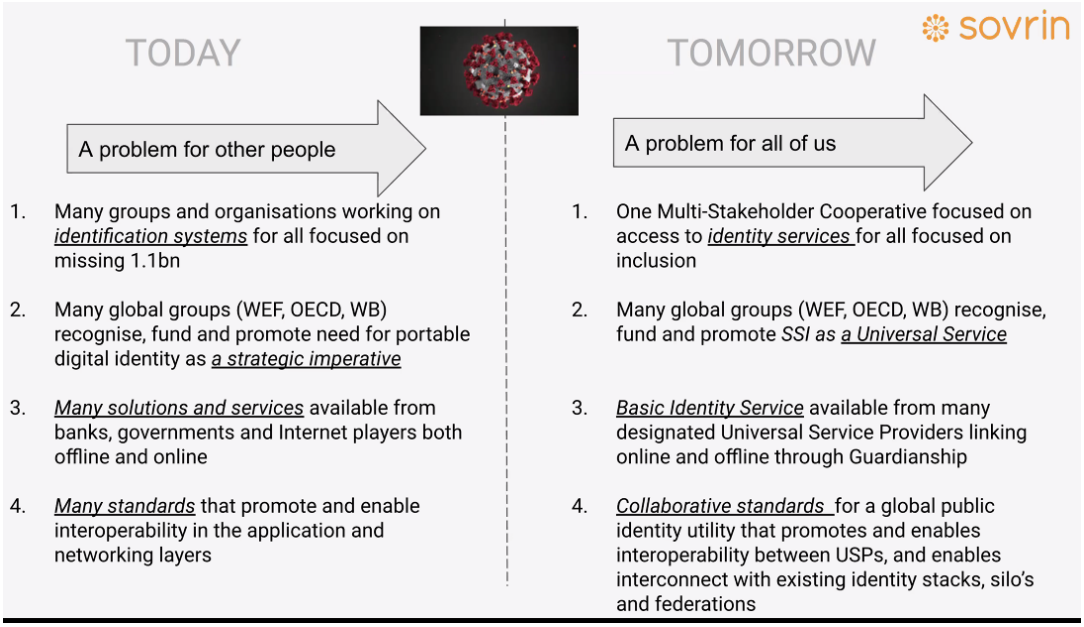
Note: not all slides are being captured (some go by too fast).





Jeff's conclusion: ultimately, a project like this needs funding, and the token might help with this.

3 Next Nicky Hickman talked about “Universal SSI Service”.



Why a Universal Service?

sovrin

Universal service *is an economic, legal and business term used mostly in regulated industries, referring to the practice of providing a baseline level of services to every resident of a country. E.G. US Telecommunications Act of 1996, whose goals are:*

- *to promote the availability of quality services at just, reasonable, and affordable rates*
- *to increase access to advanced telecommunications services throughout the Nation*
- *to advance the availability of such services to all consumers, including those in low income, rural, insular, and high cost areas at rates that are reasonably comparable to those charged in urban areas*

- **Ready made** language, legal, commercial and regulatory structures
- Applies to **utilities** and basic services that are needed in society such as electricity, telecoms, basic bank account. Sometimes called a ‘**duty to supply**’
- We can work with the existing identity providers (e.g. telco’s, Internet Players, technology providers) and focus on enabling ***a functional basic digital identity*** that links with offline and is distributed

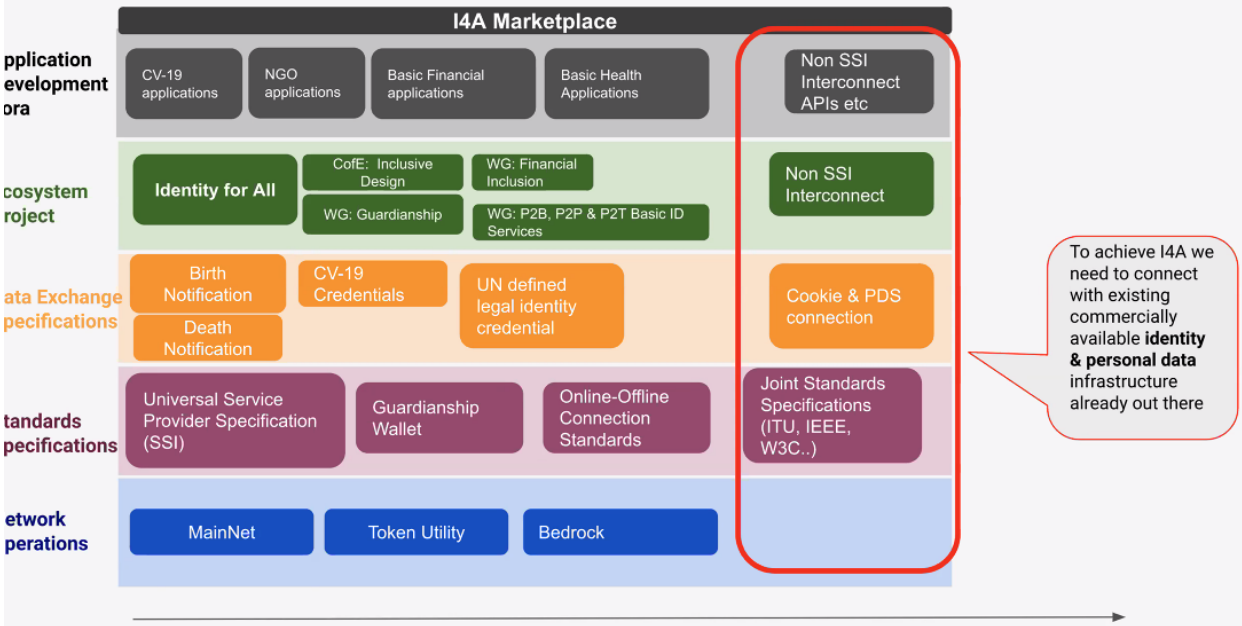
IIW Questions

sovrin

1. Does Universal Identity for All need the Token?
2. What are your thoughts on the best approach to further the Identity for All Mission?
3. Could SSI enable the kind of interconnect with existing identity services or is that some way off? i.e. we can't interconnect ourselves yet (Network of Networks is some way off), therefore this leap is too much too soon?
4. How could industry respond to the idea that this is further cost and regulation?
5. How could something like a basic identity service build market momentum for SSI as a whole?

Example: I4A Ecosystem

sovrin



Zoom Chat Transcript:

3:33:18 From Grace Rachmany : I have tokens in my background
23:33:46 From dsearls : I like those tokens!
23:35:41 From Drummond Reed : The only change I would make is to add "things"
23:36:24 From Nicky Hickman : It's from the website
Nicky Hickman : Guardianship is really essential if you want a properly self-sovereign identity system
23:40:10 From Juan Caballero : +1
23:40:31 From Darrell : +100 Nicky - Guardianship is foundational

23:40:35 From Grace Rachmany : It makes me a little queasy when I hear the "universal for all" slogan. It feels like that something "for all" will inevitably end up centralized.
23:41:26 From Nicky Hickman : Definitely not - Universal relates to basic Universal Service, like telco or electricity, or as in your talk earlier @Grace, universal basic housing & food
From Grace Rachmany : Universal electricity and telco are not provided by one organization
23:42:41 From Nicky Hickman : no
23:42:52 From Nicky Hickman : so not centralized
From Drummond Reed : +++1 to not centralized. It's not self-sovereign if its centralized.
23:43:42 From Darrell : Speed bump : meaning anti-spam
23:44:10 From rouven : How would the token be able to help with GDRP issues?
23:45:23 From Grace Rachmany : Is a dedicated token essential or just nice to have? Could another digital cash form be used.
23:46:22 From Vic Cooper : I would like to see a token for attention - as in pay me to look at your message, accept your connection, etc.
23:46:35 From Drummond Reed : +1
23:46:40 From Nicky Hickman : love it @ Vic, I call this 'identity work'
23:47:48 From Grace Rachmany : @Vic That kind of token would have to be integrated with a reputation. So if you are identified as a spammer, you'd have to pay me a lot of token to get my attention whereas if you are a reputable expert, I might have to pay you in order to get your messages
23:48:17 From Grace Rachmany : The problem with pure attention tokens is that they go to the higher bidder -- and then you just end up with The New Google
23:49:05 From Vic Cooper : This would be helpful in the cases where someone I don't know wants to connect with me. Fixes the problem with email-type spam. There is email spam because sending email is basically free
From Juan Caballero : I have heard some buzz about attention tokens-- didn't Brave integrate a token?
23:49:34 From Richard Esplin : @Grace when using a different form of digital cash, you have to figure out the on-ramps and off-ramps while avoiding introducing a 3rd party who could erode privacy.
23:49:38 From Vic Cooper : Good point @Grace
23:49:59 From Richard Esplin : A native ledger token simplifies that.
23:50:07 From Vic Cooper : Brave uses the BAT or Basic Attention Token
23:50:41 From rouven : Q: Does the token change in the network of network model?
From Juan Caballero : ^ This is what I came to hear about! Please ask that at the end :D
23:52:27 From Vic Cooper : The other great use for a token would be as a way to reward early adopters and stimulate network effects for the Sovrin network. But there are legal challenges
23:53:30 From Juan Caballero : @Vic, the media/journalists I know are super supportive of the Brave model and hoping to see it amplified/scaled! Then again, they might just be desperate for any business model other than paywalls :D
23:53:38 From rouven : ok, thx Phil
23:54:26 From Grace Rachmany : It's interesting to think about pricing for digital goods. Nominal cost of digital goods is pretty much zero-- so there's a concern about the constantly decreasing real value of any type of digital service.
23:56:05 From windley : Although credentials might represent physical goods. An airline boarding pass, for example, is a digital artifact, but it doesn't represent a digital good. It represents the authority to board a flight on a certain day to a particular destination.
00:00:28 From Grace Rachmany : Right, but unless you are flying RyanAir and you don't have a printer in your hotel, you don't pay for the actual ticket. You pay for the right to fly and the ticket/credential is a QR code that has no extra cost associated with it.
00:00:55 From rouven : @Richard - don't you still need on/off ramps even for a native token?

00:02:01 From windley : Right, but it represents the thing you paid for. You could imagine paying for your flight in tokens and what you get is the boarding pass as a credential.
00:03:36 From rouven : yeah, if it's about a write access that could work. But the combination of different use-cases with the same token make it hard… peer 2 peer payment, or payment for a credential vs. a write access
00:04:09 From rouven : if it's a fungible token with a certain value -> just a normal payment token -> could be just a usd token
00:04:34 From rouven : and a voucher for people who cannot afford it - and someone else would pay for handing out the vouchers
00:04:50 From Grace Rachmany : I can imagine paying for my flight in anything fungible. All I'm saying is that the long-term viability of a token is based on the long-term value of that token. What I'm question is the long-term value of something that is a digital good. As Jeffrey just said, look at that musician. He produces a digital good and the nominal value of the reproduction of that music is nothing, and the guy doesn't have two nickels to rub together.
From Darrell : @rouven- you can also replace "can't afford" with "can't be seen to use" as well.
00:05:26 From rouven : if people would 'invest' into the token -> there usually is an expectation for returns. otherwise - it could be just a donation?!
00:06:18 From rouven : @darrell - and how could the token solve this compared to a voucher, or someone donating a usd token?
00:08:51 From windley to Nicky Hickman(Privately) : Rouven and I have been having this argument for two years. I don't think we're going to resolve it here.
00:08:56 From Darrell : I'
From Richard Esplin : @rouven With a native token, it's easier to build on ramps that don't undermine privacy (you can buy from the network itself). Off ramps only matter if you need liquidity.
From Darrell : @rouven - just saying "I can't be seen to use" is similar to "can't afford"
00:09:19 From Nicky Hickman to windley(Privately) : I see - he seems to be missing the point that there are two ways of using the token
00:09:36 From rouven : Developing value in a refugee camp or so are interesting concepts. But how would this model of local economy tokens with the one Sovrin token?
00:09:49 From Nicky Hickman to windley(Privately) : Darrell hits on this important point about tokens masking exclusion
00:09:53 From rouven : > you can buy from the network itself
00:10:11 From rouven : Richard -> buy from the network? From a steward?
00:10:35 From Grace Rachmany : Money and value are not equivalent.
00:10:37 From rouven : Stewards could just 'sell' USD tokens against a credit card payment :)
00:10:41 From Nicky Hickman : I think he means 'network' of people @ rouven
Richard Esplin : @rouven There are various models. I don't know what the Sovrin network would choose.
00:13:25 From windley : @rouven, using single-use credential for value transfer is definitely an interesting model. But I don't think that removes the utility of on-network value exchange. If nothing else, it simplifies use case development by providing a single, well-known API for value transfer that use case developers can depend on without having to solve the problem on their own. The other benefit is finality (the value and credential exchange occur simultaneously).
00:13:27 From rouven : + 1 value not money. But isn't the topic here the Sovrin token - which is expected to have monetary value … ?
00:15:19 From rouven : @phil - onchain value transfers can be very beneficial. just could also be a stabletoken representing a currency :)
00:15:42 From windley : Sure. No argument there.
00:16:37 From windley to Nicky Hickman(Privately) : I think you ought to start on the universal service discussion or we'll run out of time (15 minutes left)

00:16:55 From Nicky Hickman to windley(Privately) : sure let's do that
From rouven : Could someone share the ideas about scaling the token transactions to use it for payments? What are the plans around privacy aspect using a UTXO model for the token transfers?
From rouven : ^^ it's late, not sure the question made sense. Basically thoughts on scaling and privacy? :)
00:22:48 From Adrian Gropper : Yes! Like clean water protects all of us.
00:23:32 From Adrian Gropper : Like Aadhaar but better
00:25:08 From Drummond Reed : +1
00:26:21 From Juan Caballero : should we use the yes/no buttons?
00:26:24 From Juan Caballero : to poll?
From Grace Rachmany : I understand we are supposed to raise our hand or say +1 or show our video to show our hands.
00:26:49 From rouven : next to the 'raise hands' -> we could use 'yes' or 'no'
00:27:05 From Grace Rachmany : we can?
00:27:09 From Juan Caballero : @Gihan: like "gas" or "usage fees" (for admin functions)
00:27:14 From Nicky Hickman : of course yes/no sounds good
00:27:20 From Grace Rachmany : Oh yeah, there is one of those. Let's do yes/no
From Grace Rachmany : That would align with my goal of using at least 1 new Zoom feature per day!
00:27:54 From Adrian Gropper : +1
00:27:58 From rouven : A token will also create extra friction :)
00:28:09 From Nicky Hickman : happy to help with your learner passport @Grace :-)
00:28:27 From Grace Rachmany : #rourven, you just gave the idea, use the buttons!
00:28:27 From Drummond Reed : Ironically, the real work wallets we use today we use for two things: 1) credentials, 2) money
00:28:34 From Drummond Reed : "world"
00:29:38 From Nicky Hickman : we have also considered that there are some basic digital identity credentials that are essential for everyone e.g. birth notification
00:30:43 From windley : @rouven only if it's the only allowed option

Digital Harms - Crowd sourcing the concept

Thursday 22B
Convener: Jeff Orgel
Notes-taker(s): Jeff Orgel

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Where are the boundaries of legal reach in terms of differing cultures?
It could be very beneficial to have verbiage to categorize / tag the delivery of harms; terms suggested "medium" / "vector" / "commonly seen as". Could be helpful for people e assess which of those factors fit into their relationship with I/T systems.
The idea of the Blinding Identity Taxonomy (BIT) came up as a hard test standard for protecting PPI. Risk overlays and sensitivity was recognized as rather unique and it would be great to offer individuals the ability to craft these variables and adjust their threshold to PPI influences almost to the level of a sort of Relational Digital DNA.

The concept of simple nouns and verbs being used early on in the surfacing and structuring references to such sorts of harms may help keep the simplicity in play in the arena of complex interplay of factors. It would help keep understanding of these factors more familiar as people think up and down the stack of expressing their thoughts and asking questions.

The concept of negatives harms possibly, and in some cases certainly, carrying a benefit as a secondary effect was explored. Example: someone spoofs me and makes me look like a genius. A shaky benefit but a maybe a benefit…somewhat – maybe? A tenuous badge of honor for sure and maybe a setup to collapse reputation after the unwarranted credit is taken? …and around and around we go then…

Frankly a fantastic gathering and much more. For a group sanctioned recording of the audio file please request @ jeffo@whatisyourrealit.com . I will look to make it available to this space as well.

An Aries Agent In A Browser Tab: Who Owns It, Who Controls It, Is It Even A Good Idea?

Thursday 22C
Convener: Bruce Conrad
Notes-taker(s): Bruce Conrad

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Repo about the problem we're attempting to solve by using an agent in a browser tab:
https://github.com/Picolab/DIDAuth-to-Manifold

Link to the slides presented: bruceatbyu.com/s/ManifoldSSI
The web application is called Manifold, and our production instance is at: https://manifold.picolabs.io

Repo for experimenting with, and provisioning, an agent in a browser tab:
https://github.com/b1conrad/browser-agent [note that the readme file is dated, referring to the agents a "sovrin Indy agents" when they are actually Aries agents]

All of this work is supported by Pico Labs (supported by the Office of the CIO (supported by Brigham Young University)), hereby acknowledged, and is entirely open source, and your participation is totally welcome.

Zoom Session Chat:
From mario Bonito to Everyone: (05:01 PM) +1 Joe Was thinking the same thing
From Me to Everyone: (05:06 PM) bruce_conrad@byu.edu ACA-Pico GitHub.com/Picolab
From Christopher Hempel to Everyone: (05:30 PM) https://caniuse.com/#feat=indexeddb
From Me to Everyone: (05:31 PM) developer.streetcred.id (or developers, not sure)
From dannysuarezpab to Everyone: (05:32 PM) Amazing Bruce

Let's Bring Blogging Back!! Let's Discuss A Collective Community Strategy

Thursday 22D
Convener: Kaliya Young
Notes-taker(s): Scott Mace

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

When this community formed in 2004-2005, Doc went around and encouraged everyone to start their own blog. Made a significant difference in several ways. Brought the conversations on our mailing lists out in the public. Who goes and finds mailing list archives. New people joined our community as a result. And people were heard on their blog so they were projecting less into mailing lists, quality shifted on the MLs. Was a rich vibrant community. 15 years later, would love to explore what we could do to bring blogging back. Actively reading each other's blogs. Do you have a blog?

Johannes Ernst: I was one of those people 15 years ago. Was rather unusual in the sense that people were blogging both personally but also from a corporate perspective. Not only broadcasting but engaging with backlinks and comments. The entire community innovated better. Not knee-jerk social media reactions or flame wars on mailing lists. It would go back and forth. Kim Cameron went out of his way to link to companies much much smaller than his, like mine for example. Not just marketing speak. I currently run several blogs. In the Indyweb world, they resurrected the idea of a webring. Maybe we could do something similar here.

Scott: Blogging is worthwhile. I'm a writer and really need to find paying work. But this is an important community.

Dee Platero: I was thinking about writing a blog. Want to share with people who aren't technologically inclined. And I'm a new person to this space. Ideas I could contribute.

Eric Welton: I don't produce a blog, but I consume blogs. Here to see it. Something has changed in the internet as we've gone from a pretty tight community, the web, there was a lot of great community and coordination. So much stuff that isn't worth reading. Production of quality content needs to come back in communities like this. Want to prote and see how that develops.

infominer; I'm a curator. I care about finding. A lot of junk out there. It's coming down from the top too. Have to be really diligent to find good sources.

Geovant Federecheski: I do have a blog I write twice a year mostly in Portguese. Thinking about writing about SSI more in Portuguese. It's going to be interesting.

Karyl Fowler: I have a blog but almost everything on it has to do with the company I co-founded, Transmute. Enterprise supply chains. Kaliya in reading her blog, talked about writing more passionately and personally. One post like that got way more traction.

Bruce Caron: It would be great to find new communities of bloggers. Syndicated feeds disappeared. Google stopped doing their feeds. Now it just adds to email. Great to have utilities to help you find the blogs. Used to be blogs with 5 links I discovered this week, would like to see more of those back again

Estee Solomon Gray: Pulled my writing energy into a book. I and others are being called to blog again. I'm inputting and I'm doing nothing with it. I love the idea of this community interconnecting. What the F is going to come out of this? How will each of us put the world in the right direction, has become the big question.

Kaliya: Maybe 2 levels to this conversation. Us, and the wider world.

Estee: It shouldn't have been surprising the IIW thing is exactly the people who I want to be stepping into the conversation about what we're making here.

Karen Advocate: Just started blogging first part of March when COVID hit Seattle. You put yourself out there and find people you wouldn't have found. We're in a climate change crisis beyond crisis. We have to do a huge reset. To me the COVID crisis is giving us that time. We need a different world. Nobody had to hop on an airplane to do it. I think it's pretty awesome. But what I don't know, I've heard of Medium and other things, I don't know what reaches to the people we need to be connecting to that are getting so much information, particularly off of Facebook.

Josh Verberg: I don't write a tech blog. Focuses on local government. I come from a very large corporation. How can we be better about communicating what we've experimented with, and be better stewards of information, and be a better neighbor. Looking to see how I can contribute.

Tom Brown: With Weather.com. Posting notes on IIW on my blog. Participate in IndyWeb, IndyWeb reader is like the old Google reader, interactive.

Shannon Casey: I'm just here for inspiration to start blogging.

Kaliya: If we were to report out at the end of the day, what would we invite the community to do to get more blogging out of the community?

Karyl: A perpetual tag. More naturally aggregate what everyone is outputting?

Kaliya: Yes.

Johannes: Ways to keep in touch with people I learn about here.

Josh: What is the scope of the community?

Kaliya: IIW and SSI community rather than bigger identity.

Infominer: Original Planet Identity feed, software, we could make a feed for everybody, so there is one place we can go.

Q: Slack?

Kaliya: Costs a lot of money. Maybe pull in RSS feeds to the IIW Slack?

Bruce: First people who looked at Slack said you're adding extra features we don't need on a service we don't use. Slack didn't care.

Q: Has IIW had anything other than the archives?

Kaliya: We're kind of the anti-brand. To me this wasn't an IIW branded thing, more like can we get a group of people inspired to blog more in part for each other. Superpat ran Planet Identity. Isn't up anymore. Infominer has been playing with that same family of software.

Karyl: I'm happy to help.

Q: Who is the audience for the blogging?

Karen: If it's just the techhies, do it. Ordinary people, you've got to meet them where they are.

Scott: Have we used Twitter lists?

Kaliya: And we've had Twitter lists for all the IIWs except maybe 29. So how do we use Twitter, and maybe LinkedIn.

infominer: Using Twitter lists. We have the technology, pull that back into RSS and there is a way, one app called Huginn that allows you to watch certain things, you can watch your Twitter list, filter it so that you get a custom feed from that.

Scott: That sounds interesting.

Bill Wendel: I first used Qiqo four years ago. Are we trying to build a thriving P2P identity community after this week?

Kaliya: This is a great segue.

Bill: I have had a blog since 2005, done about 850 posts in a vertical. I am a vertical expert trying to translate identity into real estate. In Qiqo I do events around real estate issues. If you want to get beyond our own community, you have to position yourselves as problem solvers for the world. COVID shows the firepower in this community.

Kaliya: Yes. I think I called this session in part because we as a community have not been conherent to go out in a wider world. More active blogging can grow that.

Geovane: Consistency?

Kaliya: Even if it's a short thing, 1 blog post each week from each person would be powerful.

Bill: This is where i would say, if I knew there was a stream of comments, I would look half a dozen times a day at comments from the sessions. Tim Ruff's frustration is palpable. Potency in the community to solve problems. How do we solve problems and build revenue?

Kaliya: Maybe we need to do some community clearing. The nerves are part of the problem. We have a culture that doesn't feel comfortable with conflict. This community resolves conflicts. But if we're committee to open standards and interop…[walk the talk]. Is the product consistent with open standards or not? I don't want to have a public blog fight about this either. Lots of companies who are posers, using SSI language, not adopting any of the open standards. So how are we socially policing ourselves.

Bill: We need nonviolent conflict resolution strategies.

Kaliya: If we were to use qiqo on an ongoing way, how would we use it?

Bill: Events I hosted 3 years ago. Was delighted to find out IIW was using it, to see the improvements made. It's really continuing the continuity between events. You owe it to the platform and the richness of the experience to try that. It does send out a weekly update of conversations you're following.

Kaliya: Can everyone put your blog in the chat?

Estee: Carol can you go back to your original concept? Intersection between you as company and you as person.

Karyl: I came to this space from genetic data space, very much my identity. I didn't blog until Medium. I posted one personal post, it has the most viewership in my blog. Developing a human brand online when we can't meet with each other somehow serves a purpose. Beyond being Transmute founder.

Estee: For me, this COVID time, people have been delighting seeing MSNBC hosts in their homes. The private/public, all this stuff has been, it makes sense to do it as both, multiple?

Kaliya: The people's blog centered on their professional life, but included little bits of their life that were personal that were relevant. Millennials don't blog. They do other things we don't.

Estee: We've been alert to surveillance issues way longer than others. I can't see any way to live through the next two years without doing contact tracing.

Kaliya: It's almost like we need a verifiable credential to prove you were at IIW. Work with Lucas on how his platform could adopt identity tech stuff.
Estee: Important to take something out of this idea here.

Kaliya; Inviting people to commit to blogging at least once in the next month. Use qiqo in an ongoing way. Language translation. Mentoring. Starting a Slack blog pod.

Zoom Chat notes follow:
From Johannes Ernst (Indie Computing) : Main blogs: https://reb00ted.org/ , https://upon2020.com/
From Kaliya Identity Woman : The question is … who are you…your blog if you have one :) and then why you came to this session....
15:43:00 From Bruce Caron : Here's my main blog: https://cybersocialstructure.org/
15:43:20 From Karen Advocate : Since COVID-19 began, with the encouragement and help of Kaliya, I started blogging for the first time: www.letshaveaplan.blog
15:43:24 From Karen Advocate : Goal is to harness this public health crisis and help us transition to new resilient, sustainable and just economy/society.
15:44:32 From Geovane Fedrecheski : I write about twice a year here: https://geonnave.com/posts/identidade-auto-soberana/
mostly in Portuguese though
15:46:01 From Tom Brown : herestomwiththeweather.com
15:46:44 From Bill Wendel1 : Just joined: Is blogging discussion about Digital Identity specifically, or collaborative blogging in general?
15:47:20 From Josh Verbarg (State Farm) : Feedly

15:47:29 From Karen Advocate : The later. Picking up from 2004 when Doc Searles suggested we all blog and read each others' work and collaborate.
15:47:33 From Kaliya Identity Woman : It is about - seeing if we can get the community around identity to start blogging more - connecting to each other.
Johannes Ernst (Indie Computing) : Note: there are many Google Reader replacements available … from hosted services to open-source software for self-hosting like Selfoss or Nextcloud News.
15:48:34 From Bruce Caron : Book to blog!
15:48:51 From Infominer : or maybe we could host a reader fitted with ID blogs\feeds, where the community could curate feeds in some collaborative fashion? (wink wink)
15:49:57 From Karyl Fowler : +1^I like this idea
15:53:01 From Johannes Ernst (Indie Computing) : There used to be Planet Identity …
15:53:13 From Kaliya Identity Woman : INfominer this is your cue….
15:53:50 From Bruce Caron : currently happening: https://www.eventbrite.co.uk/e/reset-everything-a-virtual-conference-about-our-changing-world-tickets-102077833548?utm_source=eventbrite&utm_medium=email&utm_campaign=reminder_attendees_event_starting_email&utm_term=eventname&ref=eemaileventremind
15:54:17 From Karen Advocate : It is going to be a very different world....and we either shape it or it will be done to us. Since COVID-19 began, with the encouragement and help of Kaliya, I started blogging for the first time: www.letshaveaplan.blog
Goal is to harness this public health crisis and help us transition to new resilient, sustainable and just economy/society.
16:00:06 From Tom Brown : blog rolls
16:00:54 From scottmace to shancasey(Privately) : I sent you a message with my contact info - should be in the email associated with your IIW login.
Karen Advocate : Hastag #IIW Feels a bit exclusionary if trying to engage beyond 350 - IIW folks.
Eric Welton (Korsimoro) : gotta chg space - very much looking forward to reading what you all write! happy iiw all.
Johannes Ernst (Indie Computing) : I got to run an errand … not sure when I'll be back. Stay safe and connected in the meantime!
16:07:09 From Infominer : https://github.com/infominer33/pluto-planet-demo
16:07:52 From Bruce Caron : Didn't Slack start as a custom client for RSS feeds?
16:08:23 From Infominer : https://rss.infominer.id/i/
16:08:47 From Infominer : ^^^ demo of a hosted reader
16:12:30 From Karen Advocate : Can I ask who is the audience for the blogging?
Bill Wendel1 : Kaliya, Think i heard you mention QiQo earlier. Is one of your goals to develop QiQoChat as a thriving peer to peer for the identity community after this week? Ive used it sparingly over the past 4 years, and know that it's go a Q&A function built into it. If those Q's linked to the sessions we've attended, I think that might build a following and continuity between semi-annual events.
16:19:33 From Infominer : ooooo
16:19:39 From Bruce Caron : OOPS… it was an IRC client (not RSS). my bad.
16:20:42 From Infominer : thx for clarification, bruce. now my curiosity is piqued
16:29:30 From Karyl Fowler : karylfowler
16:29:30 From Bill Wendel1 : Karen, see http://realestatecafe.com/blog
16:29:35 From Karyl Fowler : https://medium.com/@karylfowler
16:29:47 From Tom Brown : herestomwiththeweather.com
16:29:59From Karen Advocate : Started tweeting after Occupy Wall Street: @_KarenAnna Started blogging after first US COVID-19 out break: www.letshaveaplan.blog COVID-19 provides the disruption opportunity we need to do a reset. We are banging pots for the healthcare workers right now.
16:30:01From Bruce Caron : On IRC and Slack: https://tedium.co/2017/10/17/irc-vs-slack-chat-history/

16:30:51From scottmace : My blog (fairly inactive) on Blogger: http://openingmove.blogspot.com
16:33:42 From Bill Wendel1 : Love what you're saving Estee
16:33:47 From Bill Wendel1 : * saying
16:39:24 From Geovane Fedrecheski : Rebooting the web of rings
16:39:45 From Bruce Caron : Blesting with books
16:40:02 From Karyl Fowler : lol
16:40:22 From Bruce Caron : visitor just arrived… got to hop off.
16:41:50 From Tom Brown : +1 for languages!
16:42:26 From Karen Advocate : I cannot even figure out how to get people to sign up for my blog.
<3 Pleasure to meet all of you. Thank you Kaliya!! I need to participate in my weekly frontline call with NYC, so won't be at the closing circle.

Learning Wallets

Thursday 22E
Convener: Timothy Ruff

Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

FYI to all -- here's the learner wallet spec coming out of the U.S. Chamber of Commerce's T3 Innovation effort:
https://docs.google.com/document/d/1gBKx47cgxsUnTMLxqg6Poswp4-led3x51unUY42fKUU/edit#

Come Teach A Student How ZKP's Work Technically. Anybody Else Who Wants To Know, Please Come, And Someone Come Teach Us!

Thursday 22F
Convener: Michael Black
Notes-taker(s): Michael Black

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Useful Slides: https://docs.google.com/presentation/d/1hGEpWIpl9hp8QoTIXjlozY7Gzy6zXY9lAL2x6U1b7Fk

Shoutout to Brent Zundel for teaching! Shoutout to Mike (malwhere) for the support!
Brief overview
an anonymous credential is a verifiable credential
Anything that isn't explicitly made public will not be disclosed on verification

A holder identifier can be used to bind to a holder but other methods can be used like a blinded secret

Anonymous vs. Verifiable
Anonymous is a verifiable credential but doesn't disclose values

Must be comfortable with exponents and modular arithmetic to understand ZKP technically

Prime field is a finite field that contains a prime number of elements

Diffie Hellman

- Generate prime n
- Pick a random 1 < g < n
- Alice chooses random a
- Alice computes:
- Alice sends A, g, and n to Bob
- Bob chooses random b
- Bob computes
- Bob sends B to Alice

Went over RSA

RSA
Things to remember g^x mod n
g is the generator and the holder knows but can't change x

ZK Protocol

- verifier needs to know holder can't cheat
- holder needs to know verifier can't discover secret
- Both contribute to randomness
- randomness is unique per transaction

NIZK
Prover convinces Verifier she knows x
Prover receives n, g, i, H
Prover
Generates: random r < n
Computes:
a test value:
a commitment to the secret:
a challenge hash:
a challenge value:
Sends: y, s, cH to Verifier

- Important for verifier to pick a good hash function
- That's where the probability comes in

Make a commitment to every single message (blind everything you are proving)

- commitment (g^x mod n)

- blinded commitment (g1^x * g2^r mod n)

A credential ({m}, A, e, v) consists of these values:
Attributes (integers): {m1, m2, …, mj}
Signature (integers) (A, e, v)
Issuer Private Key (p', q') where p = (2p'+1), q = (2q'+1), p*q = n
Issuer Public Key (n, S, Z, {R})
Modulus n
Random numbers S, Z < n
Random number {R1, R2 , … , Rj}

Sorry if the notes are hard to follow. Honestly the slides walk through all of this and is much more readable

recommend going through the math step by step to help learn / Stepping through really helps understanding

IIW30: The Session Collection & Song List

Thursday 22G
Convener: Jeff Orgel

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Message from Jeff Orgel
A gift to the community. From the images on the next couple pages comes this song list is relative to each of the three days we shared together expressed as an album – as we do make music of a sort together . There is hopefully relatable tone to your experience in some of these titles and I would love to hear back from anyone who has lyrics, thoughts, a beat and or a melody that we can expand on together in such a way!

Please hit me back @ jeffo@whatisyourrealit.com if you've got something! Great being with you all!


Day 1
The XXX Sessions
IIW
mmxx


Day 2
The XXX Sessions
IIW
mmxx


Day 3
The XXX Sessions
IIW
mmxx

ZKPs For JSON-LD Using BBS+ - Round 2

Thursday 22H
Convener: Tobias Looker
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Links to repository:
https://github.com/mattrglobal/node-bbs-signatures
https://github.com/mattrglobal/jsonld-signatures-bbs
https://github.com/mattrglobal/jsonld-signatures-bbs-spec/

Link to slides: https://drive.google.com/file/d/1X1JApxDY48MJYYACNT9NPsgpZWft0wHk/view

Zoom Chat discussion:
10:29:32 From Daniel Burnett : FYI: THIS SESSION IS BEING RECORDED
10:29:46 From Oliver Terbu : 0:30 cet ;)
10:33:33 From Daniel Burnett : REMINDER: THIS SESSION IS BEING RECORDED
10:34:06 From Wayne Chang : +1 to recording reminders
10:38:48 From Siva Kannan : Is there a link to the deck?
10:39:36 From Oliver Terbu : Does it support range proofs in general?
10:39:37 From Oliver Terbu : q+
10:39:50 From Orie Steele : This suite does not.
10:40:10 From John Jordan : BC Gov is also funding Mike's work and we are eager to bring this capability to the higher layers

10:40:11 From Oliver Terbu : Yeah, but would it be possible in a kind of efficient way?
10:40:20 From Orie Steele : But that can be handled with a higher order constructions
10:40:31 From Kalyan Kulkarni : Can the link to this deck at the bottom be shared on chat?
10:40:36 From Orie Steele : See John Jordands answer :)
10:40:40 From Oliver Terbu : I am personally not super excited about range proofs but just wanted to know

10:40:55 From Daniel Burnett : REMINDER: THIS SESSION IS BEING RECORDED
10:41:23 From Kyle Den Hartog : @nader do you have the link to the slides?
10:41:47 From motoko : since you are using BLS can you do compact aggregation like BLS multisign?
10:43:08 From Kyle Den Hartog : We currently use the BBS+ signature scheme only, but I believe it would be possible to support BLS signature schemes for aggregation as well, but that would need to be defined and implemented before I'd say definitely yes.

10:44:52 From Nader Helmy : Original presentation is in a private drive so I created a copy that's open to the public

10:44:54 From Nader Helmy :
https://drive.google.com/file/d/1X1JApxDY48MJYYACNT9NPsgpZWft0wHk/view?usp=sharing

10:45:07 From motoko : perhaps two different proofpurpose, one for assertion with selective disclosure and one for multisign?

10:45:20 From Kyle Den Hartog : github.com/mattrglobal/node-bbs-signatures/
10:45:33 From Andrew Whitehead : Is there a use case for multi sign?
10:46:10 From Oliver Terbu : Does the library work in a mobile react-native environment as well?
10:46:24 From Oliver Terbu : I saw that it requires some rust bindings
10:46:28 From Nader Helmy : Let me clarify these are the slides for the presentation: https://drive.google.com/file/d/1X1JApxDY48MJYYACNT9NPsgpZWft0wHk/view?usp=sharing

10:46:54 From nembal : ty Nader
10:46:57 From Kyle Den Hartog : @Andrew I can think of a few for a web of trust issuance model where issuance is not authority based, but rather based on the number of people who issue the same data. For example, 17 people say my name is Kyle, therefore a verifier believes my name is Kyle.

10:47:40 From Anil John : Great choice of example! : -)
10:47:47 From Sam Curren : can issue a certificate that says your name isn't kyle?
10:48:28 From Oliver Terbu : thanks!
10:49:52 From Andrew Whitehead : I believe that getting the BBS+ signature scheme officially supported for w3c verifiable credentials is one goal, and doing the same for BLS signatures would be another

10:49:53 From Kyle Den Hartog : @Sam, I enjoy your rabbit hole, but will opt to not go down it right now :)

10:50:02 From Kyle Den Hartog : For the first time ever…
10:50:05 From Oliver Terbu : Would you need an additional proof of control?
10:50:28 From Oliver Terbu : Because the proof could also be produced by the issuer
10:50:51 From Oliver Terbu : Or whoever has the credentials + the public key of the issuer
10:51:38 From Markus Sabadello : I had the same question yesterday... Where's the (equivalent of) a link secret?

10:51:41 From Orie Steele : So just like a normal VP, proofPurpose authentication
10:52:00 From Oliver Terbu : Yep, thanks!
10:52:40 From Oliver Terbu : Still awesome!
10:52:42 From Nader Helmy : You can use this derived proof in two ways, either by disclosing the subject DID or using some form of link secret. The former is possible today the latter is TBD

10:53:07 From Nader Helmy : On the roadmap :)
10:53:32 From Oliver Terbu : Yep, for the first you would have correlation issues
10:53:37 From Mahmoud Alkhraishi : I think im missing something basic here, but what do I need to provide to someone else to let them know that I am over 18 for example, is it just the proof in the json ld proof section

10:54:17 From Orie Steele : @Mahmoud this will only let you disclose existing terms, it does not support predicate proofs today.

10:54:59 From Nader Helmy : @Oliver right exactly, its a tradeoff.
10:55:20 From Oliver Terbu : Still cool, because you would have a way more efficient proofformat
10:55:50 From Oliver Terbu : Looking forward to the linked secret though

10:55:57 From Kyle Den Hartog : https://github.com/mattrglobal/jsonld-signatures-bbs
10:56:04 From Kyle Den Hartog : This is the library being shown right now
10:57:53 From Orie Steele : THE CROWD GOES WILD!!!!!!!!
10:57:59 From Mahmoud Alkhraishi : +1
10:58:04 From Markus Sabadello : What's the idea behind storing the "revealedStatements" as a separate JSON-LD property? Couldn't that same data also be encoded as part of the "proofValue"?
10:58:25 From jer : what are the inputs to the verify step?
10:58:32 From Kyle Den Hartog : https://github.com/mattrglobal/jsonld-signatures-bbs-spec/
10:58:38 From Oliver Terbu : ^jer
10:58:55 From Kyle Den Hartog : This is a link to the spec which is the top link shown. The second link is https://github.com/mattrglobal/jsonld-signatures-bbs

10:59:02 From Sam Curren : Markus - that could be done.
10:59:24 From Sam Curren : also, totalStatements.
10:59:57 From Nader Helmy : Standardizing on schema attributes is what JSON-LD is for
11:00:15 From John Jordan : UX issues …
11:01:21 From Keith Kowal : Can you tell a little more about how you could prevent someone from removing a needed value like a credential expiration date?

11:01:25 From David Waite : If I understand the document per Jer's question, the verification takes in the revealed indices, total statements and input proof document statements?

11:01:52 From Kyle Den Hartog : https://github.com/mattrglobal/jsonld-signatures-bbs-spec/
11:02:41 From Oliver Terbu : The API looks very slick, so good job!
11:02:57 From Sam Curren : david: everything shown. the things you mention, and also the attributes revealed in the doc.

11:03:57 From Oliver Terbu : What is the size of the dependencies?
11:04:30 From Orie Steele : How can I use the right now?!?!!? :)
11:04:43 From Orie Steele : npm will tell you
11:04:47 From Oliver Terbu : haha
11:04:50 From Oliver Terbu : I was just too lazy
11:04:52 From Siva Kannan : Can I delegate the responsibility of reveal to someone else? Or, that has to happen out of band?

11:05:10 From Markus Sabadello : when will the Java implementation of this be released? :) *duck*
11:05:16 From Andrew Whitehead : I can tell you the python lib is about 1.7mb, which probably includes some bloat..

11:05:19 From Oliver Terbu : +1 Markus ;)
11:05:34 From Orie Steele : +1 Markus, I know there is some work ongoing for python
11:06:10 From Oliver Terbu : Thanks andrew
11:06:34 From Kyle Den Hartog : @Oliver Bundlephobia is not revealing that information to me at the moment. I suspect it may be able the same as what Python has.
11:06:35 From motoko : link to BBS+ library?
11:06:36 From Andrew Whitehead : (That doesn't include the JSON-LD parts, just signatures)
11:06:40 From motoko : curve?
11:06:41 From Oliver Terbu : Do you have a timeline and roadmap?
11:06:43 From Paul DIetrich : Great work. Thanks so much!!

11:07:16 From Nader Helmy : Here's the BBS+ signatures repo
11:07:17 From Nader Helmy : https://github.com/mattrglobal/node-bbs-signatures
11:07:23 From jer : who can generate a derived proof, the issuer and/or subject?
11:07:32 From Nader Helmy : the Rust dependencies are in Hyperledger Ursa as mentioned
11:07:54 From swcurran : Tell me about the canonicalization? Isn't that a problem?
11:09:07 From Orie Steele : Its not, its what is used to produce the messages that are signed.
11:09:07 From Oliver Terbu : Big big big kudos to mattr to get rid of the ledger-dependency
11:09:14 From swcurran : +1
11:09:33 From Micah McG : 
11:09:35 From swcurran : I wasn't serious about canonicalization.
11:09:38 From Anil John : ^ +1 to what Oliver said!
11:09:47 From Orie Steele : @swcurran canonicalization and framing are JSON-LD things this this library and implementation depend on
11:09:58 From Orie Steele : :)
11:10:06 From swcurran : :-)
11:10:23 From Orie Steele : Its one of those things I hope to never discuss again :)
11:10:39 From swcurran : I will never raise it again. Promise
11:11:14 From Sam Curren : I'm thinking Orie gives a json-ld 101 next IIW.
11:11:24 From Kyle Den Hartog : @motoko https://github.com/mattrglobal/node-bbs-signatures
11:11:34 From Andrew Whitehead : Oh yeah Orie loves giving those 101 sessions
11:11:39 From Orie Steele : rofl
11:11:44 From Mahmoud Alkhraishi : maybe 10001
11:11:50 From Kyle Den Hartog : Curve used is BLS12-381
11:12:22 From Orie Steele : You can use this without DIDs though
11:15:25 From Andrew Whitehead : Okay but what about canonicalization?
11:16:12 From Nader Helmy : There's a spec! Please review and open issues
11:16:14 From Nader Helmy : https://github.com/mattrglobal/jsonld-signatures-bbs-spec
11:16:52 From Oliver Terbu : Also kudos to Orie!
11:17:05 From Nader Helmy : We want to get this ready in time for the Linked Data Security standardization happening later this year
11:17:47 From Nader Helmy : Big thanks to all the prior art provided by Hyperledger Aries/Indy communities

11:17:48 From Mahmoud Alkhraishi : Thanks!
11:17:55 From Orie Steele : THANK YOU!

Build An SSI Proof of Concept on Sovrin – Apply What You've Learned At IIW & Get Support From Our Team

Thursday 22J
Convener: Riley Hughes & Streetcard ID Team
Notes-taker(s):

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

****Instructions for Building a Proof of Concept Session****

1. Get set up on Streetcred Developer Portal by following the directions here: https://www.notion.so/streetcred/Login-to-Streetcred-Portal-d81e04a7e07746e5af930c677b5cd6ce
2. If you want support from our team, join IIW Slack: https://join.slack.com/t/iiw/shared_invite/zt-e08ieit0-7~iZLzYJBIuaD6CG55YH7w
3. Once you're in Slack, add yourself to the channel #proof-of-concept

Then, begin working on your proof of concept!

1. Consider your use case
    a. Is there something you're working on for your current company?
    b. Do you have a startup idea you'd like to prototype?
    c. Do you want to just do a demo or tutorial to understand how it works? (if so, use this link: https://docs.streetcred.id/docs/tutorial

2. Identify the actors
    a. Who is the verifier?
    b. Who are the issuers?
    c. Who is the holder?

3. Build out the flow using the Streetcred Developer Portal
    a. Set up organizations for the issuers and verifiers
    b. Set up Credential Templates for the issuers
    c. Set up Verification Policies for the verifiers

4. Determine next steps
    a. Use the API to integrate into a demo application
    b. Build a business case
    c. Validate ideas with stakeholders

Demo Hour

Thanks to our Demo Hour Sponsor

IIWXXX #30 Community Sharing / DEMO LIST

Tuesday April 28, 2:30 - 4:30 & Wednesday April 29, 1:30 - 2:30

DEMO SPACE

1. **MySudo by Anonyome Labs :** Steve McCown & Jon St. John
   URL: https://mysudo.com
   MySudo helps users manage activity-based identities called Sudos, which sandbox online activities using unique contact points (e.g., phone, email). Upcoming Sudo versions will contain Self-Sovereign Identity elements for added security and interoperability with other SSI agents.

2. **Workday Inc. Badges with Workday Credentials & WayTo by Workday:** Kendra Bittner
   URL: https://www.workday.com/en-us/applications/credentials.html
   Using blockchain technology, Workday Credentials* offers organizations a way to securely request, issue, and verify credentials for a worker's skills, education, certifications, and more. See how we leverage open badges to provide a publicly shareable and discoverable artifact backed by your private verifiable credentials

3. **HearRo Identity Based Communication (IDC):** Vic Cooper - CEO HearRo, Inc.
   URL: www.hearro.com
   The need for organizations to easily connect with their customers/citizens in highly personalized yet secure and efficient ways has never been greater or more urgent. See how HearRo uses SSI and DID Comm to enable secure "1-click" communications between People, Organizations and Things.

4. **Validated ID - eIDAS Bridge:** Albert Solana / Xavier Vila
   URL: https://joinup.ec.europa.eu/collection/ssi-eidas-bridge (will be available this Friday)
   This project proposes a way to interconnect SSI with eIDAS Trust Framework by sealing credentials with Qualified Electronic Certificates. On this demo we will show you how.

5. **SeLF & esatus Wallet by esatus AG:** André Kudra & Christopher Hempel
   URL: https://self-ssi.com/en/
   SeLF integrates Self-Sovereign Identity into exiting IT-infrastructure. SSI credential-based access rules are transformed into authentication and authorization objects that can be synchronized and used by conventional technologies like SAML or OIDC.

6. **JLINC Labs:** John Wunderlich/Iain Henderson
   URL: https://jlinc.com
   Description: TBD

7. **Spherity Cloud Wallet:** Michael Rüther & Juan Caballero
   URL: https://spherity.com
   We will demonstrate our TPRM consortium solution, which allows cloud-based custodial wallets to present and exchange credentials.

8. **GS1 (the organization behind the barcode):** Phil Archer
   URL https://gs1.github.io/DigitalLinkDocs/principles/
   Live demonstration and discussion of the GS1 resolver. Not a DID resolver, but nevertheless a decentralized, self-sovereign system for resolving identifiers to multiple related resources over HTTPS.

9. **MattrGlobal - A performant ZKP capable digital signature scheme for use with attribute based credentials / verifiable credentials: Tobias Looker**
   URL: https://mattr.global/ https://github.com/MATTRglobal
   A demo of a performant ZKP capable digital signature scheme that enables multi-message signing and selective disclosure. We will demo how this digital signature scheme can be used to create selectively disclosable verifiable credentials.

10. **Transmute:** Margo Johnson, Karyl Fowler, Guillaume Dardelet, Orie Steele
    URL: https://www.transmute.industries/
    Transmute brings emergent technology like decentralized identifiers and verifiable credentials into global supply chain transactions. This technical demo features several core enterprise agent functions, including OICD integration, encrypted data storage, and interoperable credential exchange with the Credential Handler API.

11. **Danube Tech: Universal DID and VC Infrastructure:** Markus Sabadello and Philipp Potisk
    URLs: https://uniresolver.io/, https://uniregistrar.io/, https://uniissuer.io/, https://univerifier.io/
    We will be demoing tools such as the Universal Resolver and related tools, which allow the use of DIDs and VCs in a way that provides interoperability with as many different technologies and vendors as possible.

12. **ArcBlock "A new way to manage decentralized identities using ArcBlock's ABT Wallet."** Matt McKinney, Jon Lu
    URL: https://www.arcblock.io/en/try-identity-now
    See how ArcBlock's ABT Wallet makes it easy to manage a user's identity and online profiles and let's app builders reimagine what's possible for their customers by using an identity-driven user experience.

13. **ConsenSys: Oliver Terbu**
    URL/Link: https://github.com/uport-project/daf
    DID Agent Framework is a pluggable SSI framework which provides CLI, graphql and TypeScript interfaces. We will show how to add SSI to existing ETH wallets using the popular WalletConnect protocol.

14. **Identity & Groups & Devices for Decentralized Applications on DxOS created by Wireline:** Chris Waclawek, David Boreham, Kaliya Young
    URL: https://www.wireline.io/
    This demo two different users creating an identity and using it to edit a shared decentralized document (that uses CRDT) - its google Apps like functionality without google in the middle. It also shows users adding devices to be able to access the same document from multiple devices.

15. **Streetcred ID:** Riley Hughes, Tomislav Markovski, Matt Norton, Michael Black
    URL: developer.streetcred.id/
    Issue verifiable credentials in 5 minutes.

The IIWXXX Demo List can also be found here
http://iiw.idcommons.net/IIW_30_Demo_Hour

Identity Tech Sandbox Fair at IIWXXX
Thursday April 30, 2020 from 8:00 – 9:00am PT

Sponsored by 

@MattrGlobal

Get a real hands-on experience with the latest Identity Tech available to IIW attendees, in one on one and small group interactions.
In the foyer to the Grand Hall ~ on your way to coffee & breakfast.

MySudo by Anonyome Labs: Steve McCown & Jon St. John
URL: https://mysudo.com
MySudo helps users manage activity-based identities called Sudos, which sandbox online activities using unique contact points (e.g., phone, email). Upcoming Sudo versions will contain Self-Sovereign Identity elements for added security and interoperability with other SSI agents.

UBOSbox: Johannes Ernst, Indie Computing Corp
URL: https://indiecomputing.com/products/
UBOSbox is a pre-configured server appliance that enables consumers and small businesses to take their data home from internet platforms such as Google Docs or Dropbox onto a server they control. No spying or tracking by third parties; no lock-in and no subscription fees. Now ships with Nextcloud Hub, the leading open-source document collaboration solution that includes Google-Docs-style collaborative editing in the browser, calendaring, chat and much more.

Transmute: Margo Johnson, Karyl Fowler, Guillaume Dardelet, Orie Steele
URL: https://www.transmute.industries/
Transmute brings emergent technology like decentralized identifiers and verifiable credentials into global supply chain transactions. This technical demo features several core enterprise agent functions, including OICD integration, encrypted data storage, and interoperable credential exchange with the Credential Handler API.

ArcBlock "A new way to manage decentralized identities using ArcBlock's ABT Wallet."
Matt McKinney and Jon Lu URL: https://www.arcblock.io/en/try-identity-now
See how ArcBlock's ABT Wallet makes it easy to manage a user's identity and online profiles and let's app builders reimagine what's possible for their customers by using an identity-driven user experience.

Selected 'Chat' Closing Circle Comments

Day 1 Closing Selected Zoom Chat

16:29:19 From Will Abramson : Well I had a top day! Just cracked a beer

16:33:32 From Marc Davis : A huge advantage of virtual meeting is during the Demo Sessions. In physical copresence having over 5 people at a demo session can make it hard for everyone to see and hear—having 50 people in a Demo Session works well in a virtual session.

16:33:35 From johnnyfromcanada : Overload - but great!

16:33:39 From Heidi Saul : So quiet! :)

16:33:37 From John Jordan : Good day .. deep content in sessions!

16:33:41 From Melanie Nuce : Love the space - love the notes access!

16:34:04 From Orie Steele : Gardens worked! I had a hallway conversation and it felt like IIW IRL!

16:34:19 From Nathan George : Happy with how even as a virtual event it feels like IIW, with the same collaborative sense of community.

16:35:01 From Drummond Reed : It's almost more IIW than the real thing!

16:40:02 From Andre Kudra : Congratulations to Andrew Whitehead being in Company of The Dude! :-D

16:40:46 From Andrew Whitehead : Don't mind my roommate, he's very thirsty :)

16:47:21 From Kazue Sako : Hi, my first virtual IIW day started midnight, I went to the first session but fallen sleep at 3:20 AM in the middle of the second session. And now I woke up for closing session. Good morning!

16:47:43 From Heidi Saul : Nicky's Haiku:
First Trust People
Over red bees wax
Or a Fax
Over IP Stacks

16:47:47 From windley : Good morning @kazue!

16:53:15 From John Jordan : And a doggy now!

16:53:48 From Sam Curren : IIW needs more dogs.

16:53:55 From Heather Vescent : This is Sugar.

16:54:00 From Nathan George : But how would we know…..

16:54:03 From John Jordan : Proof?

16:54:28 From Heather Vescent : She's my latest rescue. She is a scientist that focuses on environmental testing of soil.

17:01:23 From Heather Vescent : Definitely had some feelings like IIW IRL. Have to pop off - children are insistent about their dinnertime. See you next week.

17:02:48 From Brian Behlendorf : Yay Eddie!

17:02:49 From John Jordan : Welcome from Nairobi!

17:02:52 From Will Abramson : Legend

17:02:52 From Sam Curren : Thank you Eddie for being here!

17:06:03 From Jeff Orgel : We Are Real People Really Being People. Indeed great community.

17:19:14 From Bruce Caron : Great First day… congrats!

17:20:00 From Joe Hsy : Thanks to everyone - great first day!

17:20:12 From John Jordan : Have a great night, morning, evening, day … I miss in person but this is going well … be well and "see you" tomorrow.

17:21:10 From pknowles : Bed time for this old man! I must have jet lag.

17:21:46 From Markus Sabadello : Good night from Europe and see you all tomorrow..

17:21:57 From Robert Mitwicki : see you today ;)

17:21:59 From Kaliya Identity Woman : Good night European folks!

17:22:23 From Nathan George : Labyrinth Garden is hosting an open "SSI Hallway track" if you want to bother whoever is still listening there (maybe quiet until "tomorrow" US time).

17:23:30 From Scott Mace : Zoom helps us be in two places at once! #Teleportation

Day 2 Closing Selected Zoom Chat

17:00:51 From David Huseby : I have to say, I'm actually really happy to see all of you are well

17:01:04 From Richard Esplin : I found it much easier to skip a session and take a nap than at the Computer History Museum.

17:01:14 From Orie Steele : Same :)

17:01:27 From Grace Rachmany : I may or may not have been doing dance party while my video was off during some of the sessions.

17:01:28 From PhilWolff : Parking is easier

17:01:43 From mahod mah : Also can spend a session gardening, or cooking, and still watch / listen

17:06:20 From Karyl : @anil post the link/name?

17:06:47 From Anil John : https://www.hanselman.com/blog/GoodBetterBestCreatingTheUltimateRemoteWorkerWebcamSetupOnABudget.aspx

17:25:40 From Sam Curren : Phil is on the Grill

17:25:59 From David Huseby : The best part of IIW is the other perspectives

17:26:04 From dsearls : I believe it's 2:25am for Rouven.

17:26:27 From Phil Windley : it's Wed night, BBQ right? 🤷

17:26:41 From Sam Curren : No excuse needed Phil!

17:26:45 From Lisa LeVasseur : mmm bbq

17:26:45 From Justin Richer : I'm missing an online cocktail party for this 🤷

17:26:58 From Justin Richer : But I did have BBQ for lunch so that's ok on balance.

17:27:16 From rouven : yes, Doc - it's 2:25am. I will sign off soon …

17:28:34 From rouven : Anytime before 2am would not feel like a real IIW ;)

17:29:33 From dsearls : Instead of jet lag, some of us have conf lag.

17:29:40 From Drummond Reed : Yes, Rouven's right. I am definitely missing the late night Rouven-over-drinks discussions

17:52:52 From Kazue Sako to Lisa Horwitch (Facilitation Team)(Privately) : on View-Only IIW Agenda Day 2, I could not find when closing circle starts. would be nice if that information is included so that I know when I need to wake up to catch it.

18:05:03 From Drummond Reed : +1 to Qigochat. Lucas has performed a miracle with this.

18:06:00 From Lisa LeVasseur : i think this conference should minimally be hybrid [f2f + remote] going forward. In fact, maybe one per year could be strictly remote.

18:08:08 From Justin Richer : I'm going to get kicked out of my office soon because it's also the guest room and people are going to bed 😅

18:08:32 From Lisa LeVasseur : the platform democratizes the voices/participation somehow

18:09:28 From Wip : +1 my first IIW, been on my radar since before I started at Napier

18:09:47 From Marc Davis : Definitely agree with Lisa LeVasseur that at least one IIW per year be remote: lower cost for attending (especially for independents); sessions can scale effortlessly to more attendees than can easily be done in physical world (without privileging physical proximity to session host), especially important for demo sessions; side conversations during session are enabled in a largely nondisruptive way.

18:24:43 From pknowles : I'm going to the Beer Garden for one beer before I get some shut eye. If anyone wants to shoot the breeze

Day 3 Closing Selected Zoom Chat

16:42:52 From Richard Esplin : Sorry, thunderstorm and loud thunder here in Utah.

16:43:28 From Justin Richer : Better than the kids running and screaming at my house. And thunder is likely quieter. 🤷

17:10:12 From dsearls : 117 people in day 3 closing session may be a new record.

17:11:03 From Vic Cooper : We had a impromptu session where we are shared what is behind the virtual backgrounds with cameras and other video tech.

17:12:11 From Vic Cooper : Maybe next time we'll do a session on video tech?

17:12:23 From Sam Curren : A 101 Session!

17:12:30 From Juan Caballero : lol

17:12:31 From Sam Curren : but hold it 3 weeks before IIW so we can all up our game.

17:12:50 From pknowles : This IIW has been super fun. I've thoroughly enjoyed it. I really wasn't expecting it to hold up as a virtual event. 117 people in day 3 closing session. Truly sensational.

17:14:05 From Timothy Ruff : Agree with Paul. It really came together well and still generated great content and discussion.

17:14:55 From Vic Cooper : I like that we had all the different people attending from all over the world. +100 to the people who stayed up all night

17:39:34 From KathrynHarrison : Thanks everyone!! I have to run but this has been such a special experience. So glad to reconnect with so many people and look forward to touching base afterwards!

17:41:12 From David Huseby : this whole community will be so beautiful next time

17:43:43 From Nicky Hickman : Definitely appreciate the opportunity to join without knackering the planet with air travel

17:47:11 From Lisa LeVasseur : Thanks everyone! Maybe my favorite IIW to date. Dogs are giving me the stink eye...

17:47:42 From Drummond Reed : As I always say, this IIW was the best yet. Dunno how we can keep topping it, but we keep doing it. Congrats everyone!

17:48:28 From Marc Davis : Thank you! Virtual IIW was amazing and really worked!

17:48:51 From johnnyfromcanada : Thanks all! Great first time at IIW!

18:02:48 From Kazue Sako : Mostly I only participated opening and closing circles

18:03:24 From Drummond Reed : It was still great to have you at those

Stay Connected with the Community Over Time - Blog Posts from Community Members

As a follow up to the session 'Let's Bring Blogging Back' an IIW Blog aggregator has been created here: https://identosphere.net
If you want your blog to be included please email Kaliya: kaliya@identitywoman.net

A BlogPod was created at IIW - Link to IIW Slack –
https://iiw.slack.com/archives/C013KKU7ZA4
If you have trouble getting in email Kaliya@identitywoman.net with BlogPod in the Subject.

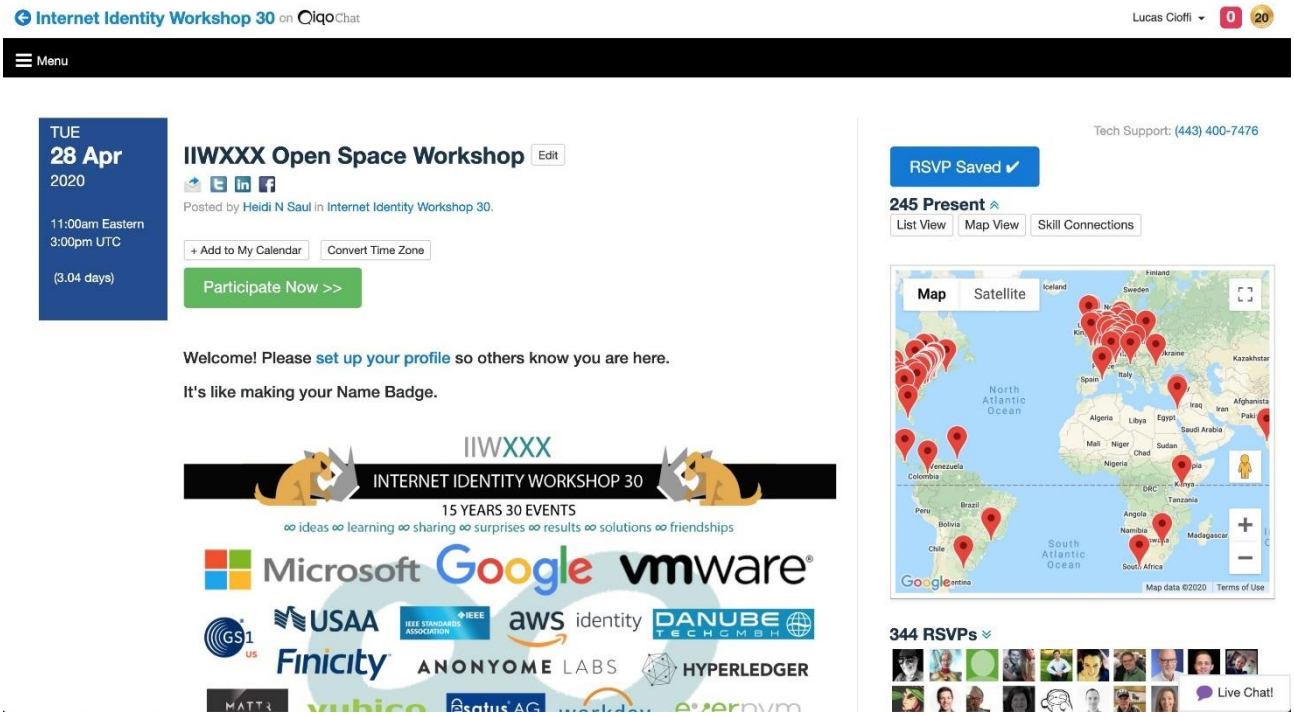
Planet Identity Revived ~ @identitywoman & @#InfoMiner cleared out & updated Planet Identity (see links below) you can support the work here:
https://www.patreon.com/user?u=35769676

IIW Community Personal Blog's shared via: https://identosphere.net/blogcatcher/
IIW Community dot.org's in the IIW Space: https://identosphere.net/blogcatcher/orgsfeed/

IIWXXX #30 Screen Shot Album by Doc Searls

Check out Doc's great variety of 'Screen Shots' from our first online IIW! @dsearls

https://www.flickr.com/photos/docsearls/albums/72157714514497786



See you October 20, 21 and 22, 2020

for

IIWXXXI

The 31st Internet Identity Workshop

REGISTER HERE

https://iiw31.eventbrite.com

www.InternetIdentityWorkshop.com