IIWXXXI

INTERNET IDENTITY WORKSHOP 31

OCTOBER 20-22, 2020

Book of Proceedings

www.internetidentityworkshop.com

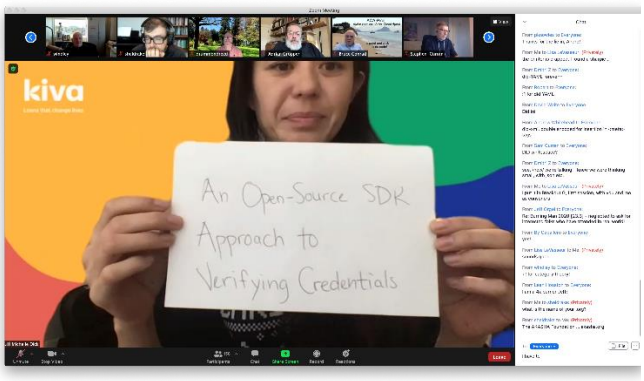
Collected & Compiled by
LISA R. HORWITCH and HEIDI N. SAUL

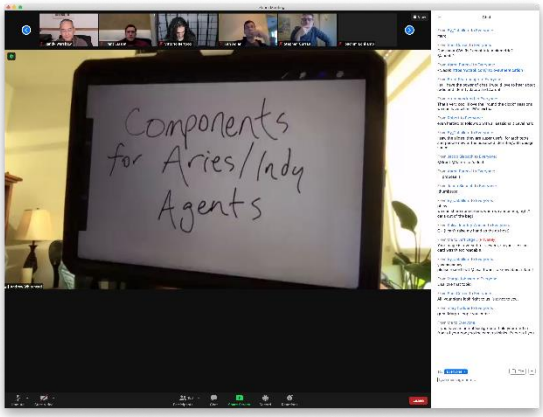
October 20, 21 & 22, 2020
On Line, Near You ~ via QiqoChat

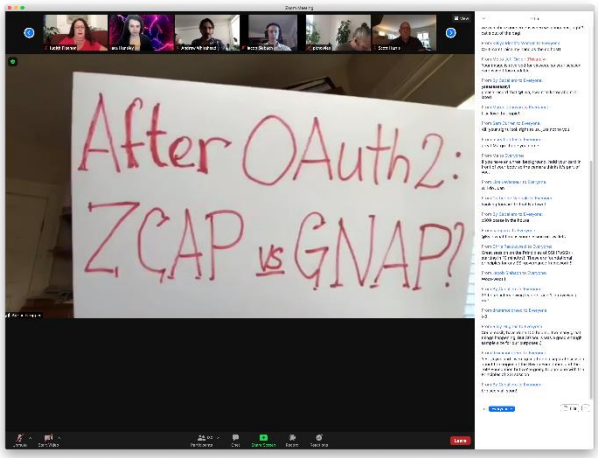
The Internet Identity Workshop Global Community

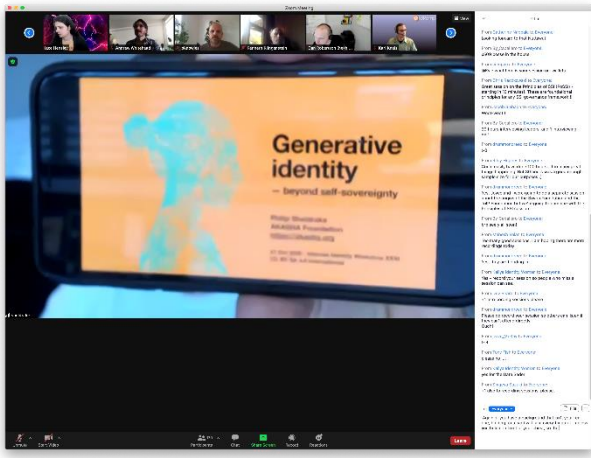
IIW founded by Kaliya Young, Phil Windley and Doc Searls
Co-produced by Heidi Nobantu Saul, Phil Windley and Kaliya Young
Facilitated by Heidi Nobantu Saul, Kaliya Young, Lisa R Horwitch

IIWXXXI Online
April 20 - 22, 2021









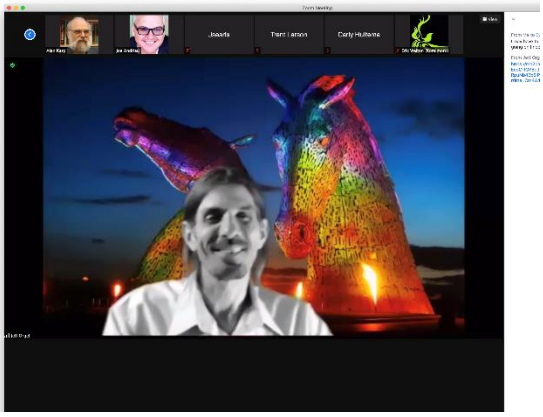
Contents

Thank You! Documentation Center & Book of Proceedings Sponsors JOLOCOM – IBO Institute – AyanWorks

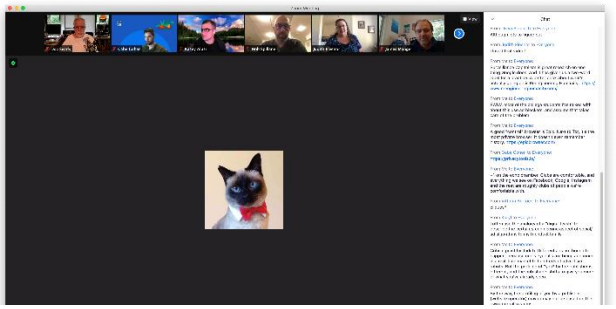
@GETJolocom **@ayanworkstech**

At IIW Online You Can….

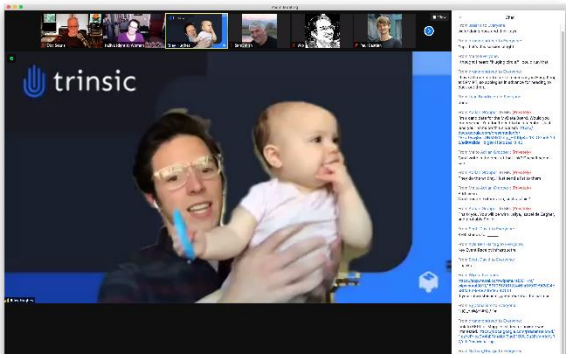
Though we lost some of our favorite parts of meeting together at the Computer History Museum there are many things you can do at an online IIW:



Choose Your Environment!

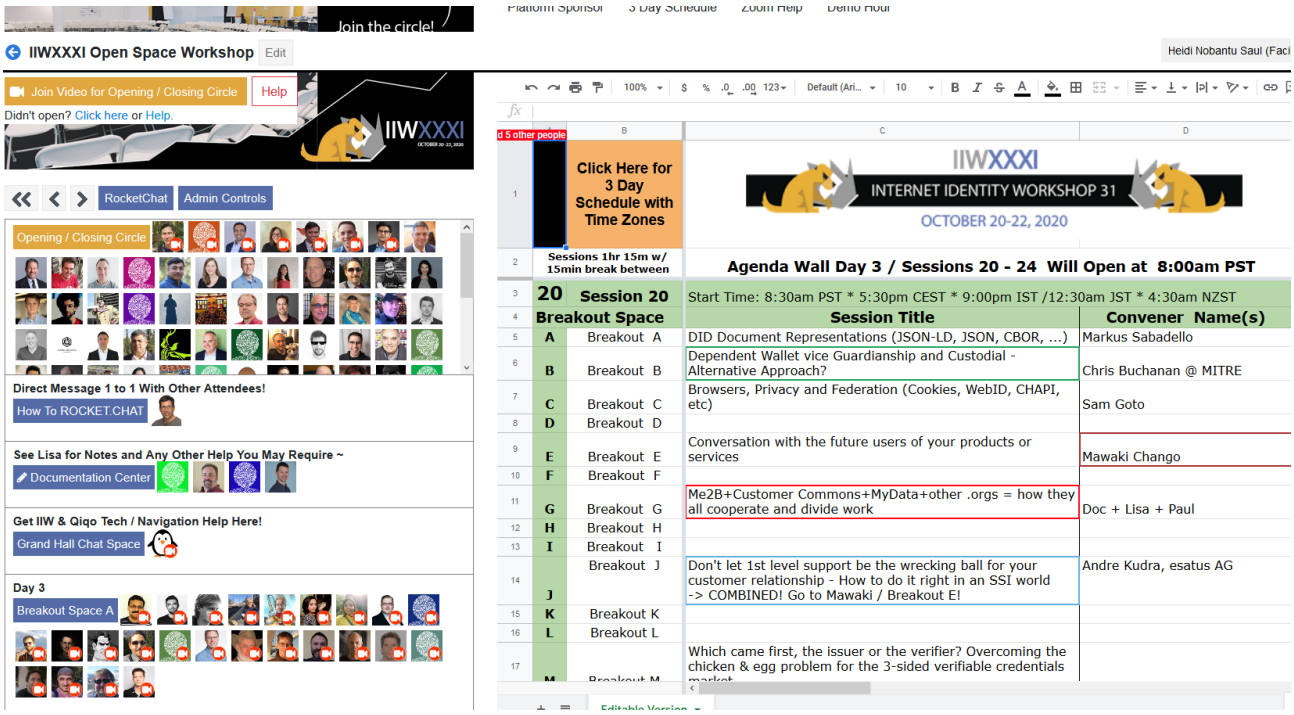


Attend as Your Cat



Show Off Your Beautiful Baby

Enhance and Disguise Your Appearance



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 (#33) will be April 20 - 22, 2021 online on the QiqoChat platform. Registration will open in mid-December 2020.

Thank You to our Sponsors!

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 Sponsorship information.

Upcoming IIW Events

IIWXXXI #32 Will be Online
April 20 - 22, 2021
MORE INFORMATION HERE

IIWXXXII #33
Fall 2021
Location TBA

IIWXXX 3 Day Global Schedule

OCTOBER 20-22, 2020

The IIWXXXI three-day schedule includes 24 Session time slots (with 15 breakout spaces for concurrently running sessions) spread over multiple time zones to encourage and accommodate regional and other time zone specific meetings/-sessions. Sessions are scheduled for 1 hour and 15 minutes, with a 15-minute break in-between each session. There are also Opening/Closing Circle start times (based on PST) and two Demo Hour's. There are no scheduled meal times. Below you can find the time that each session will begin in your part of the world.

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

Register here: https://iiw31.eventbrite.com

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 October 20 SESSIONS 1-5	GRAND OPENING Agenda Creation	PST	8:00 A.M - 9:30 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	AEDT	2:00	
		EST	11:00	IST	20:30	NZDT	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	AEDT	2:30	
		EST	12:30	IST	22:00	NZDT	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	AEDT	4:00	
		EST	14:00	IST	23:30	NZDT	6:00	
	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	AEDT	5:30	
		EST	15:30	IST	1:00	NZDT	7:30	
	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	AEDT	7:00	
		EST	17:00	IST	2:30	NZDT	9:00	
	DEMO HOUR Americas & Asia	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	AEDT	8:30	
		EST	18:30	IST	4:00	NZDT	10:30	
	CLOSING Open Gifting OPENING Agenda Creation	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	AEDT	10:00	
		EST	19:00	IST	5:30	NZDT	12:00	
	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	AEDT	11:30	
		EST	20:30	IST	7:00	NZDT	13:30	

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)
WEDNESDAY October 21 SESSIONS 6-15 DAY TWO	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	AEDT	19:00	
		EST	5:00	IST	15:30	NZDT	21:00	
	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	AEDT	20:30	
		EST	6:30	IST	17:00	NZDT	22:30	
	SESSION 8	PST	5:00 A.M - 6:15 A.M.	BST/WAT	13:00	ICT	19:00	
		MST	6:00	CEST/CAT	14:00	JST	21:00	
		CST	7:00	EEST/EAT	15:00	AEDT	22:00	
		EST	8:00	IST	18:30	NZDT	0:00	
	SESSION 9	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	AEDT	23:30	
		EST	9:30	IST	20:00	NZDT	1:30	
	OPENINIG *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	AEDT	2:00	
		EST	11:00	IST	21:30	NZDT	4:00	
	SESSION 10	PST	8:30 A.M.- 9:45 A.M.	BST/WAT	16:30	ICT	22:30	
		MST	9:30	CEST/CAT	17:30	JST	0:30	
		CST	10:30	EEST/EAT	18:30	AEST	2:30	
		EST	11:30	IST	22:00	NZST	4:30	
	DEMO HOUR *Europe & Americas*	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	AEDT	4:00	
		EST	13:00	IST	23:30	NZDT	6:00	
	SESSION 11	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	AEDT	5:00	
		EST	14:00	IST	0:30	NZDT	7:00	
	SESSION 12	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	AEDT	6:30	
		EST	15:30	IST	2:00	NZDT	8:30	
	SESSION 13	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	AEDT	8:00	
		EST	17:00	IST	3:30	NZDT	10:00	
	SESSION 14	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	AEDT	9:30	
		EST	18:30	IST	5:00	NZDT	11:30	
	CLOSING *Open Gifting* OPENING *Agenda Creation*	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	AEDT	11:00	
		EST	20:00	IST	6:30	NZDT	13:00	
	SESSION 15	PST	6:00 P.M. - 7:15 P.M.	BST/WAT	2:00	ICT	8:00	
		MST	19:00	CEST/CAT	3:00	JST	10:00	
		CST	20:00	EEST/EAT	4:00	AEDT	12:00	
		EST	21:00	IST	7:30	NZDT	14:00	

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)
THURSDAY October 22 SESSIONS 16-22	SESSION 16	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	AEDT	20:00	
		EST	5:00	IST	15:30	NZDT	22:00	
	SESSION 17	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	AEDT	21:30	
		EST	6:30	IST	17:00	NZDT	23:30	
	SESSION 18	PST	5:00 A.M - 6:15 A.M.	BST/WAT	13:00	ICT	19:00	
		MST	6:00	CEST/CAT	14:00	JST	21:00	
		CST	7:00	EEST/EAT	15:00	AEDT	23:00	
		EST	8:00	IST	18:30	NZDT	1:00	
	SESSION 19	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	AEDT	0:30	
		EST	9:30	IST	20:00	NZDT	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	AEDT	2:00	
		EST	11:00	IST	21:30	NZDT	4:00	
	SESSION 20	PST	8:30 A.M.- 9:45 A.M.	BST/WAT	16:30	ICT	22:30	
		MST	9:30	CEST/CAT	17:30	JST	0:30	
		CST	10:30	EEST/EAT	18:30	AEDT	2:30	
		EST	11:30	IST	22:00	NZDT	4:30	
	SESSION 21	PST	10:00 A.M. - 11:15 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	AEDT	4:00	
		EST	13:00	IST	23:30	NZDT	6:00	
	SESSION 22	PST	11:30 A.M. - 12:45 P.M.	BST/WAT	19:30	ICT	1:30	
		MST	12:30	CEST/CAT	20:30	JST	3:30	
		CST	13:30	EEST/EAT	21:30	AEDT	5:30	
		EST	14:30	IST	1:00	NZDT	7:30	
	SESSION 23	PST	1:00 P.M. - 2:15 P.M.	BST/WAT	21:00	ICT	3:00	
		MST	14:00	CEST/CAT	22:00	JST	5:00	
		CST	15:00	EEST/EAT	23:00	AEDT	7:00	
		EST	16:00	IST	2:30	NZDT	9:00	
	SESSION 24	PST	2:30 P.M. - 3:45 P.M.	BST/WAT	22:30	ICT	4:30	
		MST	15:30	CEST/CAT	23:30	JST	6:30	
		CST	16:30	EEST/EAT	0:30	AEDT	8:30	
		EST	17:30	IST	4:00	NZDT	10:30	
	CLOSING CIRCLE Open Gifting	PST	3:45 P.M. - 5:00 P.M.	BST/WAT	23:45	ICT	5:45	
		MST	16:45	CEST/CAT	0:45	JST	7:45	
		CST	17:45	EEST/EAT	1:45	AEDT	9:45	
		EST	18:45	IST	5:15	NZDT	11:45	

IIW 31 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 31 the prompt questions were focused on the following questions. When groups returned to the main room, they were asked to share what was discussed in the Zoom Chat.

- How are you & where are you?
- What's exciting and inspiring right now for you relative to your work in the industry?
    - If you are new and don't have an answer to that question:
        - what are you keen on learning about?
- What is worrying you?

08:30:02 From Charles Lehner : problem: "how to get money from verifier to issuer"

08:30:12 From George Fletcher : Lots of interest in IoT, blockchain, SSI/decentralized ID

08:30:13 From Bradley Hinson : COVID credential initiative and other COVID related SSI projects.

08:30:14 From By_ Caballero : @Michel was it Domi? ;)

08:30:17 From RAVIKANT AGRAWAL : exchanged thoughts about the difficulty with digital identity - such as education, customer experience

08:30:26 From Richard Astley : Talked about interoperability and difficulty with users managing their keys.

08:30:28 From Riley Hughes : Karyl from Transmute shared my sentiment - SSI adoption has really picked up this year!

08:30:35 From Brent Shambaugh : The Hufflepuff threw me in random rooms. Nice people.

08:30:38 From Aaron Parecki : sorry to miss you breakout room 20! My computer crashed when I tried to switch cameras

08:30:43 From Scott David : Folks are stoked!

08:30:46 From jonathan holt : Highlight: Regarding application of DID spec, we should eat our own dog food or perhaps more elegantly stated drink our own wine.

08:30:56 From Stephen Curran : What I learned about -- curated list of articles, etc. about identity: https://identosphere.net

08:31:00 From Scott David : Thank you Sponsors!!!!

08:31:10 From Dan Bachenheimer : Biometrics, although sensitive, are arguably the best way to tie a verified identity poof to the presenter of the proof

08:31:24 From Ed Eykholt : During the breakout session, we had an interesting conversation, mini-debate about the role of biometrics and SSI. Without them, do you trust the Holder = Subject?

08:31:25 From John Phillips : More hopes shared than worries, at least at our table

08:31:35 From George Fletcher : Some discussion around concerns in the dependence on libraries as security issues arise in those libraries can have a very large blast radius.

08:31:42 From Joachim Lohkamp : A few folks from our group shared the excitement of the German SDI projects where 11 consortia are funded by the German government to work on digital identity. Bundesdruckerei, Esatus and Jolocom are companies involved.

08:31:54 From Mahesh Balan : Concern in Group 29 was around distrust of governments, the move towards centralization of identity in many parts of the world

08:31:54 From timcappalli : +1 ^

08:31:57 From Denys Popov : +1

08:32:00 From Deepak Maram : +1

08:32:06 From Hunter Cain : How do you explain blockchain to the laymen for them to understand it and trust it?

08:32:38 From Steve Holyer : I heard the group "the difference between this conference and other online conferences seems to be based on a good invitation —— mmm … and then whoever comes is the right people 😀

08:32:45 From Mahesh Balan : One bright spot was Govt of Japan being very interested in SSI and starting to sponsor work on it group 29

08:33:32 From Kaliya Identity Woman : What happens when the UX is turned over to those who have control over it now on our phones like Apple.

08:33:42 From Nicky Hickman : thank you to sponsors

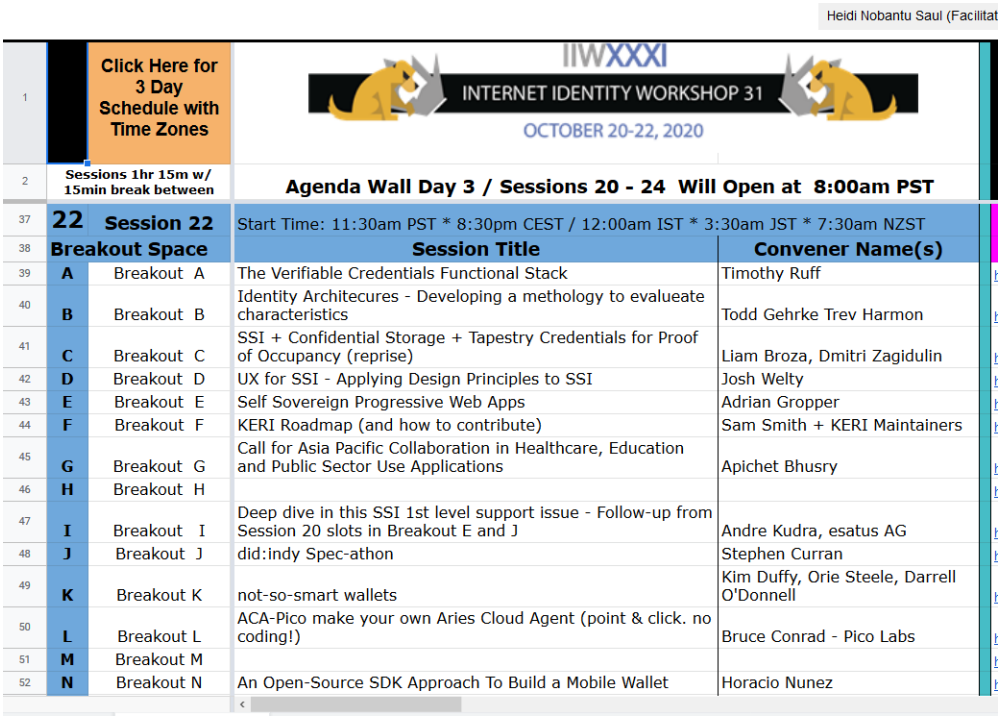
08:33:54 From By_ Caballero : INTROVERT SHELTER

08:33:59 From Bob Wyman : In our group, there was a concern for complexity, but: The complexity of a useful software system must equal or exceed the complexity of the system that it models.

08:34:41 From Marc Davis : In the Breakout Session, Johannes Sedlmeir made the excellent point that governments that support personal data rights and don’t resist individuals using end-to-end encryption technologies could be better venues for SSI adoption—for example, the EU with the GDPR, rather than the United States.

08:34:54 From George Fletcher : Excellent question @Kaliya

Session Topics / Agenda Creation



Heidi Nobantu Saul (Facilitat

1		Click Here for 3 Day Schedule with Time Zones	IIWXXXI INTERNET IDENTITY WORKSHOP 31 OCTOBER 20-22, 2020	
2	Sessions 1hr 15m w/ 15min break between		Agenda Wall Day 3 / Sessions 20 - 24 Will Open at 8:00am PST	
37	22	Session 22	Start Time: 11:30am PST * 8:30pm CEST / 12:00am IST * 3:30am JST * 7:30am NZST	
38	Breakout Space		Session Title	Convener Name(s)
39	A	Breakout A	The Verifiable Credentials Functional Stack	Timothy Ruff
40	B	Breakout B	Identity Architecures - Developing a methology to evalueate characteristics	Todd Gehrke Trev Harmon
41	C	Breakout C	SSI + Confidential Storage + Tapestry Credentials for Proof of Occupancy (reprise)	Liam Broza, Dmitri Zagidulin
42	D	Breakout D	UX for SSI - Applying Design Principles to SSI	Josh Welty
43	E	Breakout E	Self Sovereign Progressive Web Apps	Adrian Gropper
44	F	Breakout F	KERI Roadmap (and how to contribute)	Sam Smith + KERI Maintainers
45	G	Breakout G	Call for Asia Pacific Collaboration in Healthcare, Education and Public Sector Use Applications	Apichet Bhusry
46	H	Breakout H		
47	I	Breakout I	Deep dive in this SSI 1st level support issue - Follow-up from Session 20 slots in Breakout E and J	Andre Kudra, esatus AG
48	J	Breakout J	did:indy Spec-athon	Stephen Curran
49	K	Breakout K	not-so-smart wallets	Kim Duffy, Orie Steele, Darrell O'Donnell
50	L	Breakout L	ACA-Pico make your own Aries Cloud Agent (point & click. no coding!)	Bruce Conrad - Pico Labs
51	M	Breakout M		
52	N	Breakout N	An Open-Source SDK Approach To Build a Mobile Wallet	Horacio Nunez

142 distinct sessions were called and held over 3 Days.

We received notes, slide decks, and/or Zoom Chats for 129 of these sessions.

Tuesday October 20, 2020 ~ Day 1

Session 1
1A/ ToIP and Digital Trust Ecosystems
1B/ 101 Session OAuth2
1D/ Human-Centered Interoperability: Gold Button
1F/ OpenID Connect Credential Provider
1J/ DIDComm Messaging V2 - Where we are and what to expect
1M/ Toward a More Ethical Digital World: How to Think and Talk About Life in the Digital World

Session 2
2A/ Meet the NEW Sovrin Foundation
2B/ 101 Session OpenID Connect
2C/ Rebase: Decentralized Keybase
2D/ Regional Indy Networks - setting up, running, share experience
2E/ KERI for Muggles
2F/ The History of Cryptography
2G/ SSI + Confidential Storage + Tapesstry Credentials for Proof of Occupancy (Encore Wed)
2I/ Active & Passive Identifiers: Elements, objects and characteristics of a decentralized network
2J/ Rolling Back Surveillance Capitalism. Part 1: Describe the future (in detail)

Session 3
3A/ KERI for Mudbloods (Key Event Receipt Infrastructure) This is a more advanced session following KERI for Muggles in Session 2
3B/ 101 Session: UMA User Managed Access
3C/ Build an SSI Proof of Concept (30 minutes or less - code optional)
3D/ Bringing Emerging Privacy-Preserving Technology to a Public Health Crisis - A Case Study of the COVID-19 Credentials Initiative
3E/ Better DID Mehtods with Zero Knowledge Proofs (ZKPs)? - Privacy Preserving, Globally Verfiable DIDs
3F/ Exploring Governance Frameworks - Practical Approaches
3H/ Identity Index: A decentralized protocol for indexing and discovering and a DIDs resources
3J/ PBAC 101: Four Pilars of IAM, History of AuthZ, What IS PBAC
3M/ Cross-platform Rendering and Rich Selection of SSI Credentials

Session 4
4A/ The Past, Present, and Future of Indy Network Monitoring
4B/ 101 Session: SSI and Decentralized Identity
4D/ VC Revocations: On & Off Ledger
4F/ Moving Trusted Data across Untrusted Parties in Global Supply Chains
4G/ Chaining Verfiable Credentials - Completeness Proofs for history and event squences in VCs
4H/ A Regulatory Approach to Digital Identity (US) / A Jawful of the Lawful and the Awful
4J/ Privacy and Identity in mobile Driving License ecosystems

Closing Circle – Open Gifting & Opening for next 5 Sessions

Session 5
5A/ Explore Personal Data Collection - LifeScope Digital Memory (Encore Thurs)
5B/ Minimum Device - iOS, Android, and SIM Card Free participation in modern life
5C/ Intro to VR - How to get into IIW Doctown VR on Altspace
5D/ Enterprise Information System for Peer Production (EISPP) - Animations/Wireframes (2015-pre DID), payments, VRM, LinkedData…

Wednesday October 21, 2020 ~ Day 2

Session 6
6A/ SSI in Developing Countries: Product & Usability
6B/ Active & Passive Identifiers: Elements, objects and characteristics of a decentralized network (Repeat Session for EU/APAC Attendees)
6E/ Initial Trust
6J/ Rolling Back Surveillance Capitalism: Part 2 -- what are the Obstacles and what Assets can we use?

Session 7
7A/ Beyond Binary - How do we use the Web of Trust and move beyond the green checkbox?
Session 8
8A/ Trusted Digital Assistant - why I don't need to manage my identity
8O/ Brief Introduction to Picos

Session 9

9A/ Birth Attestation = Initial Guardianship
9E/ Secure Scuttlebutt: Peer-to-Peer Social Network
Closing for 5 Sessions that were held & Opening / Agenda Creation for Upcoming Sessions

Session 10
10A/ The Principles of SSI
10C/ Bypassing eSignature Regulations for SSI Adoption
10D/ PBAC 102: Architecting Authorization to Protect Your Data
10E/ Initial Trust in SSI Triangle - Analysing Trust Relationship, Existing and New Mechanisms
10F/ Ideas to Action: BYOB (Bring Your Own Blockers)
10G/ KERI for Wizards
10O/ GS1 Digital Links, DIDs, and VCs…issuing from HTTPS

Session 11
11A/ Service Delivery & Ecosystem Management with Verifiable Credentials (VC).
11C/ Unified Front for SSI/DI Messaging
11D/ After OAuth2: ZCAP or GNAP?
11E/ Components for Aries/Indy Agents
11F/ Dealing with Import/Export Wallets: What About Malicious Wallets?
11G/ Generative Identity - for psychological sociological, and ecological health (aka: the dystopia of SSI)
11H/ Universal Declaration of Digital Identity
11K/ Overlays Capture Architecture (OCA): Global Semantic Harmonzation
11L/ The Thoughtful Biometrics (un)Conference coming in January - Sharing Ideas
11M/ AUTHtung! Can digital identity resist authoritarianism?

Session 12
12A/ KERIfying DID Methods & KERI for Interop
12B/ Current & Future Adoption of Verfiable Credentials - How we get from new tech to ubiquitous adoption.
12C/ SSI and IoT
12D/ Does SSI require DIDs?
12E/ Extending the DID doc with IDX: A better way to manage service endpoints?
12F/ Custodial/Guardianship Agencies - hosting agents on behalf of agentless users
12I/ A Legal Layer for the Internet & IEEE 7012 Machine Readable personal privacy terms
12J/ Rolling Back Surveillance Capitalism: Part 2: What are the Obstacles and what Assets can be use?
12L/ JSON-LD BBS Signatures 101* plus status updates
12O/ Sidetree Updates and did:elem Progress

Session 13
13A/ Defending the Human OS: Augmention vs Displacement
13B/ CanDID**:** Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability
13C/ Survey of Aries Frameworks PLUS announcing two new mobile native Frameworks
13D/ An SDK approach for Issuing Credentials
13E/ DIDn't: did:un and overlap between DIDs & KERI
13F/ DIF: Presentation Exchange, progress updates!
13G/ The Rising Tide of Deanonymization - The consequences to Self-Sovereign Identities in the context of organizing the world's information and making it universally accessible and useful.
13H/ ToIP Interoperability Profiles (TIPs)
13I/ Decentralized Identity Based Communications - Getting Rid of Phone Numbers

13J/ The Web Platform, Privacy and Federation (thoughts on WebID)
13K/ Online JWT Interactions (QR Codes/Buttons For Claiming and Sharing VCs)
13L/ Notice and Consent Comes of Age
13N/ SSI for COVID-19 -> Compared to the altenratives which we want to articulate)

Session 14
14A/ Verifiable Trust Bases: How to make the web of trust new again with KERI
14B/ SIOP - progress on the laundry list (wrt DID)
14C/ Guardianship, SSI, and the Sovrin Working Group
14D/ Fusion: Leveraging Federated Identity to Scale Verified Credentials
14E/ Interop between SSI stacks - A proposed handshake protocol
14G/ Amateur Radio and Identity
14H/ The Sovrin Technical Ecosystem
14I/ Is identity only transactional?
14J/ Data Seder: A dinner ritual for our generations

Closing Circle – Open Gifting & Opening for next 5 Sessions

Session 15
15A/ did:web 201 - Risks and Mitigation

Wednesday October 22, 2020 - Day 3

Session 16
16A/ Overlays Capture Architecture (OCA): Global semantic harmonization (Repeat session for EU/APAC attendees)

Session 17
17B/ Deep Fakes, Rival Goods and Verifiable Goods

Session 18
18L/ Brief intro to ACA-Pico (starting at 6:00am PST)
Session 19
19A/ 7 Essential Life Credentials for Identity for All
19B/ Identity and VR - Will meet in both Zoom and present in Altspace - send your Altspace ID to Vic to get in to the event. Link to Altspace event
https://account.altvr.com/events/1587179898034717357

Closing for 5 Sessions that were held & Opening / Agenda Creation for Upcoming Sessions

Session 20
20A/ DID Document Representations (JSON-LD, JSON, CBOR, ...)
20B/ Dependent Wallet vice Guardianship and Custodial - Alternative Approach?
20C/ Browsers, Privacy and Federation (Cookies, WebID, CHAPI, etc)
20E/ Conversation with the future users of your products or services (Combined with Don't Let 1st level support be the wrecking ball for your customer relationship - How to do it right in an SSI World.
20G/ Me2B+Customer Commons+MyData+other .orgs = how they all cooperate and divide work
20M/ Which came first, the issuer or the verifier? Overcoming the chicken & egg problem for the 3-sided verifiable credentials market

Session 21
21A/ The Real-World Benefits of KERI (muggle-friendly, really!)
21B/ Policy-based Authorization: The Abacus
21D/ DIDComm Mediator Agents (v1 & v2) - Intro and where open source projects are.
21F/ Biometrics and Identity: A preview of the future
21G/ Mobile App Impersonation Attacks & Mediations
21J/ Ideas to Action: Putting Decentralized Identity to Work (Alternate title - Get Over It: What are your barriers to adoption?)
21L/ Secure Data Store Working Group
21M/ EISPP/VRM, Interop., RDF, Category Theory, data migration

Session 22
22A/ The Verifiable Credentials Functional Stack
22B/ Identity Architecures - Developing a methology to evalueate characteristics
22C/ SSI + Confidential Storage + Tapestry Credentials for Proof of Occupancy (reprise)
22D/ UX for SSI - Applying Design Principles to SSI
22E/ Self Sovereign Progressive Web Apps
22F/ KERI Roadmap (and how to contribute)
22G/ Call for Asia Pacific Collaboration in Healthcare, Education and Public Sector Use Applications
22I/ Deep dive in this SSI 1st level support issue - Follow-up from Session 20 slots in Breakout E and J
22J/ did:indy Spec-athon
22K/ not-so-smart wallets
22L/ ACA-Pico make your own Aries Cloud Agent (point & click. no coding!)
22N/ An Open-Source SDK Approach To Build a Mobile Wallet

Session 23
23B/ Burning Man 2020 - When Private Behavior Goes Quite Public
23E/ SSI, Privacy and and the disinformation ecosystem
23F/ Explore Personal Data Collection - LifeScope Digital Memory
23G/ Discovery: Solving the Kobayashi Maru of SSI
23H/ Interoperability Working Group
23I/ Asset ownership transfer using Verifable Credentials
23K/ Paper: Your best friend for SSI adoption
23M/ An Open-Source SDK Approach To Build a Mobile Wallet

Session 24
24A/ Realizations about Diversity, Inclusion, and Our Industry
24B/ Contributing to Hyperledger Identity projects: How to engage and what is missing?
24C/ I like personalized ads: a discussion on how to convince laypeople to care about privacy
24D/ Verifiable Photo and attachments in Aries .. How we approached it
24E/ did:web 201 - Risks & Mitigation
24G/ What are Our Questions?
24H/ Credentials, Connections, and Conversations
24K/ Dynamic Data Economy:The big mountain behind SSI hill
24M/ An Open-Source SDK Approach To Build a Mobile Wallet

Closing Circle – Open Gifting

Notes Day 1 Tuesday October 20 / Sessions 1 - 5

ToIP and Digital Trust Ecosystems

Tuesday 1A
Convener: John Jordan, Dave Luchuck, Karl Kneis
Notes-taker: Sankarshan

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

- Link to Trust over IP whitepaper: https://trustoverip.org/wp-content/uploads/sites/98/2020/05/toip_introduction_050520.pdf
- [Karl] Welcome notes - to share the Trust over IP Foundation story. Introductions for John Jordan, ED of ToIP
- [John Jordan] Note of thanks for the organizers of IIW31. ToIP was launched a week after the IIW30 and started out with 27 member organizations. Growth to 160+ members - working and collaborating for interoperable digital trust. It has been a busy 6 months for the ToIP Foundation (a JDF under The Linux Foundation). We have 6 Working Groups - the engine of the Foundation. The examples we'll discuss are not hypothetical - these originate from members of the ToIP working on using VCs based on open standards and implementing in their ecosystem "The Trust Triangle". The credentials have to work inside their own trust domains and across trust domains - how can a group of organizations make use of credentials originating from another domain. Our goal is making people's lives easier and more secure. We want people to be able to use the internet to do business and in their personal lives and feel confident in doing so - without fear and impediments.
    - John shares anecdotes from his interactions with the nursing staff.
- [David Luchuk] Introduction - focus of his roles. Introducing the "dual stack" at ToIP
    - The stack provides us with a model for ecosystems of credentials to emerge.
- [Karl] The Ecosystem Foundry Working Group has attracted many businesses across industries seeking to get together to focus on interoperability and success in real life use cases.
    - Introduction to the members from the EFWG
        - [Gena Morgan / GS1] - currently identifying a few use cases for PoC efforts. Looking for feedback on these use cases from experts in SSI, DIDs and VCs
            - [John Court] So currently I assume there is no protection around proving who minted an RFID ?
                - [Timothy Ruff] FYI KERI addresses proving who minted an ID. Curious if GS1 is looking into KERI?
        - [Charles Walton / Mastercard] https://idservice.com/ - identity inclusion was quite causal to the lack of financial inclusion. Digital payments are led by identity - ID and authentication are core topics to types of payments. Identity is pivotal. Mastercard is a platform for the bank partners - the digital identity service being rolled out works cross borders. Placing the individual at the center of the digital interaction - privacy is preserved. Transparency and multi-market interplay is important and a key aspect. Design principles, identity-tech standards, standards around vertical market and representation of claims (types of claims and how they appear during data exchanges). The vision of ToIP as a multi-layer model is key to the outcomes being worked on and the group of individuals/companies motivated to join. There is still a lot of work to do. Collaboration is they key to be able to address the

challenges and problems to be able to make the data exchanges required for payment systems.

- [Jim St.Clair / Lumedic] Lumedic is a member of the Steering Committee at ToIP. Patient identity has unique challenges - the issue of patient identification - correlating to the right individual is what is the current focus. It does not inherently do not align to or support SSI or decentralization of identity. This brings about marketability of healthcare data. How do we build in mechanisms to preserve privacy while being able to healthcare engagements in a frictionless environment. The work on the ToIP stack contributes to making this outcome possible.
    - [Drummond] With ToIP stack having both governance and technology, how is governance being used?
        - [Jim] Lumedic is providing the technical underpinning, business framework and policies, rules for the exchange members when sharing and exchanging credentials.
- [Drummond Reed (standing in)/ GLEIF] GLEIF is a governance authority and issues an identifier LEI - classic federated identifier. GLEIF would be creating a digital trust ecosystem through LEIs. LEI holder can also issue VCs to organizations and things. Not limited to people. GLEIF is a founding member of ToIP
    - [Timothy Ruff] GLEIF was formed post financial collapse. The G20 authorised the identity to issue LEI to every financial institution on earth eg. BoA has a single identifier of all entities across the world. This solves the problem of regulators and compliance entities could assess how extended banks were. Outside of ICANN this is the only other identity to issue globally unique identifier.
- [Ajay / Stanford University] (presentation) How might we return to campus safely? Every informed decision must rest on a foundation of trust? ToIP based interoperable framework between test labs, doctors/hospitals and the community of students and staff. 'Protected Entry Use Case' - for access to public areas and requires proofs that they were recently tested -vely along with other specific proofs around being a student and so forth.
    - [Charlie] have you (or anyone in the community) defined what a CV19 health status, or a CV19 vaccine claim looks like within a W3C VC? This is an important interoperability topic for the industry (travel, health, government) to work through. I would be quite interested to understand if there are answers, thoughts, details, something/somewhere in Github or elsewhere address this detail. I am reachable at charles.walton@mastercard.com if anyone is aware of an answer for the industry.
        - [Daniel Hardman] Orie Steele did some great work to define a schema for COVID credentials, and I believe his proposal was checked into a W3C repo. I don't have the link to his schema at hand, but you could ask him for it.
        - [Margo Johnson] I believe is the previously mentioned repo re: COVID credentials: https://github.com/w3c-ccg/vc-examples/tree/master/docs/covid-19
    - [Jeff Kennedy] If this is done on a phone, how do you assert that the holder of the phone is the person they claim to be?
        - [Daniel Hardman] binding a holder to a credential can be done in various ways, depending on the level of assurance you need.

Biometrics is one of the strongest ways. Hyperledger Aries is about to have two RFC proposals about biometric binding to credentials; see https://github.com/dhh1128/aries-rfcs/blob/bsp/features/0529-biometric-verification-protocol/README.md

    - [Dan Bachenheimer] How do we know that the presenter is that person?
- [John] Horizontal ecosystems. A call out for the Human Experience WG at the ToIP. Would like to see ToIP find a way to bring in some of the voices who are at this moment not being included.

OAuth 101 - An Introduction

Tuesday 1B
Convener: Aaron Parecki
Notes-taker(s):

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

Slides provided/presented by Aaron Parecki: https://speakerdeck.com/aaronpk/oauth-101-internet-identity-workshop-xxxi

Human Centered Interoperability

Tuesday 1D
Convener: Chris Lee & Adrian Gropper
Notes-taker(s):
Tags for the session - technology discussed/ideas considered:
#HumanCentredDesign

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

Showed video of Golden Button
https://www.dropbox.com/sh/bs876wqqdzkclxm/AABp_SYpZAhFqG2gdtWlsDSba?dl=0

Based on an agent rather than wallet model:

- Discovery includes context, applies intelligence to evaluate policies and make risk-based decision on trust

Exception management?

1. Exception when policies don't match results in text message from Agent
2. Where the relying party doesn't want to honour the token e.g. for compliance reasons.

Session tomorrow on authorisation - technical session GNAP, UMA, ZCAPS. OAuth2 is a problem meaning that UMA is superseded. GNAP is a successor to OAuth 2 and OpenID Connect.

- Looking for the minimum bundle of standards that are good for a transport badge.

Privacy preserving - Zena principle, from anonymous to pseudonymous to legal identification, which can be pulled back.

Use of Notary (keeps a log of transactions in the wallet which enable emergency audit) in case of need.

Not just policies that you inherit but also information fiduciaries who help your agent form policies for you.

OpenID Credential Provider

Tuesday 1F
Convener: Tobias Looker
Notes-taker(s): Lionello Lunesu
Tags for the session - technology discussed/ideas considered:

OpenID Connect, Credential
https://mattrglobal.github.io/oidc-client-bound-assertions-spec/

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

- Extension to the OpenID Connect Core spec
- New scope: “openid_credential”
- Adds “sub_jwk” and/or “did” to request object = used to sign the request object and the public key to be used for the response
- Adds “credential” to the request object “claims” (in addition to “userinfo” and “id_token”)
- Discussions around having both/either “sub_jwk” vs “did”
- Using the “did” as the “kid” inside “sub_jwk”?
- New OpenID Discovery fields: “dids_supported”, “did_methods_supported”, “credential_supported”, “credential_format_supported”
- Question around necessity of having new scope, new “credential” response

Zoom chat:
From Lio Lunesu : OK if I take some notes in the google form?
From Wayne Chang : No apologies necessary, I prefer ascii art!!
From Orie Steele : Can we get w3cvc-jsonld -> w3c-vc-jsonld :)
From Dmitri Zagidulin : and waste an extra character??
From Dmitri Zagidulin : think of the bandwidth and/or the children!
From Nat Sakimura : It could be ephemeral as well.
From Wayne Chang : imo, it’s a different trust model between just using the included key vs. DID resolution
From Wayne Chang : specifically if you rely on sub_jwk then you are trusting the direct presenter, whilst with the DID you are trusting the DID method’s resolution process
From Dmitri Zagidulin : for an introduction to dpop - https://link.medium.com/B1c7jI94Jab

From Oliver Terbu : Well, you have to trust the authentication step in OIDC. I assume this can be anything from social login to a national eID scheme.
From Dmitri Zagidulin : tobias - this vc request spec syntax is fabulous. I'd love to unify/integrate it with the CCG vp-request-spec
From Oliver Terbu : The provider knows the user and issues a VC to the wallet
From Wayne Chang : https://openid.net/wg/ekyc-ida/
From Sascha Preibisch : I do not see a hands-up icon
From David Waite : in the participants list
From Wayne Chang : @sasha, you may need to open the participants list
From Xavier Vila : Click on participants button, From Wayne Chang : hah From Sascha Preibisch : thanks
From Wayne Chang : https://xkcd.com/927/ <- glad we're moving to prevent this
From Nat Sakimura : FYI: eKYC/IDA WG product that Wayne mentioned: https://bitbucket.org/openid/ekyc-ida/src/master/openid-connect-4-identity-assurance.md
From Orie Steele : Massive ID tokens
From Orie Steele : Nested base64url is one of my least favorite things From Lio Lunesu : :D
From Nat Sakimura : What Lio talked about is called distributed claims. From Lio Lunesu : correct
From Nat Sakimura : It is like "claims by reference". It is got many nice characteristics if you are not concerned about the RP anonymity towards the CP.
From Vittorio Bertocci : it seems what yu want is response_type; scope isn't really the right place
From Sascha Preibisch : That comes close, yes
From Wayne Chang : +1 to embedding things as a workable path
From Orie Steele : I think its more likely That DIF PE would offer this as a channel
From Wayne Chang : Just need to be super explicit about the layers of trust here and how they're transversed by different pieces
From Vittorio Bertocci : did I read "auth0" in the URL? :) From Oliver Terbu : haha From Orie Steele : yep
From Nat Sakimura : bit.ly/3jhuRF6
From Orie Steele : userinfo seems like maybe a better place
From Orie Steele : But then the id_token still needs to be updated in some way I think.
From Wayne Chang : Without getting too ahead of ourselves, I feel that a keycloak module would be a powerful demonstration for this
From Lio Lunesu : Please, folks, check and add to the notes
From Orie Steele : "Use the protocol features, don't overload unless you are forced to"
From Lio Lunesu : The notes I took might be biased to things I noted
From Dmitri Zagidulin : @Lio - do you have a link to the notes?
From Lio Lunesu : It's in the qiqo, click on Session 1F On top From Dmitri Zagidulin : thx
From Oliver Terbu : OIDC CP = issuance flow
From Alec Laws : Thanks! Very interesting
From Richard Astley : Thanks Tobias, great session.
From Thomas (Evidence) : Thanks ! Was very nice !
From Wayne Chang : tyty; Great stuff

DIDComm Messaging V2 - Where We Are and What toEexpect

Tuesday 1J
Convener: Sam Curren
Notes-taker(s): Gabe Cohen

Tags for the session - technology discussed/ideas considered:

#DIF #DIDComm

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

https://docs.google.com/presentation/u/1/d/1YiL-A9YaNgQpFBraJJOLLUPyFfZ6uQ1uqtTCiDZxNqI/edit?usp=sharing

Link to repository to file issues: github.com/decentralized-identity/didcomm-messaging/
Session will be recorded.

Sam:

- Message-based communication; trust in DIDs
- Originated in 2019, now headed toward complete draft
- V1 originated in Aries, V2 being discussed in DIF/now
- DIDComm sits between Protocols (above) and DIDs & DID Docs (below)
- DIDComm depends on DIDs & DID Docs

Johannes Ernst: What prompted V2?

Sam: People liked V1, but there were improvements to be made. Moved to DIF. Due to being Non-indy communication.

Johannes: As much organizational issue as technical.

Sam:

- Related work: JWM, ECDH-1PU in IETF
- more standards based and similar to DIDComm
- DIDComm benefits:
    - Security independent of transport
    - Foundational layer of interop
    - Repudiable by default - non-repudiation support
    - Fills gap b/w DIDs and protocols
    - Protocol development becomes easier + more robust
- Goal is to provide more efforts on evangelism (how to use it + what it is)
- DIDComm Transports -- agnostic
    - Http(s), websockets, bluetooth sockets, qr encoded msgs, etc

Michael Schafer: NFC?
Sam: Yes, discussed, but no formalization yet.

- Current work:
    - Spec flow, completeness, examples, guide expansion
- What's new in V2?
    - Adjustments for Standards Track Deps
        - JWM & ECDH-1PU for authcrypt
    - 0-RTT instead of DID Exchange
        - Includes more keys in original message – reduce noise
        - If you want to rotate, you can do it along w/ flow of messages. Don't need to pause. DIDComm allows agents to be offline (cell-phone died, bad service)
        - Important to be as efficient as possible
        - Can send several messages if you know someone's DID

Johannes: Comparison to email?

Sam: Yes, intended to work similarly. Extensions to DIDComm spec that allows "last-mile" messages to be sent. Can be compliant while having queue methods work differently. Allow msg to be routed in a standard way. Moving to 0-RTT makes this much more efficient. Supports rltns of any length.

    - JWM Headers vs decorators
        - V1 had decorators about the message itself. Moved into JWM headers.
    - Return-route as an Extension
        - Allows a standard way of queuing. Extension in V2 makes it easier to be compliant with the protocol.
    - Authcrypt Only - No Anoncrypt directly, use Peer DID for better effect
        - Authcrypt (authenticated encryption), anoncrypt (different way for key to be communicated). For simplicity: no anoncrypt directly.
        - Peer DIDs provide value that anoncrypt did. Peer DIDs: DID can be created + communicated with another party without being recorded on a ledger. Efficient and desirable privacy aspects.
    - Impl Guide
        - Now exists!

Hob: Where's the impl guide?
Sam: I'll share

Bengo: Can you elaborate on protocols you're excited to enable?

Sam: Focus on credentials. Excellent use. More excited about other protocols that facilitate interactions we have now. Ex. DIDComm relation we have with a website. Facilitate payment. Protocols that are powerful for business, but privacy respecting. Don't want spam, but capability to have new conversations that one is in control of as a user.

Location sharing. Location sharing apps on phones are controlled by a central server (run by Apple or Google). Permissioned location sharing is useful. Where's my wife???

Dave Huseby: JWM for messaging...does that mean we're only talking about ??? transport protocol.

Sam: REST is not a term we use.

Dave: HTTP?

Sam: Doesn't have to be HTTP. Websockets used in V2. Scanning QR codes, bluetooth, NFC popular for mobile uses.

Dave: JWM over arbitrary transports??
Sam: Yes!

Daniel Hardman: Implemented one over SMTP. Sockets, etc.

Dave: Encoded as text, using JWM?
Sam: Yes.

Kyle: Allowing for extension points in the future to improve. WG is not addressing all right now. Currently a PR.

Sam: Not trying to solve CBOR/other binary encodings right now.

Matthew Hailstone: How does it interact with other DID protocol stacks? What are the requirements?
Sam: Indy/Anoncreds will be quite receptive. It is a nice companion to things like DIF Credential Manifest/Pres Exchange. Can work well over DIDComm. No limit to the type of info that can be passed across DIDComm messaging. But not really trying to solve real-time-comms stuff.

Matthew: If I have a credential issued by a Sovrin protocol, how can I exchange the data back and forth? Is that something not targeted?

Sam: DIDComm doesn't specify how creds are passed, but instead how such a protocol would be created. Existed in V1...yet to be done in V2. I hope you can use a well-supported protocol over DIDComm.

Bengo: DIDComm depends on a transport layer. What properties are required? Can it work on top of UDP or snail-mail?

Sam: Yes. Can be transported on anything, doesn't have to support encryption. Some are more common: HTTP & Websockets. Lots of common use-cases on other transports.

DH: Other than HTTP & sockets, the filesystem is important. Has to be possible for one to save a DIDComm message on thumb-drive, stick it on a network file system somewhere. Has to be an option. Few demands on the transport layer.

Why isn't it binary -- messages passed in DIDComm messaging is structured info that describes stuff. Nothing that prohibits moving binary data over DIDComm. A cred is binary. CBOR based creds over DIDComm -- knock yourself out. Problems would arise on a transport (e.g. 10GB over HTTP Post). DIDComm itself is un-opinionated.

Bengo: What would we be using HTTP/Websockets for if we had TCP+DIDComm 25 yrs ago?

Sam: No core ID layer on the internet. We don't do mutual authN with HTTP. Possible to launch a video chat session coordinated w/DIDComm. Better foundation of trust for the resulting connection. Lots of current ID problems would go away. Would the "you are who you say you are" be different?

Places where DIDComm is not the right answer. But a good cousin/tool to travel alongside other things. Push notifications -- relationship with a bank, instead of SMS (security problems), a notification could arrive over DIDComm. A richer, more secure protocol.

Not betting on a single transport. Betting on a wide variety of interesting things being built on DIDComm as a platform.

Bengo: what would you like to see building that depends on the work you're doing?

Sam: a number of these technologies. Involvement of DIDComm with a relationship w/ a website. DIDComm instead of username/pw. Longer-term DIDComm relationships. More mobile apps -- efforts underway. Make it easier for devs to do the right thing in terms of privacy.

I'd still use an email+pw for login (not social login!), but it's universal & people get it. Need to change that. Get traction into systems people already use.

DH: Mesh networking if I had infinite time. DIDComm allows that HTTP does not: chatting with everyone around you at a sporting event. Reaching out to other devices in a connected mesh + talking to them. The future! No more HTTP calls back to some backend. More point-to-point comms. Still sci-fi.

Also digital cash. Not bitcoin. Transacting w/o internet -- phone to phone.

Sam: ultra-wide-band stuff. Location sharing, people in backcountry without a satellite.

Kyle: Automated scheduler using agents. Pass an .ics to someone, they pass one back, find a time to meet. Something similar to SSB -- a way to pass GIT files.
Authentication would be great.

Bengo: what would a traditional http server look like?

Kyle: lightweight wallet into an express server or something. Use it as ID management. Pass DIDComm messages over the webpage.

Bengo: I will reach out to Sam + co.

Sam: Can go straight to authZ in some cases without authN. Cool from a privacy perspective. Can skip the "who are you step." Progress to be made in the next 6 mo.

Matthew H: curious about QR code cases. QR codes for ticketing systems for events. Would it be a DID connection, or embed a credential in the QR code?

Sam: Initial use-case in spec has to do with passing invitation/initiation with another party. Designed to be scanned by a phone. Session tomorrow around custodial agents: interact in an SSI model without involving a device (by choice or limitation). Spec so far talking about QR code as an easy way to pass things between screen + camera. Facilitate the transfer of a cred.

Johannes E.: Do another session on the level of the actual code. I'd love to, in my terminal, send something and see it arrive at another participant.

Sam: Next IIW! Have code for v1, need more time for code examples for v2.

Johannes: Can be a foundational piece for a lot of things that are broken today on the internet. Email is broken. I encourage going to hands on.

Sam: Hasn't happened yet, moving a lot. Moving less. Next couple of months there will be code examples + products (maybe).

Geovane Fedrecheski: Routing. With DIDcomm we have E2E encrypted channels. Is routing needed because we have NAT which prevents E2E channels? What is the role of routing in a home? How does it work?

Sam: NAT traversal, routing can help. Can send a message through an intermediary. Beyond network traversal issues, routing is useful for herd privacy. Cannot inspect the contents of a message, but can see it from A->B, I can do size inspection, etc. If passed through the routing protocol, your message is blended with many other messages. Much harder to determine what's going on.

The routing protocol is simple but provides a wide variety.

Geovane: Is the routing protocol optional?

Sam: Mandatory to compose and send messages that respect the routing config of the receiving party. Up to the receiving party.

Micha Kraus: Q on Key rotation? How is it handled in V2? Difference b/w peer and ledger DIDs.

Sam: Key rotation is the problem of the DID. Done in the DID Doc it's associated with. DID info can be provided in to/from fields in messages.

DID Rotation allows a party to change from one DID to another. A way to prove the rotation is authorized to happen.

Kyle: Question Ajay asked on how to migrate from V1 to V2?

We haven't actually discussed this. We need to figure this out as we build impls. Going to be building an open source impl.

Migrating relies on the DID-layer. The serviceEndpoint itself is passed, and use that separation to handle it. Some edge cases.

Sam: We will have a section in the impl guide that addresses converting from V1 to V2. (identity.foundation/didcomm-messaging/guide/). Will be relatively straightforward.

Links on last slide.
Timeline: what's next and moving forward. Depends on community effort. Pretty darn close to "final" before next IIW. Won't be things moving around as much. Ongoing work will be guide expansion & reference functional code.

#wg-didcomm on DIF slack.

Andrew Whitehead: Routing protocol - what about re-encoding? Increasing the size of the payload?

Sam: Discussed, but not solved yet. When forwarding, contents are encrypted, 3-4 byte b64 encoding, there ends up being a ~30% increase in size of the message. Have ideas on how to solve, but not yet.

Kyle: Routing is likely to change the most. Expect to see a lot of innovation. Expect things to merge over time.

Sam: DIF WG will work on it until we decide where it will go. Not quite there yet. Will end up in the right place, unsure where yet. As it reaches stability here. No hindrances to building right away.

Toward a More Ethical Digital World: How to Think & Talk about Life in the Digital World

Tuesday 1M
Convener: Lisa LeVasseur
Notes-taker(s): Lisa LeVasseur
Tags for the session - technology discussed/ideas considered:

#Me2B #Me2P #Me2T #Me2B #Commitment

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

Me2B as an ethos: Healthy, balanced Me2B Relationships are better for both Me-s and B-s.
Me2B reflects human rights + consumer rights.
Me2B is deliberately more on the side of the individual because of the current asymmetry in the relationship.

Not just about "Me-s"; reflects and respects truth of interrelatedness and interdependency; Me-s and B-s exist in social web/fabric, not in isolation.

The Me2B Commitment isn't binary; there are shades of "grey" in the Me2B Relationship; both in the physical world and the digital world.

Revised the deck to incorporate the different kinds of Me2B commitments. Deck will be here soon: www.me2ba.org/resources
https://me2ba.org/wp-content/uploads/2020/10/me2b-101-for-iiw-31-toward-a-vocabulary.pdf

Will update with final url as soon as it's posted.

Zoom Chat window:
From Danielle Batista to Everyone: Hi All, I am a PhD Student at UBC Vancouver and I am an Intern at Molecular Your where we are working on a solution for secure health data sharing using SSI

From Trev Harmon to Everyone: Hello everyone. I'm Trev Harmon, Certification Manager at ID2020. We are a non-profit working towards improving identity systems around the world through advocacy and technology work.
From Jeffrey Aresty to Everyone: Hi. Jeff Aresty, founder of internetbar.org and techforjustice.org - building trusted norms for the justice layer of the internet
From Zakir Suleman to Everyone: Hi everyone, I am a Master's Student at UBC Vancouver and I am a UX Intern at Molecular You working on secure health data sharing using an SSI approach, and my research is at intersection of UX, Trust, and Blockchain systems.
From Marc Davis to Everyone: Hi everyone in Breakout Space M, my name is Marc Davis. I am a former UC Berkeley Professor, Yahoo!, and Microsoft, who works on inventing the future. I am focussed on the political economy of the internet and tools and policies for empowering people to have control over their digital identity and personal data.
From Oun Finema to Everyone: Hi, Oun from Finema, we are working on SSI development in Thailand both public and private sectors.
From Scott David to Everyone: Howdy. I am Scott David. 30 years as attorney. Now at applied physics lab. Doing "engineered policy" to support human interests in information technology systems. Apply compensating controls across BOLTS "business, operating, legal, technical and social" variables to help assure that "technically feasible" systems are also BOLTS reasonable
From Alan Cameron to Everyone: Hi everyone. I'm Alan Cameron, Director of Programs and Operations with iRespond which delivers privacy-protecting biometric identity solutions for the humanitarian and health sectors in developing countries.

From Scott David to Everyone: Important to demonstrate symbiosis in language of each stakeholder
From Fabiane Voelter to Everyone: Hi all, I am Fabiane, a Doctoral Researcher from Germany looking into user interaction with IS,, specifically blockchain-based Systems.
From Bob Wyman to Everyone: https://moralfoundations.org/
From skyberg to Everyone: "… By clicking, you agree that Company X and it's affiliates…."
From Scott David to Everyone: Legal burden is surface of power relationship
From Bob Wyman to Everyone: In "normal," physical world, we are constantly entering and exiting relationships. However, those relationships are often implicit while in the digital world they are often explicit.
From skyberg to Everyone: The self serving trickery of pretending customers are disinterested because they are simply overwhelmed.
From Jeffrey Aresty to Everyone: That's exactly the problem; creating trusted online communities where individuals and companies who join agree to norms, such as the ones you've described, changes the power play. Broad adoption is needed to make them relevant. That's why we work in the developing world.
From Scott David to Everyone: The phone is like a mining shovel, It is like a bank branch, a scoop for deposits/attention for fractional reserve lending/identity leveraging
From Tony Fish to Everyone: loving this
From Scott David to Everyone: Capitalism was "great" to conquer nature (extract resources). But now it has turned its extractive apparatus on us. Mary Shelley markets? BY the way, when I say "great" I am intentionally being ironic about the harms and suffering under colonialism, imperialism, etc.
From skyberg to Everyone: Volume is good
From mary hodder to Everyone: https://www.w3.org/community/privacycg/
From Tony Fish to Everyone: confusion - who knows what mobile or broadband tariff comparison are on. Compare utilities and flights. when in a utility/ commodity your only differentiator is confusion - you avoid direct comparision . when it is free …. confusion(squared)
From Scott David to Everyone: Joe Andrieu is a very clear thinker in the identity space.
From mary hodder to Everyone: Wouldn't you have Me2B further back at the 2 hearts?

From Catherine Nabbala to Everyone: Nice one
From Chris Buchanan to Everyone: Surveillance implies unilateral action by the observer.
From Judith Fleenor to Everyone: The user doesn't know the cost… often.
From Scott David to Everyone: Power relationships are embedded within the ceremony itself
From Marc Davis to Everyone: One of the reasons that TOS and PP are "contracts of adhesion" is that people do not "recognize the costs" of agreement.
From Scott David to Everyone: We need to alter the ceremonies
From skyberg to Everyone: Agree! I'd love to get the deck!
From Scott David to Everyone: Contracts of adhesion can also occur when you do know the costs, but are compelled to accept the bundle. It is a power abuse generally.
From Jim Fenton to Everyone: What's the relationship between this initiative and Doc Searls VRM?
From Scott David to Everyone: Unconsciounability is a grounds for voiding a contract (ab initio - Ohhhh. Latin!) when parties don't under the terms/costs. No meeting of the minds. Both Me2B and VRM have a theory of change of inverting the power relationships (See Derrida)
From Jim Fenton to Everyone: @Scott That's what I was seeing too. What are the differences between them?
From Scott David to Everyone: The opportunity for inversion is here. Internet and COVID has dis intermediated ALL institutional relationships. How shall we reintermediate them? M2B and others are aspirations.
From Chris Buchanan to Everyone: Prosopagnosia causes serious social discontinuity and isolation. In the digital sense, it also causes security issues.
From Scott David to Everyone: Like a poster in my "lab" says: "Futurism: Building a fake future in the hope that the real future will come along and mate with it!"
From skyberg to Everyone: @David Scott, I love that? ^
From Scott David to Everyone: Economic power is a useful pathway to social and political power
From John Kelly to Everyone: Are their potential incentives outside the specific transaction or regulation that would move toward ethical Me2B? Is a 'subsidy' for a cleaner transaction ethic a possibility?
From mary hodder to Everyone: i'm muted
From Scott David to Everyone: Its like the t-shirt says "I cannot believe I am still protesting this shit!"
From Paul Dunphy to Everyone: re: the point about not being legally allowed to destroy art in Europe - I think the French are uniquely strict on that topic. Other countries in Europe are not.
From skyberg to Everyone: Seems like that starts with reducing the burden of understanding, right?
From Scott David to Everyone: Voting and consumer market behaviors have been hijacked by agenda laden, a-humanitarian considerations. United we stand. What is the vector of unification at present? Us to B?
From Brent Shambaugh to Everyone: One of my favorite business ontologies: https://github.com/valueflows/valueflows (open value networks)
From Scott David to Everyone: Substitute "negotiation" for current "notice/consent" choreography
From Lisa Levasseur to Everyone: www.me2ba.org
From James Manger to Everyone: id aliasing -> "you'll have nothing" … but you'll have nothing only for the 1% who take the effort to do the aliasing
From Me to Everyone: lisa.levasseur@me2ba.org
From Judith Fleenor to Everyone: Thanks for this background, history and interconnections information, Mary. Helpful.
From Judith Fleenor to Everyone: Thanks Lisa!
From Zakir Suleman to Everyone: Thank you very much for this talk, and your work!
From Tristan Nicolaides to Everyone: THANK YOU VERY MUCH LISA

Meet the NEW Sovrin Foundation

Tuesday 2A
Convener: Chris Raczkowski
Notes-taker(s): Sankarshan Mukhopadhyay, Nicky Hickman

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

Please see notes, included with the slide screenshots that are provided below.

[Chris R] What is happening at Sovrin and the plans we have. Members of the BoT are also on the call to be able to respond to comments, questions and clarifications.

[Chris] 2020 has been a busy year for Sovrin. There have been adjustments which were undertaken in Q1. Sovrin1.0 (or the old Sovrin) - had a fair amount of uncertainty and concern around the direction as well as financial constraints. The transition team took over during Q2 for the daily operations and stabilized Sovrin financially and from the overall direction of the organization. There is a pipeline of projects which are in the works for Q4 and beyond.

Chris acknowledged the huge help of a tireless team for transition including those not trustees, includes Joyce Searls, Riley Hughes, Paul Knowles, Anna Johnson, Karl Kneis, Drummond Reed, Darrell O'Donnell, Dan Gisolfi and Jason Law

[Sankarshan] As a response to the question from Karn Verma "Could you say a bit about the MainNet for those new to Soverin?

[Stephen Curran] The foundation of Sovrin has been Indy - a very stable product. MainNet has had 100% uptime (there is an upcoming session around the technology of Sovrin). There are stable operating nodes from Stewards

Sovrin is a governance organisation that manages, monitors network, coordinates with Stewards and MainNet, Staging and Builder are all rock solid and high performing.

Sovrin is a "not for profit" business. The BoT has also taken a new approach and a fresh perspective to look at Sovrin as a "sustainable social enterprise".

Sometimes you have for profit businesses that still have a social purpose, Sovrin remains NPO

Who does Sovrin's social enterprise mission serve?

Who is "All"?
Sovrin serves the SSI community as a whole, including:

⇒ ***All*** *individuals & organisations from everywhere and from every culture*

⇒ ***All*** *businesses from global financial firms to local start-up, NGOs, multilateral orgs, ...*

⇒ ***All*** *entities independent or not, natural or man-made*

sovrin
identity for all

What is Sovrin Today?

sovrin
identity for all

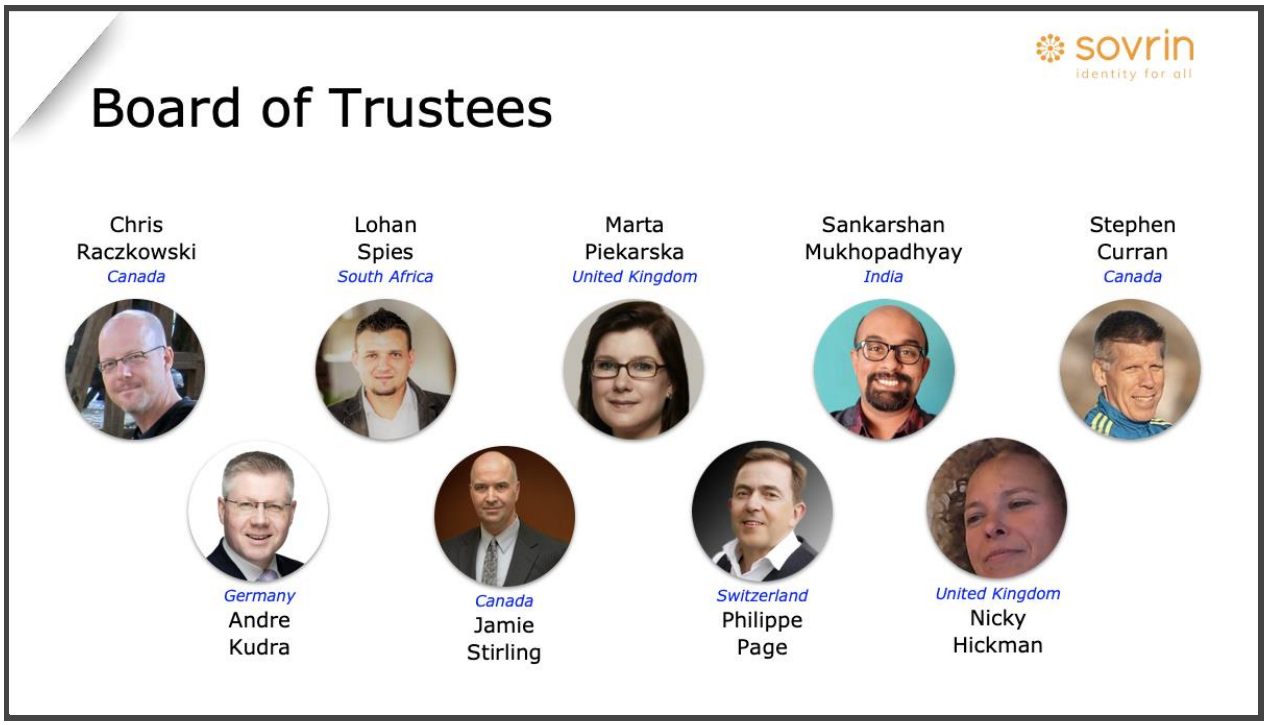
- a ***passionate*** global SSI community, including:
  - ⇒ 50+ Stewards operating network nodes
  - ⇒ open source global Working Groups and Task Forces
- a ***dedicated***, globally diverse Board of Trustees
- a ***growing*** execution team (lean and efficient)
- ***financially stable***; careful and conservative cash flow management
- clearly defined product lines aligned with the *Identity for All* ***mission***

There are aspects to Sovrin that are not limited to the utility network. Rather the multiplier effect of the community and stewards contribute to the health and growth of the Sovrin brand.

[Arnon Zangvil] Is Sovrin a democratic institution?

[Nicky] Yes @ Arnon, although we don't have voting members. We are going through a process of 'decentralizing governance' making things more open and community led. Not quite there yet, but certainly a benevolent oligopoly at this stage

Christmas Survey coming up to seek and receive feedback from the community.



Question: Sovrin vs ToIP

[Joyce] Can the board members explain the difference between Sovrin Foundation and the ToIP Foundation?

[Phillipe] The relationship between these 2 activities are perhaps a natural one. Drawing upon the work being undertaken in the Guardianship WG, when the Sovrin GF was v2.0 - and yet the solution needed work to be taken up at the both technical and governance levels. The Sovrin Guardianship TF paper led naturally to the “dual stack” which underpins the way ToIP see this.

ToIP is scaling out everyone to a global scale - thus there is a wider representation of community. Sovrin Foundation will continue to do its work as a pioneer (as a first utility network) - and in effect is a practical instance of what is being built in the ToIP.

Sovrin is the instance, ToIP is the class. Sovrin is doing, ToIP is framing

[Chris] ToIP’s origins lie in the Sovrin world but at the same time it focuses on the wider set of requirements originating from the SSI stack.

[Nicky] There are briefings with APAC based communities and groups as part of the open Board meetings. The present set of meetings and engagement timings are US/EU centric. A decentralised and federated

model is possibly something to consider. Being guided in our work by the "Identity for All" mission to have a council around I4A.

[Phillipe] I4A allows the Sovrin Foundation to focus on activities across the globe. Identity is not to be looked at in the same way across regions - instead local requirements, nuances and aspects need to be factored into the way designs have been created.

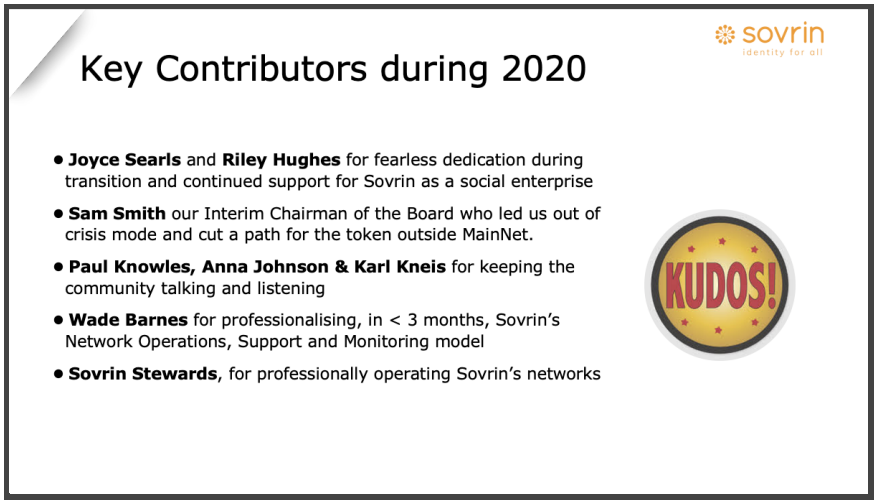
[Karn] How many SSIs are operational in the world today.

[Andre] would like to seek clarification around the usage of SSI

[Stephen Curran] - to interpret it as "how many credentials have been issued". From a BC Gov perspective - there have been millions of credentials. The specific number will not be possible to declare as a result of the privacy preserving design. Also see https://indyscan.io

[Arnon] So how can we know if you are delivering on the mission?

[Karn] How does Sovrin Foundation measure progress on the mission through metrics?



Key question: How are you able to measure delivery on the mission? Some qual and some quant metrics, but Aaron is right we need to be able to measure this and show our delivery


sovrin
Sovrin 2021 (& beyond)
Delivering on SSI Business


Preliminary Goals for 2021
sovrin
• Continue to strengthen the BoT and execution team
• Add global diversity within Sovrin
• Organize Sovrin as an internationally distributed entity
• Deliver multiple projects for the Identity for All mission
• Demonstrable progress with Network of Networks, and interoperability
• Facilitate SSI adoption with productive use cases on MainNet
Grow Sovrin's reputation as an independent, neutral and trusted champion for SSI, based on delivering valuable results to the global community


Key Messages
• Identity for All is the mission that informs all Sovrin activities
• Sovrin is a sustainable Social Enterprise
• MainNet continues to be a stable and robust global public identity utility
• Network of Networks and Interop are key strategic initiatives
• Sovrin is healthy, energized and open for business
sovrin
identity for all


sovrin
identity for all
Thank you!
</>
{code}

Introduction to OpenID Connect (a "101" session)

Tuesday 2B
Convener: Michael B. Jones
Notes-taker(s): Michael B. Jones
Tags for the session - technology discussed/ideas considered:

#OpenID #OpenIDConnect #OpenIDCertification

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

The presentation is posted at https://self-issued.info/?p=2130. (links to PowerPoint & PDF)
The links there are stable. The session was recorded to the cloud.

Rebase - Decentralized Keybase

Tuesday 2C
Convener: Wayne Chang <wayne@spruceid.com>
Notes-taker(s): Simon Bihel <simon.bihel@spruceid.com>

Tags for the session - technology discussed/ideas considered: #Keybase #Trust

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

- Web-of-Trust related problem, mappings to your identity (twitter, websites, etc)
- Keybase was acquired by Zoom, which is problematic because of a lack of resources for innovation.
- Decentralisation allows private attestations (equivalent of proof for Keybase).
- Can you have crawlers who get information about those private attestations? No, because validators don't advertise the attestations they have issued.
- Should notaries (third parties validators) be used, for legal use-cases? Not for now, for simplicity.
- Related document https://hackmd.io/IZgDPFy6QiaZXbUk7Ik87Q
- Interoperability and standards are important so the network of trust isn't only usable by a certain company's products.
- Can't Rebase simply be the composition of some existing tools (e.g. DID methods)? Yes, the goal of the project is to abstract the technical layers.
- One way of thinking about Rebase is that we would recreate the network that big companies and banks already have on us, without our consent.
- Related to notaries, how can you integrate non-digital documents (e.g. paper)?
- A validator could only limit itself to a certain set of validations.
- Isn't Rebase a new DID method? Rebase is less strict than a formal DID method, more suited to our messy world (as well as more human-readable).
- Concerns about privacy, as you can go from the Rebase ID to the social media accounts (a global directory can be built from the data in Rebase). But attestations don't have to be only about

identity, identity proofs could also be more private (e.g. private message in Twitter, instead of a public tweet).

- Sybil resistance? BrightID was mentioned as one of the social media platforms.
- The privacy implications can be ok if the user agrees with it, but can it impact other people/connections?
- https://keys.pub/ is brought up. Rebase is focused on social attestations.
- We're monitored already as you're going about your business. But keys are something you control.
- The governance of the directory is very important to avoid companies like ClearView having access to such directory.
- What's the scope for KERI events. And isn't opt-in too weak because non-linked accounts can still be found/crawled.

Project description: https://docs.google.com/document/d/1kJhRE0CQ8BI2cOihdRE9EH-4atgwFJTwyXlB9LcebhE/edit#heading=h.dhpooiemp4fs

Zoom Chat:

From Steven Wilkinson : The participants list, claim host
From By_Caballero : https://keybase.io/by_caballero
From By_Caballero : ^ Example "medium-strong" ID
From Tobias Looker : Big +1! Also have some thinking on how to do this, and how to integrated with verifiable credentials!
From Andrew Whitehead : Not to jump ahead (okay, jumping ahead) but I'm curious about key rotation and maybe tying things together in a DID doc (or with keri)
From Tobias Looker : https://hackmd.io/lZgDPFy6QiaZXbUk7Ik87Q
From Orie Steele : : / starting with a foundation From Tobias Looker : Haha From By_Caballero : q+
From By_Caballero : can't raise hand, am host
From Orie Steele : Yep, in a way, this is decentralized surveillance as a service :)
From Gabe Cohen : surveilMe
From Tobias Looker : DSAAS
From By_Caballero : lol I was multitasking; can someone else make the notes reflect that
19:26:52 From By_Caballero : https://docs.google.com/document/d/1kJhRE0CQ8BI2cOihdRE9EH-4atgwFJTwyXlB9LcebhE/edit
From By_Caballero : something about notaries and standards? :D
From Adrian Gropper : Standardizing how people notaries keep logs
From By_Caballero : surveil.me ; notarize.me
From Adrian Gropper : human notaries From By_Caballero : i know, just teasing :D
From By_Caballero : Infominer is sitting right there; this is Infominer erasure
From Orie Steele : q+ to talk about architecture
From By_Caballero : q+ to speak to KERI analogy
From Eric Welton (Korsimoro) : q+ to speak re: KERI - KERI is about precision, this is about mapping imprecision
From By_Caballero : q- ; (i think eric might have a more eloquent version of what i was thinking)
From Orie Steele : did:github:OR13
From Gabe Cohen : did:twit!
From By_Caballero : don't you dare bring did web into this
From Orie Steele : https://github-did.com/resolver
From By_Caballero : q+ : (after Adrian)
From Orie Steele : q+ to ask about how to start with friendly names
From By_Caballero : "pet names" :D

From Orie Steele : Didn't people give up their privacy when they agreed to Facebook ToS :)
From By_Caballero : as private and secure as the LEAST secure and LEAST consented of the linked profiles
From Charles Cunningham : q+ about does/could keybase have value for sybil resistance or is that not a goal
From By_Caballero : ^ move over Idena and BrightID ! : (I want to reiterate that this is literally how credit cards protect against sybils-- by paying data brokers to attest to the age and quality of the trackers you've consented to)
From Tobias Looker : But who controls that global directory namespace
From Tobias Looker : You've just created DNS essentially
From Eric Welton (Korsimoro) : you mean google?
From By_Caballero : ^ Palantir, more like; (sorry to be bleak); Bad news, eric
From Eric Welton (Korsimoro) : i'm an accelerationist in this area - at this point I think the only way to create action about the fact of Palantir, or DHS HITEC, is to open up the existing private maps to public so that they demand a social response in the face of all the other stuff we're dealing with.
From Orie Steele : Directory is inevitable; Just like thanos
From Kimberly Duffy : q+ re keybase/keys.pub replacement
From Charles Cunningham : many directories exist already, luckily we're solving portability to make it easy for them to join together 😆
From Orie Steele : bech32 ; pepelaugh
https://didme.me/did:meme:1zgswzdje885tzr8408m37sjmaa0sthw265ty6hmwzmau48kd809zzrgra4w5w
From Orie Steele : ^ also uses bech32 ; Big +1 to Adrians point
From Gabe Cohen : face..index
From Orie Steele : Biometrics can be compelled : Best not to use them as the sole factor : I would be in favor of working on this more : I think its a cool idea
From Kimberly Duffy : Epic beard Adrian! I'd be remiss if I didn't compliment you
From By_Caballero : It won't protect you from the cameras, tho : try insane clown posse paint
From Orie Steele : And infrared reflectors
From Gabe Cohen :
https://didme.me/did:meme:1zgsyjd79ruhltsc6awvakj7ays7t7ngmn9z4znp4rjf4vm8t0sacvjqnlu3hf
From Orie Steele : lulz
From By_Caballero : https://nakedsecurity.sophos.com/2018/07/04/want-to-beat-facial-recognition-join-the-insane-clown-posse/
From Orie Steele : Lets be real, it only takes like 4 calls to uniquely identify you when you get a new burner… ; The directory is inventitable
From John Hopkins : resistance is futile 😂
From By_Caballero : https://docs.google.com/document/d/1kJhRE0CQ8BI2cOihdRE9EH-4atgwFJTwyXlB9LcebhE/edit

Regional Indy Networks: Setting Up, Running, Share Experience

Tuesday 2D
Convener: Dave McKay

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

A universal wallet (in the OS?) that can hold credentials, and then branded or application specific wallets can share credentials in that device.

Portability between wallets & sync contents between wallets, devices.

Can there be one container holding all the credentials -- an OS layer of security. Apple has talked about this... Ares working group? SSI counter-intuitive to Apple, Google?

KERI for Muggles

Tuesday 2E
Convener: Drummond Reed
Notes-taker(s): Ajay Jadhav,

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

LINK TO THE "KERI FOR MUGGLES" SLIDES SHOWN IN THIS SESSION
(Note: these are publicly available Google Slides)

KERI:

- Self-certifying identifier
- No Blockchain needed.

Sam: Binding = derivation

Nuttawut: Is KERI considered a type of decentralized PKI ?
Drummond: Yes, KERI is an entire architecture for decentralized PKI

Binding = There is a secret relationship between the public key and the SCID, and you can prove the relationship only with the knowledge of the private key

The self-certifying identifier is ED25519 like digital signatures and not an hash.

https://jolocom.io/blog/how-keri-tackles-the-problem-of-trust/

KERI uses key event logs like blockchain.

Timothy: It is not a double-spend proof and cannot support a cryptocurrency. It is purely a system for SSI, Identifiers, VCs, etc.

You can prove you control a KERI identifier without needing a to rely on ANYONE outside your control

KERI writes a new digitally-signed message to a log file so you can prove you made the change.

A single KERI identifier may be derived from a set of key-pair so it supports multi-sig

KERI operates in

- Direct mode - pair-wise interaction
- Indirect mode

David Huseby: Do you consider access control for key event logs?
Not exactly, but In case of privacy, you can encrypt the key event logs and share to only those whom you want to.

KERI is about authenticity - if you want privacy you need to layer it on top of it.

Benefit #2: Each time you change your key KERI writes a digitally-signed message to an “event log” which is a simple type of log file

1.Step:	Self-certifying identifier	can prove to be the one and only identifier tied to public key using cryptography alone (no blockchain needed)	Benefit 1: You can prove you control a KERI identifier without needing a to rely on ANYONE outside your control
2.Step:	Self-Certifying Key Event Logs	Each time you change ("rotate") your public/private key pair, KERI write a new digitally-signed message to a log file so you can prove you made the change	Benefit 2: Each time you change your keys, you can prove you control to
3.Step:	Witnesses Key Event Log	all key events signed by Controller and Witness	Benefit 3: Although witnesses are not required, they provide additional evidence that you control your current public key(s) and are not cheating

4.Step:	Prerotation as simple, safe, scaleable (generate key pairs in wallet, digitally sign a proof of the next public key – write that proof and signature to the event log)	KERI can't prevent theft of your current private key - but it has an ingenious solution for hiding your next private key that makes recovery control authority through key rotation (ist like a backup – you an identifier having persistent value -> you want to protect and control of the identifier over time)	Benefit 4: You can safely "lock away" your next private key so it can't be stolen from your current device – and protect yourself if your current private key is ever compromised (this key protection post quantum proof)
5.Step:	System independent validation	Because KERI identifiers and event logs are self-certifying, they can be witnessed by any system anywhere that can store and return data – and you use all of them as witnesses	Benefit 5: KERI identifiers and keys are not "ledger-locked" – they are fully portable and can be validated using any ledger, distributed database, or other verifiable data registry
6.Step:	Delegated self certifying identifiers enables enterprise-class key management	KERI identifiers can be "delegated", meaning one identifier can create another one that can prove its relationship with its parent – so you can create any hierarchy of identifiers & keys	Benefit 6: With KERI identifier and key delegation, enterprises can scale and manage delegation hierarchies of any size and complexity
7.Step:	Compatibility with the GDPR "right to be forgotten"	When decentralized identifier for a person is written to an immutable ledger, it can creates a privacy issue because it cannot be erased – but KERI identifiers can use witnesses that permit erasure	Benefit 7: KERI infrastructure can be GDPR-compliant because it does not require the use of immutable ledgers – KERI event logs can be deleted without compromising security

The History of Cryptography

Tuesday 2F
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:

The session reviewed the history of cryptography, which in many ways is the history of many of the ideas in discussion today within the identity community. It aimed to provide a high-level overview with lots of pointers for those who wished to go deeper.
View more here:
https://app.mural.co/t/wipsmural3011/m/wipsmural3011/1591081218133/46fa91917c9f2d24ea8f4a623e4920b49af40100

SSI + Confidential Storage + Tapestry Credentials for Proof of Occupancy (Encore Wed)

Tuesday 2G
Convener: Dmitri Zagidulin, Liam Broza
Notes-taker(s): Liam Broza

Tags for the session - technology discussed/ideas considered:

SSI, Confidential Storage, Tapestry Credentials, LifeScope

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

Presentation: https://docs.google.com/presentation/d/1bwOMI5mB-mL6sKkj86-iXFdePaPlsfJpdoLTdRzROFE/edit#slide=id.p

Yuliya Panfil / Senior Fellow and Director, Future of Property Rights, New America panfil@newamerica.org

Liam Broza / Data Architect, LifeScope Labs liam@lifescope.io

Dmitri Zagidulin / Data Architect, Privacy/Trust/Storage, LifeScope Labs dmitri@lifescope.io

1 Page Summary
https://drive.google.com/file/d/1_IvefA7lYJpAe1PRpIjtUCWQH63GvIjs/view?usp=sharing

Abridged Paper
https://docs.google.com/document/d/15pUIUKTa81rAhtYNCK9EO_KisNgijGXiW1Sk1WAGtVo/edit?usp=sharing

Active and Passive Identifiers: Elements, objects and characteristics of a decentralized network

Tuesday 2I
Convener: Paul Knowles @pknowles
Notes-taker(s):

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

Paul presented a slide deck that defined the two concepts of passive & active identifiers.

- Passive: Immutable
- Active: Authenticable

Everything is documented in the slide deck which is available here.
Related blog post: https://humancolossus.foundation/blog/active-and-passive-identifiers

Rolling Back Surveillance Capitalism, Part 1: Describe the future (in detail)

Tuesday 2J
Convener: Johannes Ernst
Notes-taker(s):

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

It's time to do something.

Example: Weather site / app. Should have an alternative funding model. E.g. allow the customer to enter their credit card to pay instead of surveilling ads.

Somebody like Apple could facilitate micro payments to sites instead of them doing ads. Could be the broadband provider. Needs a clearance function like ASCAP.

Data becomes data + its attributes (rights)
Market to rights to data.

Coop form. Trade association for humans.

Information should degrade over time.

Doesn't think it can be done with regulatory intervention

Should be able to declare one's interests. Could be point-to-point. Could be broadcast.

What *assumptions* are we making about surveillance capitalism? such as data means something, data can represent you, your data is a model of you?

What does the future look like? Whose future matters? How do we make a value judgement?

Mandatory, standardised data portability (such as is already mandated in GDPR but not as yet being delivered on). More on how we make that happen when we get to the solutions session.

Digital divide - those who have value in their data and get something for free if they want and can trade their privacy Vs those who have no value in their ad data as no disposable income and have no choice - is that fair ?

Personal Data Logistics (PDL) = mobility, data sharing, data portability, data sharing ? difference by rights (controls); right data, right time, right place, right basis ('right' is defined by the individual, but recognises that many data attributes are co-managed; e.g. my bank balance).

People have rights to their digital identity, their data.

Have highly standardized contracts that govern the relationship.

Ability to monetize your intent.

Have a digital self. (digital twin) E.g. physical box that has all your info, or hosted by trusted intermediary.

Has all relationships with vendors etc.

We all already have digital twins; they are just run by GAFA. (they have a collection of data but the model does not present or represent you)

Need to change the rules, so that harvesting the data is not worth: have “purpose-based services”. Article 5 in GDPR sets out such rules (they call them principles but they are ideas or values)

Able to answer CCPA notices in bulk.

Meaningful service providers and purpose based services can lead us to the world where we don’t need apps or websites but with your digital you can figure out where to go and what to do to achieve a specific goal. Without brokers and companies which just do the business to harvest data. We need to change the rules in a way that it is not profitable to aggregate data.

Regulation has made certain behaviors illegal

Higher fidelity data is much more appealing to “consumers” of personal data, so worse data is far less appealing to acquire. Might go out of business?

Criminalize the following:
•Surreptitious user/group profiling. (that rules out all governments)

•Attention optimized information delivery.

•Algorithmic manipulation of biological processes against user consent or user interests. (however what happens when you change your diet/ nutrition and that means you improve your health/ value to society/ costs to an economy)

Data as Body
Emerging work around "Data As Body"
https://internetdemocracy.in/2020/04/data-as-body/ <- Video...watch
https://internetdemocracy.in/reports/when-our-bodies-become-data/
https://harvardlawreview.org/2013/05/what-privacy-is-for/
https://internetdemocracy.in/reports/data-sovereignty-of-whom/
https://datagovernance.org/files/research/IDP_-_Data_sovereignty_-_Paper_3.pdf
https://internetdemocracy.in/2020/05/new-video-a-feminist-perspective-on-principles-of-consent-in-the-age-of-embodied-data-draft-paper-presentation/

Who provides that piece software that holds your data / preferences?

Better governance models for humanity. YES PLEASE :)

Vishal: We (who is we) need disposable identities. We have them already ….

Zoom Chat
From Scott David To Everyone: Industry hasn’t felt need to change.
From Alexis Falquier To Everyone: This call is being recorded yes?

From Kaliya Identity Woman to Everyone: Do you want to record this session...Ok; if we want good notes folks need to chime in and do that
From Tony Fish to Everyone: what *assumptions* are we making about surveillance capatilism? such as data means something, data can represent you, your data is a model of you?
From Sam Goto to Everyone: anyone has the link to the doc?
From Tony Fish to Everyone: https://qiqochat.com/breakout/32/iiw31 From Sam Goto: ah, thanks!
From Chris Buchanan to Everyone: Surveillance implies unilateral action by the observer.

From Tony Fish to Everyone: What does the future look like? Whose future matters? How do we make a value judgement?

From Hunter Cain to Everyone: they force you into it through consolidation

From Tony Fish to Everyone: Digital divide - those who have value in their data and get something for free if they want and can trade their privacy Vs those who have no value in their ad data as no disposable income and have no choice - is that fair ?

From Chris Buchanan to Everyone: We have in the past recognized that some information should be publicly available. Arguably weather is a public safety issue and should be provided without a need for identity at all. If we drill down it an example that is more relational (one that requires identity) it may help.
From alexwykoff to Everyone: Doesn't Brave already do the microtransactions to publishers though? Is the differentiator a preference to stay in fiat?
From Hunter Cain to Everyone: To me micro payments turn into the same concept of pay to play
From Tony Fish to Everyone: +1 @chris buchanan - health data for the common good, your data helps indirectly those who sell to the health service services and products.
From Jeff Orgel to Everyone: Q = comment on trust/communication layer between provider/beneficiary leveraged by beneficiary granular controls in relationship profile. Matrix of factors filters most wanted contacts.
From Tony Fish to Everyone: +1 @scott
From Robert (Human Colossus) to Everyone: Ritghs sounds right!
From Iain Henderson to Everyone: In this future state, i'd like to see mandatory, standardised data portability so that users of any internet service can instantly request and get a copy of their service use and other related data via a button/ standard engagement model.
From Jeff Orgel to Everyone: +1 to portability too Iain!
From Tony Fish to Everyone: @iain data mobility, data sharing, data portability, data sharing ? is there any difference do they have different rights ?
From Robert (Human Colossus) to Everyone: I would slightly change Ian comment - and would say that I would like to see is that nobody copy my data rather they have right to access it, where any time I can revoke this access
From Eric Weber to Everyone: There should be standards for the payments, so you don't have Apple facilitating micro payments, but people choosing between 100 ways of transferring some kind of value to the service provide. I set my rules, may be agree to pay a few sense for using a website and the payment happens in the background automatically.
From Iain Henderson to Everyone: No difference between portability and mobility other than choice of jargon. The underlying and much bigger point is around personal data logistics - how do I, the service user and service provider ensures that the right data goes to and from the right place at the right time; and the wrong data does not. So i'd call that personal data logistics (optimisation).
From Tony Fish to Everyone: "personal data logistics" PDL

From Scott David to Everyone: Fractal policy has “scale independent elements” which is helpful for scale-free controls
From Iain Henderson to Everyone: Robert - to your point above, it is key to understand that I am not the master data manager of all data about me. For example, my bank is the master data manager as regards my bank balance. We both co-manage it, but I only have read and share access; not write.
From Scott David to Everyone: Dunbar’s number is about 120 right?
From Vittorio Bertocci to Everyone: 150
From Iain Henderson to Everyone: yes it is Scott
From Vittorio Bertocci to Everyone: look it up :)
From Scott David to Everyone: That means I can now have 30 more friends. Will you all be my friends!? +1 to Marc
From Tony Fish to Everyone: Surveillance Capitalism assumes data = behaviour and that a data model of you is a good representation of you. Is this an assumption that stands up to testing ?
From Eric Weber to Everyone: if you can undo your friends, you can choose 150 every day
From Jeff Orgel to Everyone: Local Is My #1!
From Tony Fish to Everyone: digital self or digital twin ?
From Jeff Orgel to Everyone: 27 TB QNAP
From Tony Fish to Everyone: +1
From Scott David to Everyone: Digital self can be spread across the world IF reliable system. Steven Wright said: “I have the largest seashell collection in the world - I keep it on beaches around the earth.”
From Jeff Orgel to Everyone: Some clouded and rolled to other drives too...
From Iain Henderson to Everyone: digital twin @Tony. That term is now well understood in corporate world.
From Jeff Orgel to Everyone: Ya, your stuff is quite kool Johannes!
From Scott David to Everyone: The Mirror model seems more realistic
From Kaliya Identity Woman to Everyone: just a note if you want your comments in chat in the notes…please move them over. It doesn’t seem to be easy to save the chat.
From Iain Henderson to Everyone: I could not open the session document for some reason.
From Scott David to Everyone: I couldn’t either
From Kaliya Identity Woman to Everyone: You have to click on the TAB Session 2J
From Jeff Orgel to Everyone: Yes, we must walk in "the world" of transit toward values and wants. We are seen indeed. Can we grind the optics a bit better tho!?
From Iain Henderson to Everyone: We already have digital twins (in fact many of them, octuplets or more); problem is we don’t run them, the surveillance capitalists do.
From Jeff Orgel to Everyone: We want to walk in a civilized space, not the wilder-lands. Civilization please!
From Chris Buchanan to Everyone: I also don’t agree that we have rights in the physical world that we don’t have in the digital world with respect to privacy. The issue isn’t privacy rights but the equivalencies made regarding the sameness of the mediums.
From skyberg to Everyone: Compliance is a function of liability
From Chris Buchanan to Everyone: @skyberg & liability is a function of standing.
From Vittorio Bertocci to Everyone: +1 @skyberg!
From Tony Fish to Everyone: compliance is a function of law, regulation. Liabilities rest with the directors and their insurance policy
From Chris Buchanan to Everyone: Standing is a function of injury.
From Tony Fish to Everyone: +1 chris
From Hunter Cain to Everyone: Have to monetize the data and give it a value
From skyberg to Everyone: Amazon promised me they only use my data to improve my service!
From Tony Fish to Everyone: is a promise a contract ?
From Chris Buchanan to Everyone: @skyberg… and so you were not harmed but helped!

From skyberg to Everyone: That was Scott David
From Scott David to Everyone: Market/bidding system. Fiduciary type obligations for agent to avoid conflict of interest 4th party type system. Like in Real Estate deals - Both sellers and buyers have agents - parity.
From Eric Weber to Everyone: you might want to add a data escrow account
From Scott David to Everyone: Bundling is a big deal now for information services. Unbundling will help to disambiguate rights
From Jeff Orgel to Everyone: That's what I'm talking about Marc. The HiFi Trust. At scle would be great!
From Vittorio Bertocci to Everyone: Only regulation can step in there. Uber doesn't need to know _everything_ about you to provide a better service, better position its fleet etc etc
From Scott David to Everyone: Data escrow makes lots of sense. In fact, we developed a Community Distributed Data Escrow for disaster response/refugees, etc. It is like a eBay/UBER for data - Data stays where it is, but is escrowed by "duties" moving to the data.
From Jeff Orgel to Everyone: Limited HiFi too toVittorio's point. From Sam Goto to Everyone: right
From Hunter Cain to Everyone: technology will always outpace our right to privacy .
From Sam Goto to Everyone: if uber got a directed identifier, it wouldn't be able to export it
From Tony Fish to Everyone: regulation is the answer when your principles are wrong, your risk framework is broken and governance has no down side implications
From Vittorio Bertocci to Everyone: Any service you use with any regularity can track you regardless of the identifiers infrastructure. Weak features are enough for ML to extract identification with the data model is big enough
From Scott David to Everyone: No one knows who you are really. Perhaps we should focus on gradients of information entropy associated with identity attributes. Set gradient as appropriate for interaction. Gradients are Lagrangian Coherent Structures that stand still (like lenticular clouds) as the interaction winds blow past.
From Vittorio Bertocci to Everyone: and Uber data cannot be obtained anywhere else, only Uber has your ride data
From Jeff Orgel to Everyone: Well put Marc - Guessing v Knowing...
From Sam Goto to Everyone: that's a good distinction indeed
From Tony Fish to Everyone: +1 scott - I don't know who I am
From Scott David to Everyone: 07:42 PM +1 to Chris
From Vittorio Bertocci to Everyone: Guessing in the MLworld can lead to more accurate knowledge about yourself that you think you yourself know
From Jeff Orgel to Everyone: "That you make lists, not what's om them. That we share, not what we share." Zubboff not verbatim
From Scott David to Everyone: Like a buddhist - If you want to know yourself, observe what you actually do, rather than what you think are your motivations.
From Tony Fish to Everyone: is there more volume of money and margin in guessing than knowing?
From Iain Henderson to Everyone: +10 to what Marc said about using ML and Big Data for the individual
From Tony Fish to Everyone: @scott unless your emotional literacy is not in your control such as diet and illness
From Jeff Orgel to Everyone: I believe people want to truths about themselves into a space of services if they aren't predated. Pull the teeth of skimmed-prediction pushed nudging, etc...
From Hunter Cain to Everyone: again, monetize data. when corporations have to pay to use it, they stop using it
From skyberg to Everyone: +1 Hunter. And reduced subscription because you are forced to disclose how you use the data results in paying to use it. I know there's a WIT event today also. Bad timing, cuz I know of some folks that aren't here due to the conflict.
From Chris Buchanan to Everyone: Privacy is not about property. Soldal v. Cook County (1992)

From skyberg to Everyone: There is zero altruism in capitalism.
From Chris Buchanan to Everyone: The privacies of life must be protected against arbitrary power. Carpenter v. US (2017)
From Marc Davis to Everyone: personal data is an extension of the body, so the issue is about control, rather than ownership per se.
From Jacob Siebach to Everyone: I disagree that there is no altruism in true Capitalism. Data shows that the greatest givers to charity, before government involvement, are individuals.
From Tony Fish to Everyone: +1 scott shareholder don't own companies - they (the company) is owned by itself. We created something that does not exist without a common belief (yuri)
From Iain Henderson to Everyone: Genuine co-management of data will be the steady state for many important types of data. There are some data types I can manage for myself (e.g. intentions) as I generate them. For other types they are necessarily and rightly co-managed (bank balance, Covid status in NHS patient record). So in many cases we are talking about 'Our Data' not 'My Data'.
From Hunter Cain to Everyone: corporations are the greatest threats to humanity
From Jacob Siebach to Everyone: Corporations that do not act in a moral way are a great threat, but not all.
From Tony Fish to Everyone: @iain surly "data"
From Eric Weber to Everyone: Your money can be on 10 bank accounts, so the bank only has a fractional view. Only you know you total balance.
From Marc Davis to Everyone: @Ian agree. most personal data has joint rights.
From Chris Buchanan to Everyone: Sea captains lost their sovereignty with the invention of the radio.
From Hunter Cain to Everyone: They only operate in a way to make money in that fact they have no morality
From Chris Buchanan to Everyone: Corporate altruism is still an optimization of revenue which is engendered by an externality of tax law and social norms.
From Scott David to Everyone: Start at the beginning
From Tony Fish to Everyone: @roundtable - the pure shareholder return of the 80's is dead, exist to create a sustainable eco-system +10000000000 doc
From Scott David to Everyone: Yes, but now the time has come
From Kaliya Identity Woman to Everyone: Please put JEMS from the chat INTO the document
you can not cut and paste the chat. you literally have to type them.
From skyberg to Everyone: Morality in corporations is imposed. That's not a judgement - just a fact that we need to leverage in order to drive corps to a more moral position.
From Scott David to Everyone: Time to use your miles for the wonderful items in the "SkyMall" magazine
From Tony Fish to Everyone: we have agency, power and influence ….
From Scott David to Everyone: WE is the operative word. Communities of interest can cohere and have amplified voice. Vectors of economics, politics, markets all have channels for group action.
From Jacob Siebach to Everyone: You cannot legislate morality--Samuel Adams.
We can create a culture that promotes corporations acting in moral ways, but the government can only punish wrong, not ensure right.
From Hunter Cain to Everyone: I think this is extremely important to talk about, when corporations are only focused on profit and that profit is obtained by your data, how do you defend yourself?
From Scott David to Everyone: +1 to Jacob
From Tony Fish to Everyone: is our rear view focus on finance and creating models from them as a predictor of the future a framing that trips us up with data. we assume that data will model our future.
From Scott David to Everyone: +1 to Tony. We use gaussian (normal) distributions to predict the future in complex systems that display non-linear behaviors
From Eric Weber to Everyone: may be he did not pay his subscriptions
From Vittorio Bertocci to Everyone: :P
From Scott David to Everyone: The "linguistic turn" of interoperability

From Tony Fish to Everyone: as a community we should talk about the complexity and then compress it into a linear narrative which allows us to explain where we are going
From Scott David to Everyone: "Place cells" in the brain are freaking out!; Law is artifact of philosophy. Enforceable stories about thinking and "self."
From Tony Fish to Everyone: @scott - watch out for those bacteria
From Zakir Suleman to Everyone: ^ I'll add: a couple of very particular European conception of "self"
From Scott David to Everyone: This is not a pipe!
From Kaliya Identity Woman to Everyone: before you push 'send' on a message in here - cut and paste it into the notes… too. :)
From Scott David to Everyone: I cannot access the notes. I tried.
From Robert (Human Colossus) to Everyone: the chat is stored and put in the notes later on
so need for that
From Doc Searls to Everyone: "Enforceable stories!" Yes!
About stories: https://blogs.harvard.edu/doc/2019/07/23/where-journalism-fails/
From Sam Goto to Everyone: +1 from vishal
From Scott David to Everyone: On "enforceable stories" let's discuss 4 steps of institution construction later. Practices to best practices to standards to institutions. That process organically creates legislative, judicial and executive functions that characterize ALL governance systems.
From Sam Goto to Everyone: "phone-home" and "correlation", i like the wording
From Tony Fish to Everyone: @kaliya *phone home * IIW 1?
From Scott David to Everyone: We should not feel bad about these being perennial human challenges in society - Anaxamander (sp?) and Epicurus/Lucretius struggled with the same questions of individual/group. Human sapiens sapiens are about to add a new "sapiens", e.g., those who "know that they know that they know"
From Tony Fish to Everyone: +1 @scott
From Scott David to Everyone: +1 Jeff. Human operating system; Morphological computing at least; Social computing
From Tony Fish to Everyone: "human operating system" is an abstraction as the humans system runs on chemistry which is the OS
From Scott David to Everyone: Maybe institutions are meaning making machines. Humans interacting with institutions give and get meaning. Like a reaction vessel for converting data into information that can inform future interactions for both parties
From Bill Wendel1 to Everyone: Doc asked, "How can we have better signaling about us rather have {players in the surveillance capitalism marketplace] guess about us all the time?
A post-surveillance capitalism real estate ecosystem needs to (1) create IntentCasting tools — #Intend2Buyer and #Intend2Sell, and (2) move past the assumption that homebuyers & sellers will use a one-size fits all buyer or listing agents. "Autonomous homebuyers" (a word Realtors made up) need an OPEN #HousingID that enables them to interact P2P. That would empower consumers to save BILLIONS of dollars annually. After three decades, that Holy Grail now seems attainable because of a massive, $50B class action lawsuit against the real estate industry, see recent article in
NYTimes: https://bit.ly/RESuit_v_ExcessFees The suit not only threatens to restructure Realtor compensation but reimagine, "What would the real estate ecosystem look like if the MLS did not exist?" More specifically, if the Realtor-controlled Multiple Listing Services did not silo or worse, intentionally HIDE listing data with "pocket listings," how can homebuyers and sellers interact using DIY IntentCasts?
From Sam Goto to Everyone: oh vishal
From Bill Wendel1 to Everyone: This reVRM-Minifesto is now a decade old but has never been more timely because the pandemic has cause more than 1 in 5 people to move or think about moving in the next 6 months: http://bit.ly/MyREData
From Sam Goto to Everyone: "disposable identities"

From Scott David to Everyone: +1 to Bill. Did Zillow help?
From Jeff Orgel to Everyone: Dissolving IDs, yes. Like in real world. When we walk out we vanish - mostly. Like a random store experience...
From Kaliya Identity Woman to Everyone: nope
From Tony Fish to Everyone: have added them into the doc
From Doc Searls to Everyone: that's a bummer.
From Kaliya Identity Woman to Everyone: I don't know what they did you can't save the chat or at least I couldn't you can screen shot them?
From Tony Fish to Everyone: @kaliya - done
From Doc Searls to Everyone: screen shot is way too hard, especially when the whole chat is 10 feet long.

KERI for Mudbloods /Key Event Receipt Infrastructure (A more advanced Session following KERI for Muggles in Session 2)

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:

See slide deck here:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI2_Overview.web.pdf

User Managed Access - 101 Session

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

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

Presentation slides can be found here:
https://kantarainitiative.org/confluence/download/attachments/17760302/2020-10-20%20IIW%20UMA%20101.pdf?api=v2

Build an SSI Proof of Concept (30 minutes or less - code optional)

Tuesday 3C
Convener: Riley Hughes, co-founder of Trinsic
Notes-taker(s): David Schmudde

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

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

Trinsic: verifiable credentials and self sovereign identity

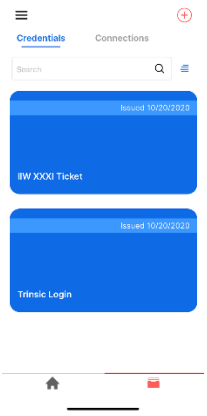
SSI:

- Like Apple pay for everything else.
- Verifiable credentials: Issuer → Person → Verifier
- As long as the verifier trusts the issuer, then it all works
- Trinsic is a platform for all the participants in this system

The underlying technology Trinsic uses is based on Hyperledger Aries.

Trinsic has 3 different APIs. You can build business logic into your application

- Credentials API
    - The most standardized component.
- Wallet API
    - More unique to Trinsic
    - Allows you to create cloud agents for holding credentials
- Provider API
    - More unique to Trinsic
    - Allows you to create cloud agents for issuing credentials



Q: Are there any rate limits to the number of verified credentials issued?
A: The price is usage based.

Goto Trinsic Studio and signup (https://studio.trinsic.id).
Sign up with a credential.
If you want to experiment with the provided IIW token, note that there are two different credentials:

1. A Trinsic credential to login
2. The IIW token

Build an SSI proof-of-concept. First click here.

- Create two organizations on the Sovrin Staging network.
- When you create an Organization in Trinsic, you're creating a cloud agent hosted on a dedicated tenant in the Trinsic platform **capable of issuing or verifying credentials**. This Organization also gets a public DID on the network it's provisioned on.
- The three players: **college** (1st org) → Alice → **job** (2nd org)
    - Create a credential template in the first organization (**college**). There will be a 1-3 second delay while the template is written to the ledger. It should show up here.

    - In order to accept a digital credential, Alice (you) will need an agent. Download the Trinsic Wallet to your phone. The college should issue the credential

Bringing Emerging Privacy-Preserving Technology to a Public Health Crisis - A Case Study of the COVID-19 Credentials Initiative

Tuesday 3D
Convener: Lucy Yang (lucy.yang1030@outlook.com), Kaliya Young, John Walker (jwalker@semanticclarity.com)
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:
Verifiable credentials, COVID-19, public health crisis

Article by Kaliya Young and Lucy Yang on the challenges CCI has encountered as a grass-root community: https://medium.com/@cci.2020/the-covid-19-credentials-initiative-cci-b00c1d858ccb

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

- General - this session is being recorded.
- Link to the deck of the session: https://docs.google.com/presentation/d/1Nr6ECAiwD-aBwND8dYNHwM0PWElje2E7zgAIdHOVMuE/edit?usp=sharing

Articles referenced:
CLEAR article: https://link.medium.com/hhj3wLkxDab
DHS articles: https://www.dhs.gov/news/2020/08/26/weekly-update-dhs-response-covid-19
https://www.dhs.gov/science-and-technology/news/2020/07/27/news-release-st-releases-solicitation-address-emerging-covid

MS article: https://didproject.azurewebsites.net/docs/verifiable-credentials.html

Links:

- The COVID-19 Credentials Initiative (CCI) Website: https://www.covidcreds.com/
- CCI Newsletter Archive: https://us10.campaign-archive.com/home/?u=1e21ad08ed0422a5dac0b8eed&id=ebe791efe9
- CCI Twitter: https://twitter.com/CCI_CovidCreds
- CCI Use Case Implementation Group Page: https://docs.google.com/document/d/1dbWvs1m8uziTsbhUQv_nPofTXAyDSkxI5CZtoo1SlRY/edit?ts=5e85430a#heading=h.8oej31ec0two
- CCI Governance Group Page: https://docs.google.com/document/d/18ImvPqTxKsqaqhX8_pIXxCq1p1xmHqfO0vo-OzSbBl8/edit
- Article about CLEAR's solution https://link.medium.com/hhj3wLkxDab
- OP-Ed Published by Alexandra: https://calmatters.org/commentary/my-turn/2020/09/legislation-offers-solution-to-safely-store-covid-19-testing-data-critical-information/

Session feedback to the challenges that CCI has faced: (see slides)
How can we remedy these challenges ?

Todd from ID2020 - Chief Architect
The editorial content and voice from the community should be provided to strengthen CCI's message.
Create positive, "carrot" approaches.
Solution around Travel getting press in the NYTimes - its a big part of the use-case.
Todd could support developing an editorial rebuttal to the NY Times article.

Phil Wolff - CCI should / could reach out to professionals who advocate to the Government and Health IT vendor community.

ACTION ITEM coming off this call - one or more groups to write open editorials and seek to get them published?

Most of CCI is startups in small organizations, how do we gain visibility?

Phil Wolff - CCI should / could reach out to professionals who advocate to the Government and Health IT vendor community.

End of the day CCI has to represent open standards
NOT credentials from any one solution - solutions CCI supports needs to be usable cross venue.

Work with interoperability groups - "who's wallets can you read, from who's solutions?"
If they have the connections they don't need VCs or privacy preserving. In the context they have the contacts.

Q: How to package something ready to go?
Q: Has the committee's results been proven?
Q: Could we develop: (from Kaliya)

- Model policy for governments?
- Model RFP language for governments?

Responding to the model policy creation question : Alexandra Medina

Principles named in the AB 2004 Bill that needed to be flushed out.

Security
Privacy
Portability
Interoperability

Represented the Blockchain Advocacy Group

- Worked with ID2020 folks on language, got Verifiable Credentials Bill passed in California. Excited about the applicability for other things besides COVID.
- Unique opportunity to get the state to start thinking about it.
- Has gotten op-ed published.

CCI could pattern it's work based on Uniform Law Commission

Which works for state governments.
AB 1489 - 80 page policy on Crypto. Written by lawyers
ALEC - gets language in.
Jurisdictions States like to have standard language
Reciprocal model - for states to recognize

Vishal Gupta: Indian government is going forward with a centralized model for COVID tracking.
We need to get privacy concerns heard right now. COVID problem is giving an unforeseen power to governments. They are grabbing it and side stepping privacy regulations.

DEVELOP PRINCIPLES….then model language…

Kaliya: The JSON-LD ZKP BBS+ provides a lot of hope to address the issues you are naming most of the community is excited about it as a new baseline that meets everyone's needs.

Created an initial draft
Larger business, smaller business - another organization.

Q. Can we build our own competency for advocacy?
Q. is the community committed to sticking with this project even if we miss this pandemic? to be ready for the next one?

Public health is the ongoing framework for CCI to work 'within'

There was a DHS request for proposals RFP - Tom Jones reference
https://www.dhs.gov/science-and-technology/news/2020/07/27/news-release-st-releases-solicitation-address-emerging-covid

Tom Jones - Kantara reference

There are two kinds of lists:
Aspirational manifestos. We want privacy.
Thou shalt…
Acceptance tests. You know it's minimally acceptable when…
Thou shalt not… Thou must…

DHS SVIP has asked for information re: COVID
https://www.dhs.gov/news/2020/08/26/weekly-update-dhs-response-covid-19

> The Department of Homeland Security (DHS) continues to work with partners across both public and private sectors to execute the Whole of America response to COVID-19 and ensure the challenges we face during these unprecedented times are met. Our partners at the DHS Science and Technology Directorate (S&T) have worked diligently with our private sector partners to find creative solutions to those challenges, while carrying out the mission of DHS to secure our homeland.
> "When it comes to security and safety issues, the government doesn't always have all the answers, which is why S&T works with the private sector to find technology solutions to the nation's toughest challenges," said William N. Bryan, DHS Senior Official Performing the Duties of the Under Secretary for Science & Technology. "S&T's Silicon Valley Innovation Program has reached out to the innovation community seeking technologies that can help DHS and the nation in this battle against COVID-19. We are seeking solutions to ensure the security of data in contact-tracing apps, automatic disinfection of surfaces, and tools to deconflict available information about the virus. Our National Urban Security Technology Laboratory in New York is conducting a market study on non-invasive febrile temperature screening technologies for the responder communities. Meanwhile, our studies are continuing at the National Biodefense Analysis and Countermeasures Center to characterize and learn as much about the deadly virus as possible, so that efforts to combat this disease are effective in protecting people, not only across the nation, but around the world."

Q. Who isn't in the room that should be?
Phil Wolff - regarding CCI gaining the interest and interaction with larger Government, Public Health, and Health IT organizations with potential interest in CCI.
Their solution buying and evaluation criteria are:

"What do you buy off the shelf?"
"Where is the kit to do your pilot?"

"Test your assumptions to widely deploy with low risk."

(Is the vendor or solution) "We aren't prepared to help people manage those risks."

"Buying from the "crisis bucket"
OR
Buying from the sweeping technology - choice affecting everything.
"Yes" decision dependent on doing everything well.

CCI - Don't know if we can make claims that these third party vendors are ready as business let alone buying

Better DID Methods with Zero Knowledge Proofs (ZKPs)? - privacy preserving, globally verifiable DIDs

Tuesday 3E
Convener: Rouven Heck, Martin Riedel
Notes-taker(s): Oliver Terbu

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

PDF Slidedeck:
https://drive.google.com/file/d/1Q8OGjdO8MOS7wsC2CiMVA-J_9mpfwSJk/view?usp=sharing

Chat-Log:
David Huseby: 😂
Oliver Terbu: Pls raise hands if you have questions
David Huseby: too many fucking did methods; most will never be used
Tobias Looker: Haha too true
David Huseby: running a universal resolver is way too hard
mitfik: 77 is not a lot ;)
Oliver Terbu: We have so many, so I need to create a new to rule them all
bsuichies: Is there a link to this presentation?
mitfik: but so true and hoping that KERI would solve that by going into did: without need for a method
David Huseby: any ledger that requires significant resources to be able to resolve DIDs against them are no better than a corporate identity silo
Oliver Terbu: @bsuichies: yes, will be provided
bsuichies: thx
Tobias Looker: IMO the DID method registry is more of a social tool, to get people thinking about the same stuff together in one room
mitfik: KERI is blockchain is DLT less :)
Kyle Den Hartog: "BuT HaVinG mORe DiD MetHOds MaKeS thEm MoRE DeCENtrAliZeD"
David Huseby: there will be one did methods everybody will use because it will have preferential attachment; like how google won From By_Caballero: ^ :(
mitfik: KERI is globaly verifiable is matter of witnesses around
bsuichies: did:ftw? From By_Caballero: did:wtf
David Huseby: the cost of supporting another did methods will be enough that implementors of VC systems will only support one, maaaaybe two.
balazs (DIF): fair point
David Huseby: and they won't be any methods that require running a full blockchain node
bsuichies: @david: define implementors of vc systems
David Huseby: so not bitcoin. not ethereum. not Indy. not any shitcoin. Any engineers building systems that accept verifiable credentials/containers for authentication/authorization
bsuichies: @rouven someone is stealing your furniture! From Tobias Looker: Hahaha
David Huseby: for example a covid credential checking device+system for airport security
bsuichies: verification or issuance? or both?
David Huseby: both
Oliver Terbu: Airport security will use digital travel creds (DTC). I was just on a call where ICAO presented that.

David Huseby: the VC economy is about accepting VCs and then monetizing credential issuance; @Oliver there is no winner yet
Oliver Terbu: I know
David Huseby: I know of at least six different efforts that have different levels of government and corporate support
Oliver Terbu: ICAO issues passports; Ok, not ICAO
bsuichies: so if keys remain in hardware, wallets are going to be the critical element.. seems pretty difficult in an open standards, interoperable world
Ryan Faulkner: keys remaining in hardware will have implications for portability :/
bsuichies: yeah, we're basically back to individual apps and siloes
By_Caballero: yeesh
Nader Helmy: yeah that's a difficult one. rotate everything everytime you move?
By_Caballero: MPC and threshold signatures, easy! <ducks>
bsuichies: how is an issuer going to prevent issuance to a wallet that he does not approve of, if the wallet is properly interoperable
Dan Bachenheimer: ICAO issues ePassports and will issue DTCs; they both require a centralized PKD and they both can be used to create a derived credential; specifically, a verifiable credential
Nathan_George: My device management and message routing shouldn't be my peer's concern
Charles Cunningham: Keris rotation model would allow you to rotate and identifier to another hardware module, so to say, by rotating to the keys within
Oliver Terbu: ICAO standardizes passports through ISO and provides guidance/regulations. The countries are issuing passports.
By_Caballero: your freedom to swing your fist ends at my security needs and nose, nathan
camparra: Shouldn't you also be adding changing crypto algorithms for keys?
Oliver Terbu: My hope would be that they choose VCs as their DTC containers
balazs (DIF): that would be HUGE! @oliver
Nader Helmy: +1 Charles, I think the difficult part would be enforcing that on a policy level as well as technical one, and do so in an interoperable way
bsuichies: zero-trust wallets
Nathan_George: @By_Caballero my point is that device rotation and message routing can be strongly correlating, I need the ability to limit that leakage, but yes, you still need to know "it is me", but granularity beyond that is dangerous to the entity model
camparra: Eh that's cool and all but you have to be able to upgrade crypto
Dan Bachenheimer: ISO standards wrt ICAO define air interface protocols, security, and biometric quality
camparra: KERI doesn't do that
By_Caballero: @Nathan, I was kidding, but your clarification was super useful, thanks!
camparra: Nor do most wallets
Oliver Terbu: @Dan: yes
bsuichies: Observation: in the physical world the wallet is not secured, and the credentials and tokens are secured
bsuichies: that's pretty scalable. and portable
Kyle Den Hartog: For encryption keys we could use the tree-kem structure being developed for MLS to agree on a symmetric key, but that's a rabbit hole for another day :)
Andrew Whitehead: treekem does seem nice, especially for smaller groups
camparra: That's assuming symmetric key encryption will forever hold it's security @kyle
Kyle Den Hartog: Symmetric is unlikely to be broken by quantum computers because most ciphers are just one-time pads with a way to consistently expand the key
bsuichies: @kyle: 5 dollar wrench
Kyle Den Hartog: The unsolvable problem best left out of scope

bsuichies: :)
Tobias Looker: Yeah lots of the ZKP's schemes have a massive amount of public parameters required on setup too
Tobias Looker: Which is something that many people tend to ignore the complexity it introduces
Oliver Terbu: @David: could you pls lower your hand
David Huseby: yup
Oliver Terbu: ty
By_Caballero: ^FFR I believe multiple people can claim host simultaneously, and hosts can lower people's hands for clarity of queue :D
Oliver Terbu: :)
By_Caballero: but then you can't raise your own hand, which gets complicated if you're an opinionated host :D
David Huseby: still not scalable ;)
Oliver Terbu: Ack jonathan
Rouven Heck: Not on Bitcoin ;)
David Huseby: true. ; I keep coming to the conclusion that bitcoin is only useful for two things: 1) storing data that cannot be changed by governments/corps and 2) a cryptographically secure source of "not before" time stamps for things like non-revocation proofs.
mitfik: why Bitcoin and noth Eth? or overall permissioneless ledger ?
Jordan McKinney: All of which (and more) can be done on Ethereum
Oliver Terbu: +1 eth
David Huseby: incentive structures are different
mitfik: so you saying that Bitcoin have the "best" incicentive ? ; for that specific purpose?
David Huseby: no. but bitcoin is simpler. that's more attractive to me for security things ; I don't know which incentive structure is better.
Jordan McKinney: Imo bitcoin security is long-term unsustainable, which is a problem
David Huseby: I'm not a bitcoin shill. not going to argue for them. not sure I understand how you can to that conclusion tho ; how you came to that conclusion...
Jordan McKinney: https://medium.com/coinmonks/bitcoin-security-a-negative-exponential-95e78b6b575
I wrote several posts on the issue ^ ; That's the first ; Tl;dr hard cap on issuance means all miner revenue has to come from fees which are much lower, less certain, etc
By_Caballero: breaks are optional-- something tells me this group is gonna stay until the bottom of the hour and have to be hosed down like rabid dogs :D
Oliver Terbu: yep, 3 slides left, then we could use the remaining time for all the rabbit holes :)
By_Caballero: sorry, i think I just had a stroke when martin said "recursive"
John Hopkins: What are some of the active implementations?
Kyle Den Hartog: Loopring has been working on one for DEXs ; It's not DID focused, but does build on the ZKRollup structure ; This zksync? https://github.com/matter-labs/zksync
Steven Wilkinson: https://minaprotocol.com/docs/snapps
Kyle Den Hartog: Has anyone looked to build a smart contract with go then? ; At least that you've heard of? ; Sorry, not with go with Hyperledger fabric and chaincode ; Thinking about it in the case of securekey
Oliver Terbu: I guess we don't need the raise hand feature anymore
John Hopkins: quick clarification on terminology when we say rollup, do we just mean any sort of layer 2 network?
Rouven Heck: please ping us - if you are interested to follow up, or want to discuss anything in more detail in futures session: rouven.heck@mesh.xyz ; martin.riedel@mesh.xyz
Jordan McKinney: I believe "rollup" is a specific method of taking a large collection of transactions and created a proof that sort of "contains" all the transactions in a compressed way. The transaction data is not

actually contained in the roll-up, so I don't mean a literal compression. The act of collecting tx's and creating the rollup can all be done off-chain though, so that is essentially layer 2 and chain agnostic I think
01:18:21 By_Caballero: :flex emoji:
01:18:54 By_Caballero: whoa john is calling from another room in rouven's house
Kyle Den Hartog: Vitalik " ; "The etheream guy" ; ethereum*
Tobias Looker: Thanks guys cool proposal!
Jeff Orgel: Thx!
Tobias Looker: Do you have a link to the slides?
Kyle Den Hartog: Yeah seems like a cool proposal
Michael X Shea: thx~
Oliver Terbu: Yes, will be provided in the notes
Tobias Looker: Thanks!
balazs (DIF): Thanks!

Exploring Governance Frameworks - Practical Approaches

Tuesday 3F
Convener: Dev Bharel @spacemandev and Sam Curren @TelegramSam and Alexis Falquier @Alexis-Falquier
Notes-taker(s):

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

Sam Curren Links:
https://github.com/hyperledger/aries-rfcs/pull/535/files?short_path=680f278#diff-680f278fc55f6306f095c49725b22acae9fc6cba653a94f55d508c8d0f18e7bb

https://github.com/hyperledger/aries-rfcs/pull/530/files?short_path=02a1424#diff-02a142404d8bbfcb15486ff5bd27a1968bcf1e054d42a09f42d2de8df5e0e6be

https://github.com/hyperledger/aries-rfcs/pull/550/files?short_path=54746f6#diff-54746f6fb053443ea5844d2eeb4e38bdf81616354bca3821ff1600f4032ee740

The governance frameworks have interesting application in both issuance and verification.

Currently the emphasis has been on the governance of issuance and whom to trust.

The GlobalID management of trusted issuers using GlobalID groups is an innovative approach to providing software to manage the groups of trusted issuers.

Expression of the framework and particularly its application to presentations are topics for further discussion.

PBAC 101: Four Pillars of IAM, History of Authorization, and What is PBAC?

Tuesday 3J
Convener: Jacob Siebach
Notes-taker(s): Jacob Siebach

Tags for the session - technology discussed/ideas considered:
Authorization management, authorization attributes

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

There are four components of what is commonly called "Identity and Access Management":
* Identity Management - IDs can be for people, systems, devices, etc.
* Authentication - The process of determining with reasonable certainty that the ID is who they purport to be.
* Access Management - Manually provisioning IDs to have some capabilities within a system.
* Authorization - Answering the question, "Is this ID authorized to perform this function on the given target?"

All data within a domain should be protected by policies. Policy-based authorization allows the business owners of a domain to write policies that utilize data and attributes to govern who is authorized to execute actions in the domain.

The authorization engine sits external to the domain. When a user attempts to execute a function (view data, update a file, etc.) then the domain service calls the authorization engine to get a decision. If it is "permit", then the domain moves forward. If it is "deny", the domain does not execute the function.

A domain may call the authorization engine multiple times in order to gain the required level of authorization (Step A requires x, then with that authorized, they do something for Step B and the engine is invoked again to see if they have authorization for the thing that they were trying to do.)

Authorization should be decoupled from domain business logic. A proper engine should be able to tell you where an attribute is used (i.e. what policies) and what the user is authorized for.

Business owners set the policies. Figuring out the policies is something that needs to be done irrespective of the technologies used to implement it. It is often difficult for people to agree on what policies should be required and what the definition of an attribute should be.

More to follow in tomorrow's session.

Notes from the chat
Andre Kudra To Everyone 1:41:51 PM And the next big thing: Credential-based Access Control
Kristina Yasuda To Everyone1:56:26 PM using VCs as access tokens?
Andre Kudra To Everyone1:59:22 PM Kristina, we are using user-disclosed attributes out of VCs
So the VCs are just the containers of the attributes which we are using to take an authentication or authorization decision.

Cross-platform Rendering and Rich Selection of SSI Credentials

Tuesday 3M
Convener: Horacio Nunez (horacio.nunez@kiva.org)
Notes-taker(s): Horacio Nunez

Tags for the session - technology discussed/ideas considered:
Credential Representation of SSI Credential

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

Credential Representation of SSI Credential

Key Understanding:

Is important for the User to see a representation of their credentials. Is also important to ensure that the representation is informed by the entity that issued the credential.

Except a universal representation to serve as UX backup.

There is a consensus that a subset of SVG can provide two solutions well.

1. A machine readable way to describe the credentials representation.
2. Provide a reliable rendering across well known platforms (mobile, web and desktop).

There is also a consensus that is probably not a good idea to increase the footprint of the credential definition metadata. But instead will be interesting to explore a hashlink to ensure an agent can fetch representation metadata along with saving a credential in your wallet.

Another interesting idea was to rely on a globally available representation authority to list this definitions so they are accessible

As per action items:
The convener of the session will factor in some of the feedback to articulate an RFC, and several attendants will explore some of the technical challenges with implementations.

The next step will be to combine these efforts into a spec for the greater community and a reference implementation.

The Past, Present, and Future of Indy Network Monitoring

Tuesday 4A
Convener: Lynn Bendixsen (lynn@indicio.tech)
Notes-taker(s):

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

Slide Deck of Presentation: Past, Present, and Future of Indy Monitoring .pptx

Current effort is being done on collaboration towards improved Hyperledger Indy monitoring.

https://github.com/hyperledger/indy-node-monitor

https://github.com/hyperledger/indy-node-monitor/pull/18

https://indymonitor.indiciotech.io/

Briefly covered the history of Indy network monitoring, then described the current collaborative efforts by people from around the world. Lynn showed the pieces that he has pulled together from different contributors to build a "Proof of Concept" around Prometheus/Grafana and then Lohan Spies showed the work he is doing to provide a similar proof of concept using Splunk. The main goal is to provide as many different exporters as we can so that end-users can incorporate Indy monitoring into their existing systems. Other work towards Indy Ledger monitoring being done was also presented by Will (wip).

Future effort can focus on:

1. Notifications and alerting (what notifications? Where in the pipeline should we catch the issues?) It was determined to use the mechanisms in the tools we already have to do initial alerting, but a cool idea (later) might be to move the threshold checking lower to catch and disseminate information earlier in the pipeline.
2. Ledger monitoring
3. Performance metrics

Questions asked (some were answered)

a. What about the business aspects of monitoring? What questions do we want to answer with monitoring? SLA's can be backed by actual data, instead of just being a "wish list".

b. Should we really provide all of the information we have publicly? Perhaps some of the info should not be shared, maybe we need to separate "admin" type monitoring from "public" viewable items.

SSI and Decentralized Identity (101 Session)

Tuesday 4B
Convener: Karyl Fowler @TheKaryl, Juan Caballero @by_caballero
Notes-taker(s): David Schmudde

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

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

Two major tracks

Less Identity	Trustless Identity
Legally-enabled self-sovereign identity Many governments want less data (e.g. so the post office doesn't know your tax records) Key characteristics: • Minimum disclosure • Full control • Necessary proofs • Legally-enabled	"Trust Minimized" identity Key characteristics: • Anonymity • Web of Trust • Censorship resistance • Defend human rights vs. powerful actors

- Most identity today is centralized identity
- Federated identity bridges the silos
    - Convenient
    - But masses more control through the provider your routing your ID through

Problems

- Who owns your data and how can it be used? This varies based on geography. This is a fundamental problem on the internet.
- Users can't control their data
- Single points of failure are honeypots
- Businesses don't want the liability of all the personal data to manage.
- Data isn't very portable.

DID allows the individual to reassert control

- *Verifiable credentials*: like files but with granular controls baked in. Like a "shipping container rather than a data silo
- *Universal resolvers*: "mini-DNS" can function as local namespaces (or not)
- *Secure data storage*: "lockers/vaults"

- *Verifiable credentials* (VC): is a set of tamper-evident claims. They are more standardized than the myriad of different DIDs. Shipping is one example where VCs are used, where multiple people must sign off when receiving the correct cargo.

Framework for adoption

- Is selective disclosure or privacy a priority?
    - Healthcare
    - Data infrastructure and governance

Deck Link: https://github.com/decentralized-identity/decentralized-identity.github.io/blob/master/assets/knowledge-base--october-2020.pdf
Cross referenced w/ a Day 2 Session on the Principles of SSI

***Lightly-Redacted* Chat thread w/ links (submitted by… anonymous? Can't remember, sorry):**
From Sergio Mello to Everyone: ...or you could use a smart card by Tangem ;-)
Karyl Fowler to Everyone: True^
From Ivan Temchenko to Everyone: https://play.google.com/store/apps/details?id=com.jolocomwallet
Karyl Fowler to Everyone: shameless demo plug re: Tangem and Transmute - https://nfc.did.ai/tangem
From Sergio Mello to Everyone: more shameless promotion: get a free pack of Tangem SSI Beta cards.
From bengo to Everyone: Let the market decide the business model
From Markus Sabadello to Everyone: On the Internet, nobody knows Johannes is taking care of his dog…
From bengo to Everyone: podcast name?
Karyl Fowler to Everyone: This Machine Kills
From bengo to Everyone: (5:04 PM) ty
Karyl Fowler to Everyone: https://soundcloud.com/thismachinekillspod
From Dan Robertson (he/him) to Everyone: What's the name of "Alex's podcast" that was mentioned earlier? SSI MEETUP Alex Preukschat **(it's a video webinar series, technically)**
Karyl Fowler to Everyone: https://medium.com/decentralized-identity/decentralized-identity-meetings-for-the-apac-region-7221b9aad29
From bengo to Everyone: https://mediciland.com is A 'green field' business model affecting places like Africa. The problem is... just because there is a business model there doesn't mean it's ethical. One country's citizen's international business model is another country's inhabitant's colonialism.
Karyl Fowler to Everyone: excellent point. another use case where ethics are of utmost consideration ahead of implementing Verifiable Credentials or DID tech in the current covid crisis: https://ethics.harvard.edu/immunity-certificates
From By_Caballero to Everyone: https://hackmd.io/t1cotiReTXCnkpDG8k2tVA

VC Revocations, On and Off Ledger

Tuesday 4D
Convener: Gabe Cohen, Rory Martin, Lio Lunesu -- Workday

Tags for the session - technology discussed/ideas considered: VC, Revocation

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

Spec draft hosted at https://workdaycredentials.github.io/specifications/
Other relevant specs:

- https://hyperledger-indy.readthedocs.io/projects/hipe/en/latest/text/0011-cred-revocation/README.html
- https://w3c-ccg.github.io/vc-status-rl-2020/

Zoom Chat
From bsuichies : #security
From Lio Lunesu : Spec's at https://workdaycredentials.github.io/specifications/ (draft)
From Kyle Den Hartog : Gotcha thanks
From Paul Bastian : not with anoncreds
From Oliver Terbu : Anoncreds are not w3c compliant
From Dmitri Zagidulin : sorry forgot was muted!! :)
From Stephen Curran : ZKPs are W3C compliant.
From Oliver Terbu : Looking forward to see bbs+-based w3c-compliant creds with domain proofs :) ;
@Stephen: is there a implementation of anoncreds that use the w3c vc data model?
From Denys Popov : list : 2020
From Dmitri Zagidulin : bitmapped list
From Stephen Curran : Evernym did a hack using anoncreds, but I expect that it will be BBS+ ZKPs that will get us to W3C
From Dmitri Zagidulin : +1 oliver
From Oliver Terbu : BBS+ will unite all communities :)
From David Huseby : Oliver is onto something ;)
From Dmitri Zagidulin : stephen - possibly a misunderstanding
From Oliver Terbu : Agree with stephen
From Oliver Terbu : I am wondering how we could use credentialStatus with non-membership proofs generated by the prover
From Oliver Terbu : (Which I guess is the right way of doing this)
From Mahesh Balan : IS this an alternate scheme to Hyperledger Indy revocation using cryptographic accumulators ?. Sorry, I am new to this, forgive me if it is a stupid question - https://hyperledger-indy.readthedocs.io/projects/hipe/en/latest/text/0011-cred-revocation/README.html
From Kyle Den Hartog : Yup, this takes a different approach with different tradeoffs.
From Oliver Terbu : Is it possible to define a credentialStatus method (for revocation) that requires additional info from the domain proof to be verified?
From Oliver Terbu : (The domain proof would get provided by the VP)
From Paul Dunphy : encrypted data counts as pseudonymisation under GDPR
From Oliver Terbu : Pseudonyms are PII
From Paul Dunphy : Yep
From Michael X Shea : agree

Moving Trusted Data across Untrusted Parties in Global Supply Chains

Tuesday 4F
Convener: Margo Johnson (Transmute),Paul Dietrich (GS1 US)
Notes-taker(s): Guillaume Dardelet (Transmute)

Tags for the session - technology discussed/ideas considered:
Verifiable Credentials, Supply Chain

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

GS1 and Transmute are working together to combine GS1 standards with verifiable credentials for trusted product data and answer

- How can GS1 help create trust that travels with the data?
- How might Digital link, VC, DID standards be leveraged to created business value related to product claims

What is GS1:

- 110 member organizations
- 2 million companies in supply chain space
- Governed by member companies
- GS1's goal is to develop the global language of business
    - Identity: GS1 standards for identification (**GLN**, **GTIN**, etc…)
    - Capture: GS1 standards for **Barcodes** & EPC/RFID
    - Share: GS1 standards for Data exchange (**GDSN, EDI, EPCIS**)

What is Transmute:

- Involved in standards organizations (DIF, W3C)
- Transmute secures critical trade data by digitizing key trade documents so that they are:
    - Traceable and verifiable
    - Instantaneous to access and share
    - Easily searchable and auditable
    - Impossible to forge

Product claims use case examples where VCs increase efficiency and reduce costs in supply chains

- **New product introduction**:
    - Increasing pressure from online marketplace for retailers to bring new products faster, and in a more trusted way
    - Currently a costly process: building relationships, paperwork, ...
- **Product Traceability**:
    - EPCIS events are emitted when a product moves along the supply chain
    - But parties in the chain don't necessarily want to share the events with all parties involved
    - Leveraging VCs for anonymity
- Many more, see slides

More details about the "New product introduction" use case

- The process of getting quality products on the shelves for sale
    - Retailer needs to receive authoritative data about the product and business

    - Brand is often not trusted to provide data for its own goods
    - Today processes are duplicative, expensive, easy to forge
- Planogram example:
    - Shelf space is a precious commodity
    - Product measurements coming from the manufacturer often cannot be trusted, and wrong measurements can be costly
    - Needing to hire an external third party to remeasure the products.

Product credentials work well together with brand credentials:

- GTIN / GLN will be identifiers for products credentials
- A brand can prove ownership of a GTIN / GLN with a brand credential (GS1 company prefix, GS1 GLN)
- GS1 is the root of trust: issues brand credentials to company members
- Trust flows from GS1, to Brands, to Retailers, to Customers that way

More details about the "Traceability" use case:

- Pharma traceability:
    - Need to show unbroken chain of custody
    - How did this pharma product move ?
    - Each holder of the product can issue a credential stating that they had custody of the product at some point
    - This credential can later be used as access to prove you are legitimate to see relevant EPCIS events

Verifiable Product Data considerations:

- Shared vocabulary:
    - GS1 web vocabulary
    - Traceability Shared Vocabulary (Early Draft)
- Identifiers for VCs:
    - Digilink URLs
    - DIDs: Decentralized Identifiers
- Credentials as authorization capabilities:
    - Proving legitimacy to access data and system

Q&A

Technical discussion around VCs and identifiers.

GS1 has an existing standard: GS1 digital link that provides URLs to identify companies and products, down to the batch or lot number. These URLs can be leveraged as identifiers in VCs.

OBADA: https://www.obada.io/

Zoom Chat

From Kaliya Identity Woman to Everyone: are you going to record the session if so claim the host
From Me to Everyone: think margo is planning to, providing no one objects
From Paul DIetrich to Everyone: Sounds great to me.
From Kaliya Identity Woman to Everyone: We have a note taker already - but if you want to join in you can :) ; Jonathan has his hand up
From drummondreed to Everyone: Drat. I only want to join silver bullet sessions ;-)
From Melanie Nuce to Everyone: +1 Drummond

From Tobias Looker to Everyone: Is the arrow the direction of the assertion? And does trust therefore flow in the other direction?
From Dave Crocker to Everyone: Chain of custody. No idea whether this relates adequately, but it might: The Authenticated Received Chain (ARC) Protocol https://tools.ietf.org/html/rfc8617
From Jim St.Clair to Everyone: We are building on use of VCs for authorization
From Tobias Looker to Everyone: This is awesome work! :)
From Orie Steele to Everyone: Thanks!
From Tyler @ Evernym to Everyone: Very focused application of VCs. I love it
From Bart Suichies to Everyone: where are the claims related to the products stored? And how are they linked to batch/unit?
From Dave_McKay to Everyone: https://medium.com/@rufftimo/verifiable-credentials-arent-credentials-they-re-containers-fab5b3ae5c0
From Jim St.Clair to Everyone: +1 Dave - semantic containers
From Orie Steele to Everyone: @Bart it depends, GS1 has a number of systems which can provide additional data, but obviously the claims can be embedded in the VC as well
From Tobias Looker to Everyone: The key with verifiable information is you don't have to trust where you resolve it from
From Neil Thomson to Everyone: Is a Social Insurance Number a credential or an attribute?
From Bart Suichies to Everyone: @orie: if they're embedded, where do they go? do they travel with the batch? or are they stored elsewhere?
From Jim St.Clair to Everyone: @Neil, an attribute. It may be one of several items needed for the verification
From Bart Suichies to Everyone: ie - do products/batches have wallets? or is it more lookup systems?
From Neil Thomson to Everyone: @Jim - and possibly just an identifier (sub-class of attribute)
From Bart Suichies to Everyone: got it, thx paul
From Karen Hand to Everyone: Good use case - is there any thought on the access or use of the VC's for organizations or businesses working with manufacturers or processors to increase their market access?
From Tobias Looker to Everyone: Haha here we go this session is going to pivot into a DID WG meeting!
From drummondreed to Everyone: Well, it's the perfect place to discuss 'type'!
From Tobias Looker to Everyone: :)
From drummondreed to Everyone: "Hilarious" is not the word I'd use for it ;-)
From Bart Suichies to Everyone: products have privacy rights too you know ;)
From Orie Steele to Everyone: 37371372312 === person GDPR violation!
From drummondreed to Everyone: GTIN gets richer as a Digital Link gets richer as a verifiable credential
From Jim St.Clair to Everyone: Not much, but here you go https://www.obada.io/ A good example of conflict metals too
From Orie Steele to Everyone: Yes
From Paul DIetrich to Everyone: thanks. Who was speaking about PICO
From Jsearls to Everyone: Joyce Searls

Chaining Verifiable Credentials

Tuesday 4G
Convener: Nathan George

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

Starting point for the discussion:
https://docs.google.com/presentation/d/1SgsdJkSPGeqQ2jxoH41v3RSSXIGJxCjdP3ptbygvq1w/edit?usp=sharing

Use cases discussed:

- See use cases outlined in the slides +
- Cited sources like in a news article
- Link to the authority's credential like this banking credential is linked to the proof that the bank is sanctioned or licensed.
- Common pattern that I need to be able to prove the credential that joins them but not allow use of the pieces individually
- Linking issued credentials to the evidence that issuing is based on seemed like a recurring pattern
- Educational credentials where you prove you have taken all the classes for a degree?

?When is it okay and not okay for linkages to cross issuer boundaries?

- Easy answer was that these linkages cross these boundaries all the time.
    - GS1 example of things crossing different organizations because of country-member organizations

Really interesting observation that linked proofs or presentations of credentials are not the same thing as credentials with linking attributes in the credential itself.

Multisig or providence wrinkles:
You want three parties to agree you live at a particular address, but you don't want to reuse the same proof from multiple authorities want three independent sources of proof.

Gathering multiple endorsers might also make a single proof more authoritative, so you would show that multiple members of the endorsement set approved.

A Regulatory Path for Digital Identity + A Jawful of the Lawful and the Awful.

Tuesday 4H
Convener: Chris Buchanan & Scott David
Notes-taker(s): Various

Tags for the session - technology discussed/ideas considered: Laws, regulations, identity, courts, standing, harms, exponential growth, BOLT reasonableness.

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

- Digital identity is NOT equivalent to physical identity due to the differences in mediums.
- No public space on the internet.
- Helen Neisenbau - Contextual Integrity
- Surreptitious user profiling - Maybe more clicks.

Chat transcript:

Ahoy, chat.
Chat, aye.
Anyone against recording the session?
slide three sounds like a list Doc Searls said.
Need new harms definitions
In the World Economic Rethinking Personal Data Project, we referred to "Declared/Observed/Inferred" Personal Data, which maps well to Chris' "Declared/Assessed/Inferred" distinctions.
Right-Duty-Breach-Causation-Damages-Liability-Insurance
Damages reflect social cultural norms.
Need to disambiguate identity and digital identity elements. Compare "This is not a pipe" painting (Magritte?)
The "quickly forgotten" is more a function of our human capability than a difference in models. There could be a worker at 7-eleven with a photographic memory and then it would be the same. Like a 1 to 1 scale map problem. Map is not the territory.
The "right to be quickly forgotten"
Yes @ George, but the scaling is different. not everyone has idetic memory.
NOTE TO HOSTS: CHAT COPYING IS TURNED OFF, SO WE CANNOT COPY TO NOTES.
@Lisa - yes I agree... though it's possible for digital to forget as well... it just has to be programmed that way
Our "identity" is more capacious online, and scaled for exponential increases in interaction volumes, but our identity cognition and institutions are not so scaled
Part of why digital identity and personal data have the affordances Chris outlines, is that we can learn many things in the digital world that we can't in the physical world by analyzing data about large groups of individuals to learn patterns and behavior of groups as they relate to individuals.
Symbolic - signet rings, seals, coats of arms....
Incommensurable: Not able to be judged by the same standard as something; having no common standard of measurement.
(thanks chris!)
I had to look it up. :)

it’s also a civil right
privacy is boundary management
Session Notes. Google Docs Document (1IHf…NWQ)
but you shouldn’t have to manage your boundaries at all times to have privacy. that’s too exhausting for everyone
yes, and rules
Plus many aspects of my "identity" are not mine to put boundaries around...
so making shared norms for boundaries whether you are on it or not, paying attention or not.. is key
Fascinating discussion, but very US-centric. Listening here from Melbourne, Aus and have lived in 9 countries. Perhaps look for a global view?
Do we have folks from outside the US in the room?
yeah, @george . in general i'm not a fan of "identity". prefer identification in many (most?) digital world cases.
^- agreed
@John agree
also the definition of "privacy" can be very cultural :)
identity == profile, seems like
This is a good piece on harm: thehill.com/opinion/cybersecurity/459427-privacy-law-needs-privacy-harm
To @john 's point... I'm not sure there is a consistent global view in this space
non-consensual authentication
This slide is VERY US centric. The EU context is quite different in that the EU has made an attempt to articulate, codify, and protect the the rights of the data subject / digital person.
Any reference, Marc?
Yep. US law is framing in this presentation. Lots of additional variables in multi-jurisdiction analysis! See OECD paper “Personhood”. (Approx 2007) which suggests “Hegel for personhood in EU and Locke in the US”.
Q+ (at end of presentation). Comment on memory being a part of identity
GDPR
@Heather - there is some interesting research happening in Deakin University's Cybersecurity team around the idea that the very way we select from what can (and should be) multiple choices to identify ourself - even in an SSI model - may identify ourself
The conflation of identity with full blown profile confuses me.
gdpr-info.eu/chapter-3/
@mark davis, you go next!
Ok great
Yep. Disambiguation of terms is needed.
Our definitions are part of our prior rhetoric which is not longer fit to draw together incommensurables.
Who gets to create profiles about me?
Our definitions are part of our institutions which are similarly no longer fit to de-risk interactions
Julie Cohen: “Privacy has an image problem.”
That is why need harms-based regime. Data is like “Dual use” technology. Don’t make hammers soft, but instead make hammers hard and make it illegal for folks to use hammers as weapons.
ted.com/talks/alessandro_acquisti_what_will_a_future_without_secrets_look_like?rid=WGQ0Ukdbx7HY
Data as surrogate for person because Hegel expression of self. In US - Mercantile culture.
+1 Marc

human rights violations are harms.
An interesting idea is to tax data ownership to incentivize companies to hold the set they actually need to sustainably provide services. I forgot who was working on this
Human rights are defined by humans. Might they need updating?
+1 on Chris' list of the new sorts of harms. There are also many others.
We've started trying to characterize and categorize digital harms here: me2ba.sharepoint.com/:x:/s/LivingDocuments/EcqGrfGY8qJEiioT-RpuNb4BxSIPpzWzWFl7nfTN1cbl8w?e=S1rfS4
which can be found in our resources page here: me2ba.org/resources/
Lisa - Does this include harms matrix stuff? Did I send that to you already?
You sent it David, we haven't done regulatory mapping
(it's still pretty rough)
We should combine those elements. Let's discuss later.
I think the GDPR should be an important consideration even for US orgs/companies for a range of reasons — international customer base of course, but GDPR is being used as a model for other data protection regulatory frameworks
To Heather's point: most personal data has JOINT provenance and therefore joint rights of control and use.
GDPR-like Fair Information Practice Principles already bind ALL government agencies which is a great starting point. That is from the Privacy Act in the 1970s which never applied to companies in the US, but grew to do so in the EU
But unlike copyright, where both can do whatever they want with it, jointly produced data about someone should have asymmetric controls .. where the one the data is about has more rights than the co-creator
+1 Mary
because of the civil rights associated
@Mary and human rights
yes.. and human
In the EU "Droit Morale" (Moral Rights) of artists prevent art purchasers from destroying or altering artistic works (I think that is like "data" which is not copyright protected, but is "expression-like")
In the US I can buy it and burn it
I gave a presentation many IIWs ago about the 12+ entities that could have rights to your personal location data
Transactions =interactions
Interactions with and among people, organizations and things
Consent matters.
Informed consent matters more.
Consent is surrogate for full negotiation, so negotiation matters even more
The only framing of this that makes sense to me is Helen Nissenbaum's contextual integrity
Helen is awesome.
Hate talking about identity
+1000000000 Kim
:)
I think Chris' point is that we need to disambiguate identity and the disambiguation is now even more expanded with the set of "digital" identity concepts.
Here is the personal location data right slide from 2013:
Faceting identity.
Is "attention optimized info delivery" just showing me things a server thinks I will like?
"Identity" emerges from interaction.

Contextual appropriateness and distribution norms from Nissenbaum
s/transactions/interactions/g?
an element here of ability to assert personal preferences
In the real world it's hard to "assert" personal preferences... it's more a choice of what I share or don't share
disagree.
VERY easy to assert preferences--e.g. eye contact/ vs. not
posture
Isn't it social norms that say how to interpret those gestures?
If all the slide 2 data (disclosed, observed, inferred) is part of my person, like an arm, that changes the framework from property to human rights.
yes
+1 to Jeff
+1 Phil
Everyone is a little bit right. Paradoxes (Paradoxi?) abound. That means there are lots of opportunities for meaning making in communities that are disadvantaged by the ambiguity and paradox. Good stuff!
+1 Heather yes US views digital identity and personal data as economic issues, not as human rights or civic rights issues.
Entropy engines are social/community structures that turn shared vulnerability/threat into “value”. Example is insurance
I’d be interested in hearing that Heather
That seems like a really interesting session. I'd be interested.
Agree Heather!
Yes, absolutely!!! US/Europe is very individual centric biases, vs collective centric bias (more eastern/asian)
Think of human rights (personhood) and civic rights (citizenship) that are a priori to their economic functions.
The advantages of being a tech luddite like myself — always live like you’re in 1981
Agreed, there are cultural differences where even the threshold for violations of privacy are perceived differently, e.g. WikiPedia article about Family register
Q. Is this conversation different under an authoritarian government?
Family registers are culturally perpetuated even in many highly democratic nations in east asia
It's a little unclear to me what "problem" we are trying to solve :)
or even just discussing
Me too.
I’ll restate it
Ah, i thought people were talking about different problems.
+1 @George — by calling it “identity” we make the ~problem~ too open ended
Heather’s session tomorrow: “99 identity problems”
right @judith we modulate
I to try very hard never to put the words digital and identity together - I find them meaningless
But Tom, that’s my job title…
:)
Change your title, that should be easy
Scarily well said Judith! I'm having visions of a creepy Borg thing!!
So well put @Judith re persona being profiled and digital footprint being aggregated
LOL Kim

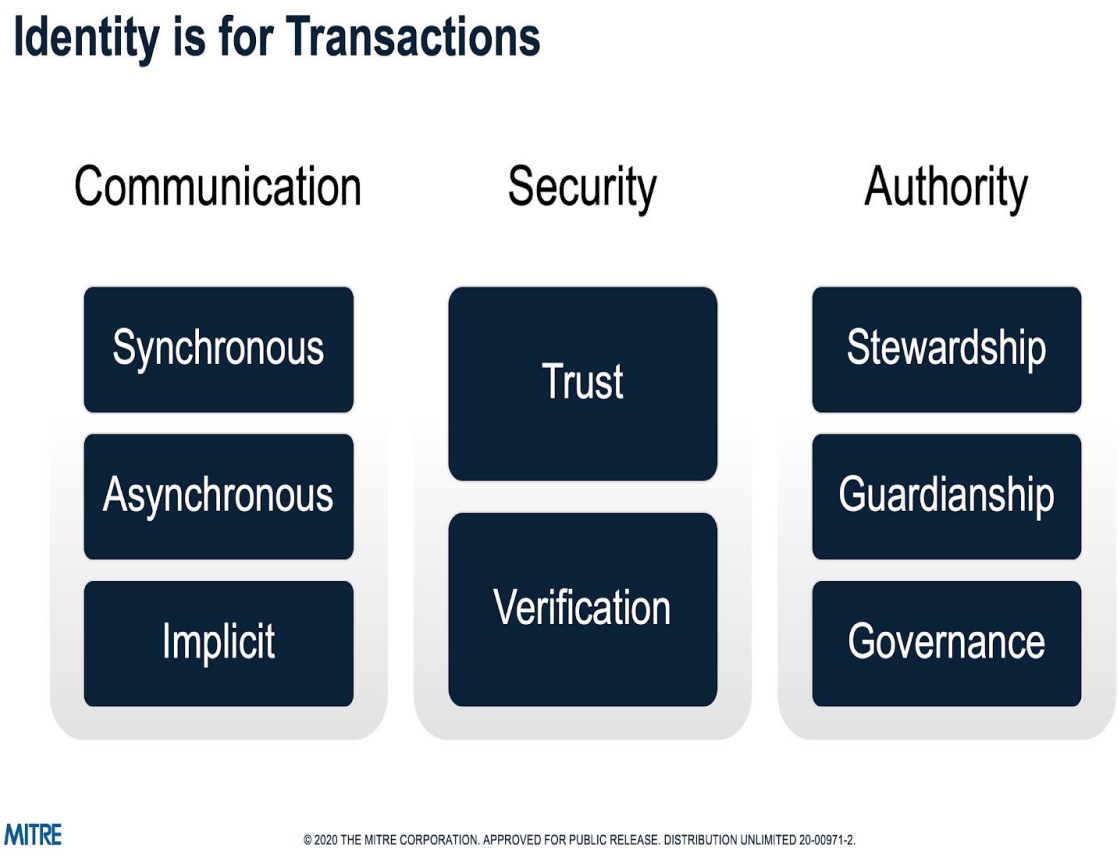
I like the focus on what to do about the “things platforms store about us that we can’t possibly consent to”
I remember a client that didn’t have to report under data breach notice statutes when thousands of paper identity files were stolen from a loading dock. Digital is a way of getting legislation passed in the 1990s.
I’m so happy to hear others revolting against that damn I word. Let’s fix this
A Hydra of myself ala AI Profiling!
Some the point about target was that the tracking was between the purchase of the folic acid, the frequent shopper card (for the discount) and the physical address that got the ads for pampers
You don’t live on line - why do you think you have any rights there?
We do live online, but there is no public space online, only corporate spaces. We are serfs working plots of land for the lords of the manor under Digital Feudalism, which is why a Digital Enlightenment is needed to assert, codify, and realize our human rights, civic rights, and economic rights in the online world.
Multiverse theory lives!
+1 well said Chris - about the Harm of Attention optimized information deliver.
TY
+1 Marc
YEs @Scott ! Imagine if there was a PUBLIC internet as opposed to our current corporate internet that supported our digital expression of our 1st amendment rights.
Thx Chris!
That's exactly what we're thinking about in ieee 7012
Also exploring a generic Legal Layer in the Me2BA
The psychology and sociology of identity?
The W&B right was to be let alone
Is there some other meaning in discussion here?
Attention optimization by personal choice, might be valuable…. but too often decisions are being made about what the optimization decision is being made for you not by what your request. That’s what hurts democracy.
Right to be left alone should be both the right not to be observed, and the right not to be bombarded. Input and output aloneness.
Lobbyists are everywhere!
@scott ... is it true in the physical world that we have a right to "not be observed" ?
Q. Do we have a list of fiduciary duties for a personal data 4th Party acting on your behalf?
In non public places
@George - only in private settings. Kind of like Nissenbaum’s “contextual appropriateness”
Ahh... I guess I more or less consider everything I do online as "public" :)
+1 Scott
Good discussion -thanks for the facilitating and for all who contributed your thoughts.
Rory has hand up
super interesting discussion, Chris. thanks for combining with Scott. rich discussion. are you going to include Chat in the notes?
If I can.
Identity integrity should not be a luxury. +1 to Rory
In the past, not everyone could own books so libraries brought books to everyone.
+1 George
Privacy is a human right. Selling personal data is like selling body parts.
+1
George

Imagine libraries hosting email of last resort
Is data the same as privacy?
@judith---oooh , interesting!
data is the stuff of privacy in the digital sphere.
What is the stuff of. Privacy in the analog sphere? Is it language, pictures (all photons?). Is it illegal to sell data or to sell privacy?
Whoa there the mdl gives you control of the attributess release - chis is wrong
data is the matter in the digital world @joyce
You do NOT need to give data to get high assurance
Fun discussion... thanks everyone... I have to drop
So data is the photonics equivalent of the boson self. Nice.
Photonic
Capitalism is not about protecting people, it's about protecting profits.
That is what Milton freeman said - corp are exclusively designed to make profits
We need truly public and truly private spaces online.
don't get me started on the sociopathy of freedman
:)
That is the idea of design patterns that came from Berkley in the real world there are public and private spaces
+1 Marc
Doesn't this then get us into a discussion on Safe Harbor and Section 230?
we were aquatic apes but - ok
Manatees?
I remember reading that book - I think is was debunked
The naked ape
WikiPedia article about Aquatic ape hypothesis
We lost our hair so we could swim
The HumanOS is designed to be VERY touchy feely Scott. +1
we are the only ones with subcutaneous fat.
Great convo all! LMK if you want to do the follow-up session tomorrow.
great discussion! thanks Chris and Scott.
Can you send us the chat, and the recording?
the chat is blocked
Thanks folks. Fun Discussion.
Yes, please add chat to the notes!
by folks thanks…I'm going to Demos.
how to invade
standards type use
but not wanting to work with big standard's body
so thinking of partnering 3 of them
I want to get you and yours involved in our social justice platform.
ok great
feel free t email
i don't think i have yours
Off to demos..thanks Chris, Scott, et al. for a great session!
but notaries get certified and annually re-up at state level
really great!
Just dropping back in to give appreciation, thanks for hosting the session! good discussion
Privacy is a 20th idea. We need agency and control and enablement over our digital selves.

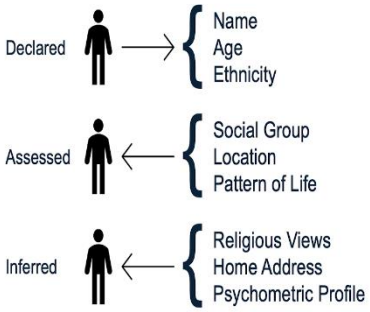
Here's a company that provides digital notary ayininternationalinc.com
Thanks everyone!

Scott:
Tempos are too slow.
BOLTS reasonableness: business, O, law, technology, socially
Synthetic intelligence.

Chris Buchanan slides:



Identity Described: Correlation as a Directed Graph



We have no rights to prevent others from assessing, inferring, or transmitting our identity information.

What is the harm?

MITRE

3

The Accumulation of Digital Identity Artifacts

Because digital identity lacks transience and degradation but has perfect retransmission, the accumulation of digital identity artifacts creates a window into psychographic and behavioral details for which **it is impossible to gain the conscious consent of the subject**.

- **Privacy is not about property.**
  - Soldal v. Cook County (1992)
- **The privacies of life must be protected against arbitrary power.**
  - Carpenter v. US (2017)
- **But… this is not a constitutional issue. It's an issue of standing (locus standi).**

MITRE

5

What is the Harm in the Accumulation of Digital Identity?

The intentional creation of an imbalance of power in the information domain which is utilized to consolidate power in the economic and political domains.

Specifically:

- **The surreptitious creation of detailed biographic or psychographic data regarding users or groups of users.**
- **The algorithmic biasing of information delivery for the purpose of monetizing users' attention.**
- **The tapping of biological processes without the consent of the user or against their best interests.**

MITRE

6

Combatting Accumulation with Regulation

Define identity data to include declared, assessed, and inferred identity.

Regulate

- *Transience* as temporal minimization.
  - Data may only be collected or kept if it is necessary for follow-on transactions with or on behalf of the user.
  - Only necessary data may be retransmitted to a third party.
- *Retransmission*
  - User must explicitly agree to any identity data retransmission.
  - Data may only be retransmitted to another entity *n* times where *n* is defined by the user.

Encode *Degradation* via differential privacy mechanisms

Outlaw

- Surreptitious user profiling.
- Attention optimized information delivery.
- Algorithmic manipulation of biological processes against user consent or user interests.

Limit the use of digital identity to transactional activities.

MITRE

Chris Buchanan
cjb@mitre.org
@MITREcorp
linkedin.com/company/mitre

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

© 2020 THE MITRE CORPORATION. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED 20-00971-2.

Privacy and Identity Considerations in mobile Driving License ecosystems

Tuesday 4J
Convener: John Wunderlich
Notes-taker(s): John Wunderlich

Tags for the session - technology discussed/ideas considered:
mDL; mobile driving license; privacy;

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

This was an introduction to a new Kantara Initiative Discussion Group: Privacy & Identity Protection in mobile Driving License ecosystems.

This discussion group arose out of work that Kantara is doing with the Secure Technology Alliance whose members are actively involved in the development of the ISO Standard for mobile driving licenses (18013-5). See the STA page on their mDL initiative here.

The framing for the discussion was that mobile driving licenses as an app on a mobile device is very likely to be the first widely distributed and adopted version of a digital wallet. The intent for the discussion group is to produce a report that will discuss the base mDL architecture and how it can incorporate privacy and identity considerations. This may (depending on the result of the discussion group and the contents of the report) lead to further working groups for conformance assessment and/or a report that makes recommendations for a specification. In short can we create a report that enables policy wonks and technologists to build self sovereign systems, verified credentials, decentralized identifiers and other ecosystems for interoperability with ISO compliant mDL ecosystems.

The following points were made:

- While the high level architecture of the mDL system involves an issuer, a reader, and a holder it does not conform to the tenets of SSI, especially disintermediation
- mDL ecosystems are not built for anonymous identifiers
- Interoperability with/between systems is a solvable engineering issue.
    - There is a defined data format that needs to be parsed
    - There will be multiple data types
    - Multiple engagement modes
- It could create problems to combine authentication and authorization in the same wallet
- Make it clear that driving licenses are issued by sovereign authorities, not self sovereign individuals.
- Need to understand what the likely secondary uses are
- mDL as a use case is misleading because it assumes capability on the part of the holder that may not be the case. There needs to be a way of delegation or ensuring agency.
- Discussion of the risks of attribute correlation
- There are concerns about presentation of the mDL as consent

My summary is that this community can absolutely enrich the discussion and help with the secondary use cases and considerations to develop mDL systems that meet the needs of the identity and privacy communities.

Closing / Open Gifting / Opening

Explore Personal Data Collection - LifeScope Digital Memory (Encore Thurs)

Tuesday 5A
Convener: Liam Broza, Dmitri Zagidulin
Notes-taker(s): Liam Broza

Tags for the session - technology discussed/ideas considered: LifeScope, SSI, OAuth, Solid, DID

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

Presentation

- https://docs.google.com/presentation/d/17gyhrpX24PuAiDMD3Cub1W2nP5OT9NckC6RwuSyCL0s/edit?usp=sharing
- Lifescope.io
- lifescope.io/xr

Action Items

- Partners
- Use Cases
- Technology
- (Identity, Collection, Storage, Encryption)

Liam Broza/ Data Architect, LifeScope Labs liam@lifescope.io

Dmitri Zagiduli/n Data Architect, Privacy/Trust/Storage, LifeScope Labs dmitri@lifescope.io

Minimum Device - iOS, Android, & SIM Card Free Participation in Modern Life

Tuesday 5B
Convener: Eric Welton
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

- Use cases for minimal device and accessibility
- Technical solutions and workaround for no-phoners, those who don't want to be tracked by govts, those who don't want to be tracked by data barons, etc

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

- Verifying hardware, open hardware

- Workaround for no-screens
    - Tangem/NFC + TEE
    - Voice print → biometrics (entails complex governance issue-- where is the hash stored?)
    - Protocol as workaround: a rasp pi, a tablet, a tangem card etc-- if it's protocol based, there's always a way around
        - "Protocol first"
    - Bluetooth has a man-in-the-middle problem (maybe NFC less so?)
    - Tangem card project
        - Shared phones, shared devices - may want NOT to have a phone, but a more private or a more durable storage (cold storage for VCs)
        - Control with one device to configure what it will show to next NFC
        - Proposal: Cloud-based system that could load a card with whatever i'll need to present that day :D
    - "Digital refugee" - non-voluntary digital
        - Will be discussed at a session tomorrow
- Legislative/regulatory recourse
    - "Anti-trust competition law and similar have broken up telcos, prevented mergers … that is probably the current answer. There are still 2 (Apple & Google). It that isn't enough, argue politically to apply anti-trust law to enable other O/Ss to succeed"
- TDA: Apps versus interfaces
- Certified devices -
- Attempt at a minimal set
    - Participant 1: Camera OR wireless comms (bluetooth or NFC, for ex?)
    - 2: At least 1 local **directional channel** (screen or camera) and some wireless comms device
        - Directional → confirm
    - 2: you have to be confident that you're communicating with exactly ONE device (NFC, camera, etc)
    - 0: Attestation?
    - 2: MITM
    - 3: HW Key + camera + authN (pin or bio)
    - 1: shortest software supply chain the better - crypto assurance shortens a lot
    - 2: [SW] assurance level may be implementation-specific
        - 4: double spend?
    - 0: bullet points
    - 3: HW key required for the use cases Kantara is working on-- all the other stuff seems like details to me?
    - 1: secure enclave and many HW solutions are useful only if you have assurance that keys can't leave device (sovrin IOT spec - theft issue, for ex.)
        - 2: that's a function of how COMPLEX the device is-- sometimes the simpler devices don't have as much concern for that (depends on directionality and comms context)
        - 0: a secure computing environment with a tiny bit of storage and minimal comms?
        - 4: directionality-- qRs are unidirectional, yes?

Links

- https://www.stiftung-nv.de/de/publikation/global-semiconductor-value-chain-technology-primer-policy-makers - The Global Semiconductor Value Chain: A Technology Primer for Policy Makers
- https://www.henleypassportindex.com/assets/2019/HPI%20Global%20Mobility%20Report_Final_190104.pdf - Henley Passport Index - mobility stats (what portion of each countries population has a passport)

- There is a working group of TeleTrusT, IT Security Association Germany, which produced a position paper on "Secure Platform", this is only available in German, though:
    - "Digitale Souveränität als Motivation für ein sicheres IT-Ökosystem in Deutschland und Europa" ->
    - "Digital Sovereignty as motivation for a secure IT ecosystem in Germany and Europe"
    - Paper website https://www.teletrust.de/publikationen/broschueren/secure-platform/
    - Press release April 2020 https://www.teletrust.de/startseite/pressemeldung/?tx_ttnews%5Btt_news%5D=1257&cHash=531dced6e3236ebb52634bec4f707d37
- https://www.nfcw.com/2020/10/13/368585/apple-files-digital-identity-credentials-patent/ is an article about the Apple patent I mentioned
- Apple US Patent Application http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=10&p=1&f=G&l=50&d=PG01&S1=(apple.AANM.+AND+20200702.PD.)&OS=aanm/apple+and+pd/7/2/2020&RS=(AANM/apple+AND+PD/20200702)
- Andre Kudra: I would also like to point you to what my Australian friend Paul Gardner-Stephen is doing in the space of low-tech mobile phones. He is a mesh network guru.
    - https://www.flinders.edu.au/people/paul.gardner-stephen
    - https://media.ccc.de/v/36c3-10800-creating_resilient_and_sustainable_mobile_phones
    - http://servalproject.org/
- This may be worth looking at:
    - https://www.trustless.ai

Intro Slides - introduction to session:

1. Slide 1
    - mobile Driver's License
    - mobile Health Records
    - mobile Travel Credentials

    Requires captive relationship with Apple or Google ecosystems in order to get basic life services, like drive to work, see a doctor, or travel to visit your family.
2. Slide 2
    - What are the minimum requirements for a handheld device
        - Made/Managed by authorized vendor (Apple, Google)?
        - Does it require a touch screen or just a display?
        - Does it require a SIM card or is Wifi ok?
        - Does it require a TEE – what are its requirements
3. Slide 3
    - Bring Your Own Device
        - Really - I can bring any compact electrical device I want onboard an aircraft?
        - Who certifies my device as viable?
        - Why is it important to have a plastic brick that you carry and maintain?
        - What is wrong with being an "internet only" person?
        - Are there size limitations? e.g. a *-phone is ok, a *-pad is ok, but a full blown laptop is too much (e.g. no keyboard)
        - Am I forced to create an "all your DIDs in one place" model, or do I carry my health care phone, my travel phone, my social phone
4. Slide 4
    - What do we need to define a Minimum Device

- Legislation?
    - Who is the authority?
    - Who coordinates multiple jurisdictions?
    - Lawsuits for “not accepting my device” and other forms of Device Prejudice
- Specifications?
    - Is this an IEEE/ISO thing, where you have to pay to get access to the specification?
    - It doesn’t seem to belong in W3C or IETF (or DIF, ToIP, LinuxFounation, etc.)
    - Who defines this specification?

5. Slide 5
    - What are the requirements
        - Camera for QR code
        - Trusted Execution Environment
        - SIM Card / Government Tracking Network or is wifi-only ok?
        - Screen for display of multiple stuff
        - Single User Only
        - Biometrics capabilities?

Final Slide - proposed minimal requirements developed during end of session

- Camera + screen
- Some contactless communication >= 2 options
    - Unidirectional → ability to present (maybe not sufficient, and subsumed by bidirectional)
    - Bidirectional → ability for mutual verification (not necessarily a concern, but required for challenge/response protocols)
- Ability to verify that you are communicating with what you think you’re communicating with – MITM protection
- Possibly “hardware keystore”
- What about always-on/ambient “network” connectivity? No. Connectivity can be moved within the business process.

Enterprise Information System for Peer Production (EISPP) – Animations/Wireframes (2015 pre-DID), Payments, VRM, Linked Data…

Tuesday 5D
Convener: Brent Shambaugh
Notes-taker(s): Brent Shambaugh

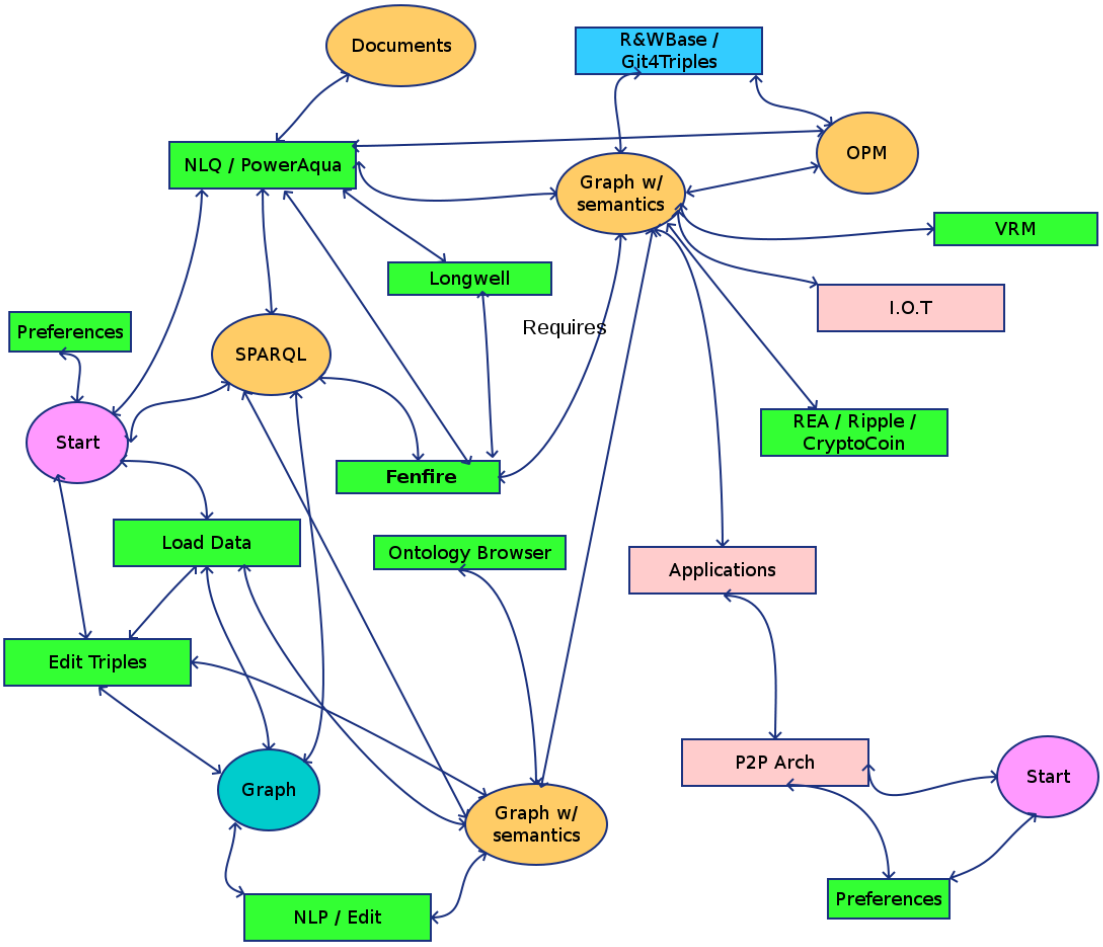
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Premise of EISPP:

Problem/Argument:
"We need a system that encourages learning and creates business and research opportunities through self-organization. The traditional model is failing us. We must go beyond the traditional model and personalize education, business, and research with self-organization, so that individuals can contribute their own ideas and work together toward common goals."

Implementation:
"Ideally, the peer-to-peer economic platform will allow for the creation of virtual teams / "companies" that will be connected to other virtual teams by means of their value networks. Potentially the system that evolves with the platform could also be an improvement or even replacement of existing means to manage intellectual property. Instead of hoarding and protecting intellectual property with patents, sharing through interconnected value networks may become the norm. Such sharing could be advantageous since the potential interconnectedness could allow value networks producing products to make themselves available to a wider audience than they could reasonably attain by themselves. Renumeration could be obtained by other value networks channelling profits to other connected value networks or through each value network selling their own finished product and keeping all profits to themselves."

Program Flow (see graphic below):



Wireframes: http://bshambaugh.org/eispp/

Description:
EISPP is a collection of wireframes, with the following scenarios:

Entry Point Scenario 1:
Preferences are set or left as they are. The user begins by making a natural language query with **PowerAqua**. **PowerAqua** returns documents and triples related to these documents as well as ontologies describing these triples. If the graph display is enabled, the triples are returned as a directed graph. If **OPM** is enabled, the triples are displayed using **OPM**. Optionally, the user can refine the resulting triple results by performing a SPARQL query. If the triples have changed overtime, the user can use **R&WBase** to see their history.

Entry Point Scenario 2:
The user may load a graph and start browsing it with **Longwell.** In the EISPP wireframes, the graph similar to {1} is used. Add a restriction in {2} means I only want to return subjects that have predicates Car_partOf:partOf and objects :Car . If I apply even more restrictions, like in {3} I return even more results.

{1}http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2powder4.pdf
{2} http://bshambaugh.org/eispp/ch_1_2_Facet/PDF/EISPP_3p2_facet2.pdf

{3} http://bshambaugh.org/eispp/ch_1_2_Facet/PDF/EISPP_3p2_facet3.pdf

Entry Point Scenario 3:
The user may load a graph and browse it like in **Fenfire**.

Beyond the Entry Point, Once a Graph Exists: Scenario 4:
I may then proceed to **Edit Triples**.

Beyond the Entry Point, Once a Graph Exists: Scenario 5:
The user may load an **Application** associated with a node, a URI, in the RDF triple graph. In this case the app was CIMBA, a microblogging application. CIMBA is based on S.O.L.I.D, which is based on the Linked Data Platform Specification, which is a restful way to obtain linked data in a filesystem like manner.

A number of other applications are included in the EISPP wireframes. In theory, these could be infinite. Data is stored per the Linked Data Platform Specification (as I recall). Semantics are expressed using mappings to an upper ontology by means of a reference library as described by
ISO 15926 {4},{5}.

{4} http://bshambaugh.org/eispp/ch_1_2_Applications/PNG/ref_library.png
{5} https://www.posccaesar.org/wiki/ISO15926Primer

Beyond the Entry Point, Once a Graph Exists: Scenario 6:
Nodes in the graph may be associated in economic intentions described by **REA/OVN.**
This allows contributors to get paid for their portion of work on a product by recording a record using a value equation.

Payment Occurs over the Ripple or Bitcoin or CryptoCoin network.

Beyond the Entry Point, Once a Graph Exists: Scenario 7:
Nodes in the graph may be producible in the real world. The **I.O.T./BotQueue** portion allows for users to select from the desired 3D printers for delivery or pickup.

Beyond the Entry Point, Once a Graph Exists: Scenario 8:
Occasionally, **Applications** need compute resources to run. Resources may be selected by location, distance, cost, time (compute time?), and common interest using **Peer to Peer Computing.**
Beyond the Entry Point, Once a Graph Exists (or doesn't): Scenario 9:
The **VRM** tool allows users to control their data with respect to the global graph (which is all of the data ultimately accessible by EISPP whether created by the user or not).

The VRM tool has 7 tabs: Bookmark Triples/Save Cache, Federate Graphs, Load Badge, Load Profile / Groups, Access Control, Transact, and Powder Preferences.

Bookmark Triples / Save Cache:
The user has the option to:
Save query result as an RDF file, Save SPARQL query input, Save the Query to an Linked Data Platform Container or (a) Collection, and list the saved items.

{...vrm{2...3...4...5}bookmark}

Federate Graphs:
This functionally allows the user to merge more than one RDF graph. This can follow owl:sameAs links or use different algorithms like the ActiveGenLink from the SILK Framework.

{...vrm2federate...2...2_2...3...4}

Load Badge:
I may want to associate a project with a badge representing my accomplishment. This is like loading a graph.

{...vrm2loadbadge}

Load Profile / Groups:
I can load different projects that I am a part of, as well as a friend of a friend file describing me.

{...vrm2loadprofilegroups...2}

Access Control:
This allows me to control who has read and write access to my projects, as well as who can change the read and write access for my projects.

{...vrm2accesscontrol}

Transact:
This allows me to purchase or start a negotiation/barter for a node in the graph. This allows me to see transaction history (receipts) for what I have bought with the node as a subject. This allows me to see information about the item, such as price, before a transaction occurs. This is modelled off of and/or inspired by the Web Commerce Specification {6}.

This allows me to find and load a wallet, and see the wallets balance.

{...vrm2transact..2..3}

Powder Preferences:
Each project has its own powder preferences. I can set them here. Powder is a vocabulary that includes things like attribution, a description, a certification by someone, etc.
{...vrm2powder..2...3...4}

{...vrm{2...3...4...5}bookmark}
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2bookmark.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm3bookmark.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm4bookmark.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm5bookmark.pdf

{...vrm2federate...2...2_2...3...4}
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2federate.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2federate2.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2federate2_2.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2federate3.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2federate4.pdf

{...vrm2loadbadge}
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2loadbadge.pdf

{...vrm2loadprofilegroups...2}
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2loadprofilegroups.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2loadprofilegroups2.pdf

{...vrm2accesscontrol}
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2accesscontrol.pdf

{6}Manu Sporny, Ed., Web Commerce 1.0, Product Offers and Digital Receipts for the Web,
Draft Community Group Specification 10 April 2014,
https://web-payments.org/specs/source/web-commerce/

{...vrm2transact..2..3}
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2transact.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2transact2.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2transact3.pdf

{...vrm2powder..2...3...4}
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2powder.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2powder2.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2powder3.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2powder4.pdf

Tools Described in Program Flow:

Longwell:
Description: SIMILE Longwell https://www.w3.org/2001/sw/wiki/Longwell
Code: https://github.com/bshambaugh/longwell
In EISPP: http://bshambaugh.org/eispp/#ch_1_2_Facet
In EISPP on YouTube: https://www.youtube.com/watch?v=zEebnDMynwE

PowerAqua:
Description & Code: http://technologies.kmi.open.ac.uk/poweraqua/
In EISPP: http://bshambaugh.org/eispp/#ch1_1_nlq
In EISPP on YouTube: https://www.youtube.com/watch?v=OQySteqxitA

NLP/EDIT:
In EISPP**:** http://bshambaugh.org/eispp/#ch_1_2_NLP
In EISPP on YouTube: https://www.youtube.com/watch?v=tq5r3g72IAg
To suggest ontologies, possibly use:
Falcons:

Gong Cheng, Weiyi Ge and Yuzhong Qu, Falcons: Searching and Browsing Entities on the Semantic Web, https://core.ac.uk/display/23721009
FALCON-AO: http://ws.nju.edu.cn/falcon-ao/
Sindice:
https://sindice.com/
Perhaps ActiveGenLink was unintentionally left out?:
Description: Robert Isele, Christian Bizer , Active Learning of Expressive Linkage Rules Using Genetic Programming
Code: https://github.com/silk-framework/silk

Fenfire:
Code and Documentation: https://web.archive.org/web/20110726051949/http://fenfire.org/
(Equivalent Code?: https://github.com/fenfire-org/fenfire)
In EISPP: http://bshambaugh.org/eispp/#ch_1_2_ldbrowser
In EISPP on YouTube: https://www.youtube.com/watch?v=e1VAYiR6iC4
Possibly Personal Data Store: *{...ldbrowserb4}*
http://bshambaugh.org/eispp/ch_1_2_ldbrowser/PDF/EISPP_3p2_ldbrowserb4.pdf

Ontology Browser:
The ontology browser is based on Franconi's work. However, natural language generation seemed lacking. Instead terms are taken directly from the ontology.
The example appears to use a more developed form of the ontology described here:
http://adistributedeconomy.blogspot.com/2014/11/asserted-car-part-model-in-protege-51.html
In fact it is here displayed in the right column:
http://bshambaugh.org/eispp/ch_1_2_OPM/PDF/EISPP_OPM3_fresnele.pdf
It appears that the class Item can have properties, hasLocus, hasPart, hasPart_directly, partOf, and partOf_directly.
With more context: http://adistributedeconomy.blogspot.com/2014/12/monthly-update-for-december-for.html
In EISPP: http://bshambaugh.org/eispp/#ch1_2_OB
In EISPP on YouTube: https://www.youtube.com/watch?v=XbTeyqJzFvs

References:
Enrico Franconi et. al, An intelligent query interface based on ontology navigation, http://ceur-ws.org/Vol-565/paper3.pdf
Theoretical foundations of Query Tool mentioned in Paper:
https://web.archive.org/web/20150927132946/http://www.inf.unibz.it/krdb/pub/TR/KRDB09-05.pdf

OPM:
Description: Dov Dori, The Visual Semantic Web: Unifying Human and Machine Semantic Web Representations with Object-Process Methodology https://www.cs.uic.edu/~ifc/SWDB/papers/Dori.pdf
Code: https://code.google.com/archive/p/web-opm/
Code: https://github.com/djafaka/web-opm
In EISPP: http://bshambaugh.org/eispp/#ch_1_2_OPM
In EISPP on YouTube: https://www.youtube.com/watch?v=827ysI8GV6
In EISPP (2nd): http://bshambaugh.org/eispp/#ch_1_2_edit_OPM
In EISPP on YouTube (2nd): https://www.youtube.com/watch?v=vdR3hxKuUiM

VRM:
Description: Project VRM https://cyber.harvard.edu/projectvrm/Main_Page
In EISPP: http://bshambaugh.org/eispp/#ch_1_2_VRM
In EISPP on YouTube: https://www.youtube.com/watch?v=ugaOafyQmwo
One bridge to SSI/DID: https://openbadges.org/
One bridge to SSI/DID: {...vrm2loadbadge}
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2loadbadge.pdf
One Bridge to SSI/DID / Digital Wallet: {...vrm2transact , ...vrm2transact2, ...vrm2transact3 }
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2transact.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2transact2.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2transact3.pdf
Personal Data Store: *{...vrm2bookmark , ...vrm3bookmark , ...vrm4bookmark, ...vrm5bookmark}*
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2bookmark.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm3bookmark.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm4bookmark.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm5bookmark.pdf
Personal Data Store: *{...vrm2loadprofilegroups, ...vrm2loadprofilegroups2}*
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2loadprofilegroups.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2loadprofilegroups2.pdf
Federate Graphs: *{...vrm2federate3 , ...vrm2federate4 }*
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2federate3.pdf
http://bshambaugh.org/eispp/ch_1_2_VRM/PDF/EISPP_directional_graph_2fresnel_gss_vrm2federate4.pdf
Utilizes ActiveGenLink:
Description: Robert Isele, Christian Bizer , Active Learning of Expressive Linkage Rules Using Genetic Programming
Code: https://github.com/silk-framework/silk

R&WBase:
Description: Miel Vander Sande et. al, R&Wbase: Git for triples, http://ceur-ws.org/Vol-996/papers/ldow2013-paper-01.pdf
Code: https://github.com/rawbase/rawbase-server
In EISPP: http://bshambaugh.org/eispp/#ch_1_2_OPM
In EISPP on YouTube: https://www.youtube.com/watch?v=827ysI8GV6

I.O.T./BotQueue:
Code: https://github.com/Hoektronics/BotQueue
In EISPP: http://bshambaugh.org/eispp/#ch_1_2_Botqueue_IOT
In EISPP on YouTube: https://www.youtube.com/watch?v=_K63xFiI3Pk

REA/OVN:
Code: https://github.com/valueflows/valueflows
In EISPP: http://bshambaugh.org/eispp/#ch_1_2_edit_triples
In EISPP on YouTube: https://www.youtube.com/watch?v=SsWJbdsq9H4
Reflections from Today: Could a OVN commitment be made binding with a smart contract?

Edit Triples:
In EISPP: http://bshambaugh.org/eispp/#ch_1_2_edit_triples

In EISPP on YouTube: https://www.youtube.com/watch?v=SsWJbdsq9H4

Preferences:
Fresnel Lens: Christian Bizer et. al, Fresnel - A Browser-Independent PresentationVocabulary for RDF, https://hal.inria.fr/file/index/docid/56132/filename/fresnel.pdf
Graph StyleSheets and Fresnel Lens used in IsaViz:
https://www.w3.org/2001/11/IsaViz/

Applications:
Solid: https://solid.mit.edu/
Documentation for CIMBA:
Andrei Sambra et al.,CIMBA - Client-Integrated MicroBlogging Architecture,
Decentralized Information Group, MIT CSAIL, Qatar Computing Research Institute
Notes:
Blog Post: http://adistributedeconomy.blogspot.com/2016/06/setting-up-solid-server-using-webid.html

Peer to Peer Computing:
In EISPP: http://bshambaugh.org/eispp/#ch_1_2_P2PArch
In EISPP on YouTube: https://www.youtube.com/watch?v=Mi9UGvlAdUM
Blog Post: http://adistributedeconomy.blogspot.com/2014/09/p2p-computing-architecture.html

Reflections from Today:
Neither EISPP nor the writing that preceded its creation "P2P World-OS: A P2P Enterprise Platform" discussed a good way to bring parts together:
Use Marko Rodriguez's (Gremlin from Apache Tinkerpop) new project as a back end?
http://www.mm-adt.org/
"mm-ADT™ is a distributed virtual machine capable of integrating a diverse collection of data processing technologies. This is made possible via three language-agnostic interfaces: language, process, and storage."

The "P2P World-OS: A P2P Enterprise Platform" document suggested an upper ontology for interoperability of components. Is this good enough, or would information capabilities provided by applied Category Theory help?

Consider Category Theory from Schema Interoperability for decentralized Identifers (DID) and schemas in general:
See the group that Henry Story Started: https://web-cats.gitlab.io/
Learn from the Applied Category Theory Tools at: https://www.categoricaldata.net/
Avoid over-reliance on upper ontologies by instead focusing on schema integration:
David Spivak: Categorical Databases : https://www.youtube.com/watch?v=bk36__qkhrk
Compare to:
Brent Shambaugh, P2P World-OS: A P2P Enterprise Platform, Software Interoperability Section in:
http://bshambaugh.org/Master_17.html

Final Comments:
EISPP is a front end. It does go into much depth as to how global data gets there to be seen by the user. To make the data accessible see:
Brent Shambaugh, P2P World-OS: A P2P Enterprise Platform, Software Interoperability Section in:
http://bshambaugh.org/Master_17.html

In particular see sections on *Peer-to-Peer Computing* and *Aggregation of Data*

Finding data: (http://bshambaugh.org/Master_17.html > *Peer-to-Peer Computing***)**
Alexander Loser, Semantic Social Overlay Networks,
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.72.7668&rep=rep1&type=pdf

Clustering data: (http://bshambaugh.org/Master_17.html > *Aggregation of Data***)**

Ahmed Charles, On the Implementation of SwarmLinda A Linda System Based on Swarm Intelligence(Extended Version), https://cs.fit.edu/media/TechnicalReports/cs-2004-03.pdf

Daniel Graff, Implementation and Evaluation of a SWARMLINDA System ,
http://www.inf.fu-berlin.de/inst/pubs/tr-b-08-06.abstract.html >
ftp://ftp.inf.fu-berlin.de/pub/reports/tr-b-08-06.pdf

Notes Day 2 Wednesday October 21 / Sessions 6 - 15

SSI in Developing Countries: Product and Usability

Wednesday 6A
Convener: Rachel Chang, Kiva
Notes-taker(s): Sankarshan,

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

- Introduction by Rachel - building out Kiva protocol is one of the recent projects. The session will be sharing the learning around adoption of SSI
    - Kiva protocol enables identity verification for KYC compliance account access and ongoing customer due diligence.
    - Started around 2y ago; one of the most common things that banks have is a KYC process to verify somehow that the individual is who they say they are (based on existing documents or even someone vouching for them)
    - eKYC platform was launched at Sierra Leone - worked with local financial providers this was launched at early 2020 (video/walk-through at Marampa Community Bank) using fingerprint the wallet is unlocked and the National ID credentials are shared.
    - Prior to launch pre-pilot testing phase was conducted for UX - 15 test subjects participated across key partners and stakeholders. Nearly all participants found a match and a correct ID record could be accessed (even if there were initial fingerprint miscaptures). Finding - users tend to use right thumbprint instead of right index fingers based on familiarity with other biometric systems in vogue
    - Key learnings
        - Flexibility in options - discouraging experience when the match does not happen first time. Enabling selecting a different finger or provide a voter ID for fallbacks
        - Integration will improve operational efficiency - customizing eKYC app for the FSP's existing MIS/core banking improves data consumption.
        - Education and awareness - bank tellers need to be well trained to explain the benefits of the process of the new verification process. Once customers see the value, the ID credential itself becomes more valuable. Having bank tellers who are engaged helped customers gain confidence and see value
    - Next Steps
        - In Sierra Leone, Wallets were held in Guardianship. With the Kiva Protocol Wallet individuals have the opportunity to manage their wallet via mobile (powered by Kiva Aries backend)
    - Open Questions - the layers of SSI - regulation, technology and trust frameworks are crucial to developing robust, scalable and compliant SSI solutions
        - Digital Literacy and appetite for technology adoption - how do we explain the benefits of SSI when literacy and digital literacy rates are low? How willing are individuals willing to adopt new technologies and processes?
        - Data protection - how do we work with a government's data protection laws? How do we influence policy?
        - Back-ups - how do we create a more flexible integration between wallets and backup services to guarantee efficient account recovery?

- Adaption of current information and digital systems - current IT systems must transition or be integrated with the issuance and verification of SSI credentials
- Trust Frameworks - what are the requirements for the different levels of assurance for different use cases? Eg. opening a bank account vs. withdrawing money
- Robust decentralized registries - how do we ensure that registries that become the source of credential data are accurate and interoperable? Are there processes and governance frameworks in place?
    - [Nicky] Were there any challenges with women being able to adopt vs men - eg social norms, literacy, digital access..?
        - [Rachel] based on the current pilot there have been no specific observations. But further validation would be needed
        - Nicky also provided context about ongoing academic studies around the lived experience of women in relation to use and consumption of technology.
        - From Kristina - Omydyar network has a great paper on women and ID and interestingly in some cases, women are in control of entire family identities while in other cases men control all identities of women depriving them of all rights..
        - From Nicky - There is also this view from ID4D https://documents.worldbank.org/en/publication/documents-reports/documentdetail/859071468190776482/the-identification-for-development-id4d-agenda-its-potential-for-empowering-women-and-girls-background-paper
    - [Kristina] so data for eKYC, you get it from local financial services? Can people who do not have a record with local Financial services cannot get eKYC services?
        - The data was obtained from the national registry of Sierra Leone as they were designing the eKYC policies for the financial sector
    - [Kristina] what aspect is exactly "SSI"?
        - The components for the solution are Aries (was previously Indy) and the VC standard. Even though the individuals are not carrying the credentials on the phone, but they control/govern the access to those credentials for services being enabled. The next step would be to evolve to a mobile wallet.
    - [Eric Drury] How has the project dealt with different trust frameworks
    - [Bentley Farrington] What was the perception around the remote guardianship model for the wallets as opposed to them physically having their national ID cards? (Did they trust it? In context of the user perception of being used to physical cards)
        - On the ground perspective this was the most efficient way to achieve the outcomes. It would be cumbersome to carry around the credentials - the concept is complex due to the low digital literacy.
    - [Bart Suichies] I may have missed it, but what's in the wallet? Biometric information? Or credentials of another kind (to enable account authorization)?
        - The VCs - the individuals can provide consent for accepting the credentials. The biometrics are part of a separate service.

- [Eric Welton] How were the wallets set up? What %age of a month's average wage is a cell phone/smart device?
    - In the existing model the wallets were in Guardianship. The evolution to a mobile device is the next phase
    - [EricW] Were TEEs for smartphones considered?
        - Sidebar chat conversation around Tykn, DIDx etc
        - Sidebar chat remark from Nicky "Maybe we need to convene a low-tech SSI group to start comparing notes, identifying gaps, sharing research? is so essential to I4A mission"
- [Ivan Temchenko] The users do not have the access to their wallets - the banks are the mediators between the users and the access. Is the full set of data being displayed or some limited/restricted view
    - The FSPs requirement drove the subset of fields in the VC and the requirements of the verifier were then considered when displaying the information. In the ongoing re-architecture - the verifying organization will set up the requirements for what they need.
- [Mike Richardson] How are the credentials being issued?
    - APIs help source the required information from the national registry and Kiva is acting as a form proxy issuer on behalf of the government
    - How does the holder know that the identity data is correct and Kiva has not tampered with it?
        - [Rachel - could you respond to this later?]
    - How do you know when any of the credentials have actually changed? Async push+revoke+issue isn't possible. How is the information kept current?
        - [Rachel - could you respond to this later?]
        - Mike - adding an expiration date?
    - How many users do you have so far and are there scale challenges?
        - Pre COVID-19 phase has had around 100+ eKYCs
- [Phillipe] About putting guardianship on biometrics - have you looked at the possibility of a neutral independent body who can be the "Guardian"?
    - [Rachel] There were questions around the topic of ethics in terms of whether Kiva should hold these wallets. Ran into challenges of finding the right organization partner who has the capacity - technology and resources to be able to fill this role!
    - Is Kiva already a member of the Trust over IP Foundation
        - [Dave Luchuck responded]
    - Phillipe also presented short remarks around the Birth Attestation project.

Active and Passive Identifiers: Elements, objects and characteristics of a decentralized network (Repeat Session for EU/APAC Attendees)

Wednesday 6B
Convener: Paul Knowles @pknowles

Tags for the session - technology discussed/ideas considered:
Paul presented a slide deck that defined the two concepts of passive & active identifiers.

- Passive: Immutable & Active: Authenticable

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

Everything is documented in the slide deck which is available here.
Related blog post: https://humancolossus.foundation/blog/active-and-passive-identifiers

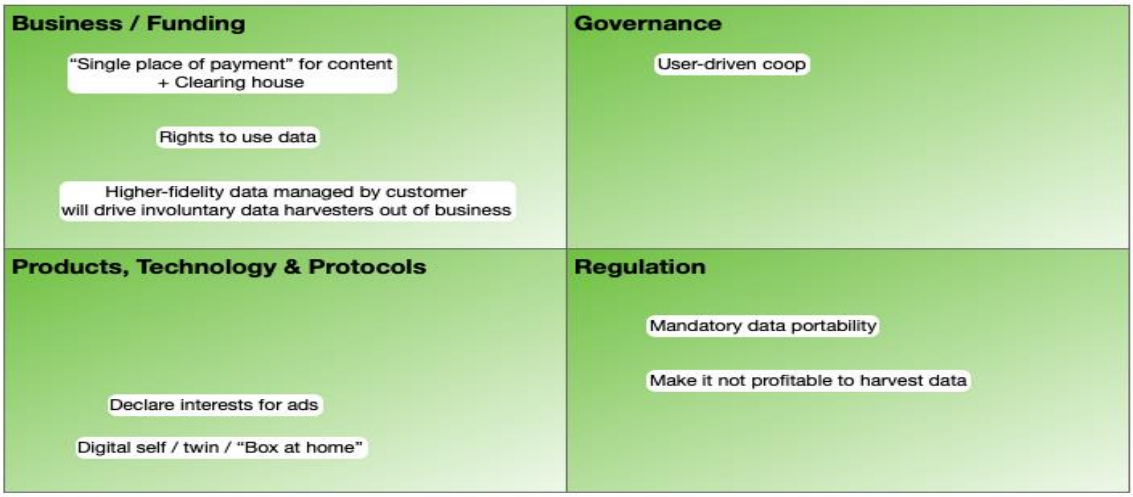
Rolling Back Surveillance Capitalism: Part 2 -- what are the Obstacles and what Assets can we use?

Wednesday 6J
Convener: Johannes Ernst
Notes-taker(s): (all)

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

Summary from yesterday:

Envisioning Non-Surveillance-Capitalism



CCPA experiment: 1) they are slow in responding, 2) the responses are largely "unusuable" by normal human beings (e.g. zip files of JSON files with no documented data dictionary) 3) some data looks intentionally obfuscated (e.g. Facebook "inlines" the names of people you chatted with, does not export the identifiers, so you can't tell the difference between two people with the same first/last name)

One avenue: acquire a telco, make it do VRM.

Want to follow personas who I trust with their product recommendations.
Challenge: how to find trustworthy personas

Zebras
Indie Hackers podcast
Could use a collection of successful business examples that's documented.
Also templates for structures that new businesses can use.

Beyond Binary - How do we use the Web of Trust and move beyond the green checkbox?

Wednesday 7A
Convener: Eric Welton
Notes-taker(s): Hunter Cain

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

- Trust being transactional and the word is overused
- Conditioned to a single summary
- A world of gray, not black and white
- Want all possible information compared to something very simple
- Levels of assurance, trusting enough to take an action
- SSI, will you go to jail for me? Type of trust
- Different levels of trust and how do you categorize that
- How do you combine information to form our own risk assessment?
- Domain specific validators
- Cookies are on their way out
- Want more detail to show what we are sharing
- How do you develop initial trust?
- Need trust anchors, maybe have to go back to centralized
- How do you trust the verifier?
- Is there a legal connect?
- Conflict of adjudication and be put in terms of a contract
    - Rights and responsibilities of the trust framework
    - Like a bug report showing what was violated
- Burden is on you to try to relate it to legislation
- What damage can ZKPs do?
- People will always opt to the easiest path, sacrificing their credentials
- Have to be able to quantify trust and how to apply it
- Only stops being binary when we have enough binary solutions
- Have to treat the digital world the same way we treat the real world as the consequences are the same
- Legal framework and how to work across borders?
    - Transactional data passing back between the U.S. and EU
    - People have to be in compliance in order to do business
- Machine interactions are deeply embedded in human interactions. And the fact that these machines are always reading our behavioral pattern. How do we use SSI to create trust for these devices?
    - We have no say in what data is being taken and sold
- What is Kerry/i?
- How do they apply the learning the data they collect from you?

Trusted Digital Assistant - Why I don't need to manage my identity

Wednesday 8A
Convener: Robert Mitwicki
Notes-taker(s): Judith Bush

Tags for the session - technology discussed/ideas considered:
Wallet, one universal wallet, TDA, trusted digital assistant, consent, negotiation, personalization, Dynamic data economy

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

TDA why digital wallet is not enough
TDA is not one thing running on a particular device, but is available across many/all your devices.

Consider Jarvis in the Iron Man/Marvel films

Digital Identity Management is hard
One doesn't _manage_ one's own passport (carry it yes, but not handle the security etc)
To truly manage, you need to understand the technology, understand the assurance, know what is safe to share where.

Consider managing your own email server….

Chat:
From Neil Thomson to Everyone: Reality check - we need a service like the legal profession for identity. Experts in configuring your identity and interactions with services (the right set of consents) consistent with your personal preferences.
From Eric Drury to Everyone: That's Iowa AI for you
From Neil Thomson to Everyone: A TDA as describe is an Artificial Intelligence, which is beyond current tech. From Eric Drury to Everyone: +1 Neil
From Neil Thomson to Everyone: An "Personal Identity Advocate"
From Joachim Lohkamp to Everyone: So do you imagine a TDA to be a algorithm that not only manages your identities, but it would also need to make decisions…. How does the TDA learn about your preferences, values, restrictions both personal and also legal? From Neil Thomson to Everyone: +1
From Eric Welton (Korsimoro) to Everyone: @Neil - we touched on that a little bit last session as well. Even if we were going to try to whip up a quick expert system or rules system or something to try to capture a bare-bones information fiduciary, acting on machine readable (IEEE 7x?) policies - we are lacking a trust expression language

What TDA can do for me

You can inform it of your needs and wants before advertising analytics can deduce
It can more accurately collect demographic and behavioral data instead of having it deduced
Manage identity & Consent (keys, policy, T&C negotiation)

Brief Introduction to Picos

Wednesday 8O
Convener: Bruce Conrad
Notes-taker(s): convener

Tags for the session - technology discussed/ideas considered: Picos, Aries agents, Manifold

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

Terry and Will joined me for a half hour discussion about picos (see picolabs.io), Manifold, and ACA-Pico. The latter is a collection of rulesets which can be installed into any Pico to make that pico be an Aries agent (along with whatever else is already was).

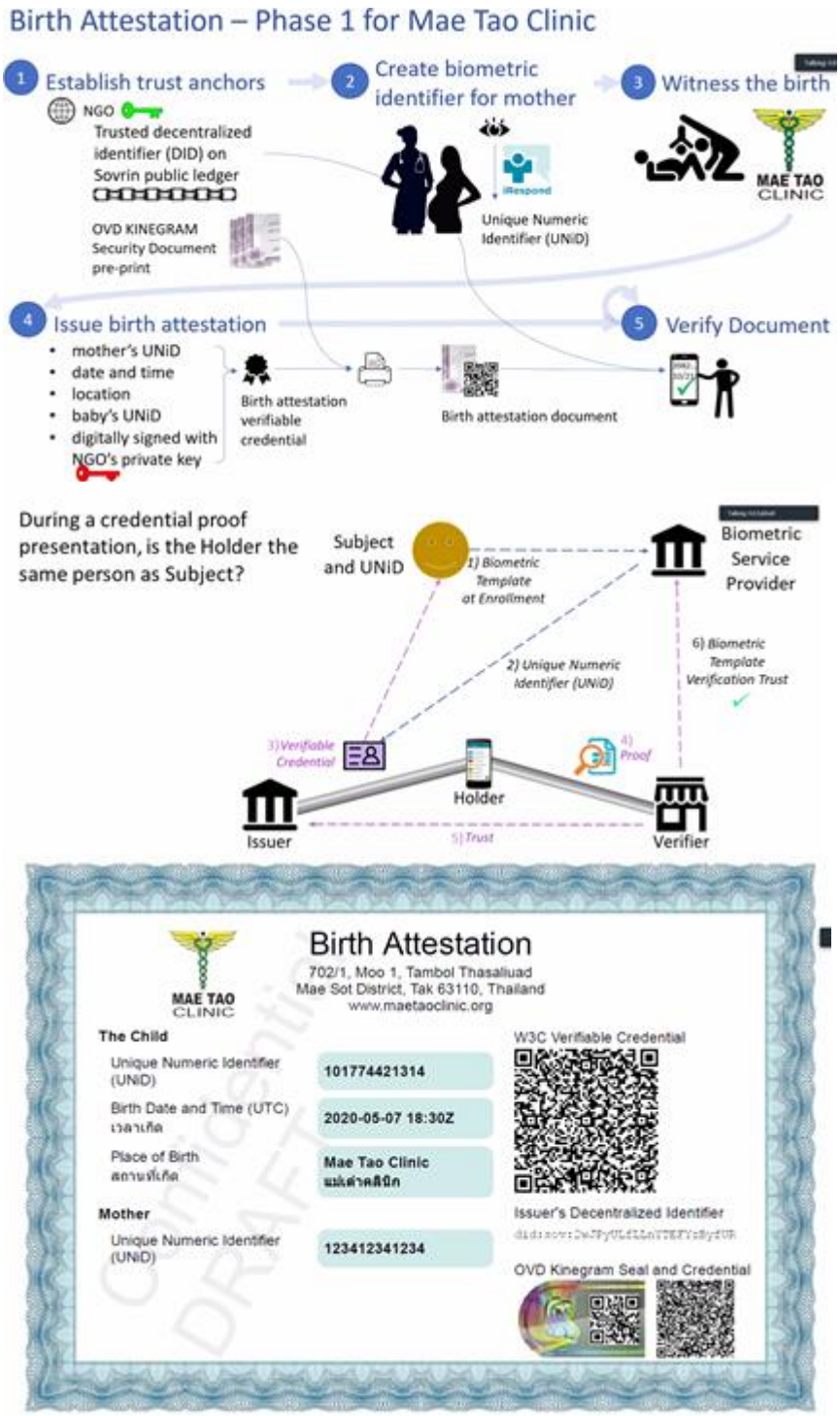
Follow up meeting scheduled with Will and a student he works with, and sent Terry my email address on RocketChat. Repeated here for convenience: bruce_conrad@byu.edu

Birth Attestation = Initial Guardianship

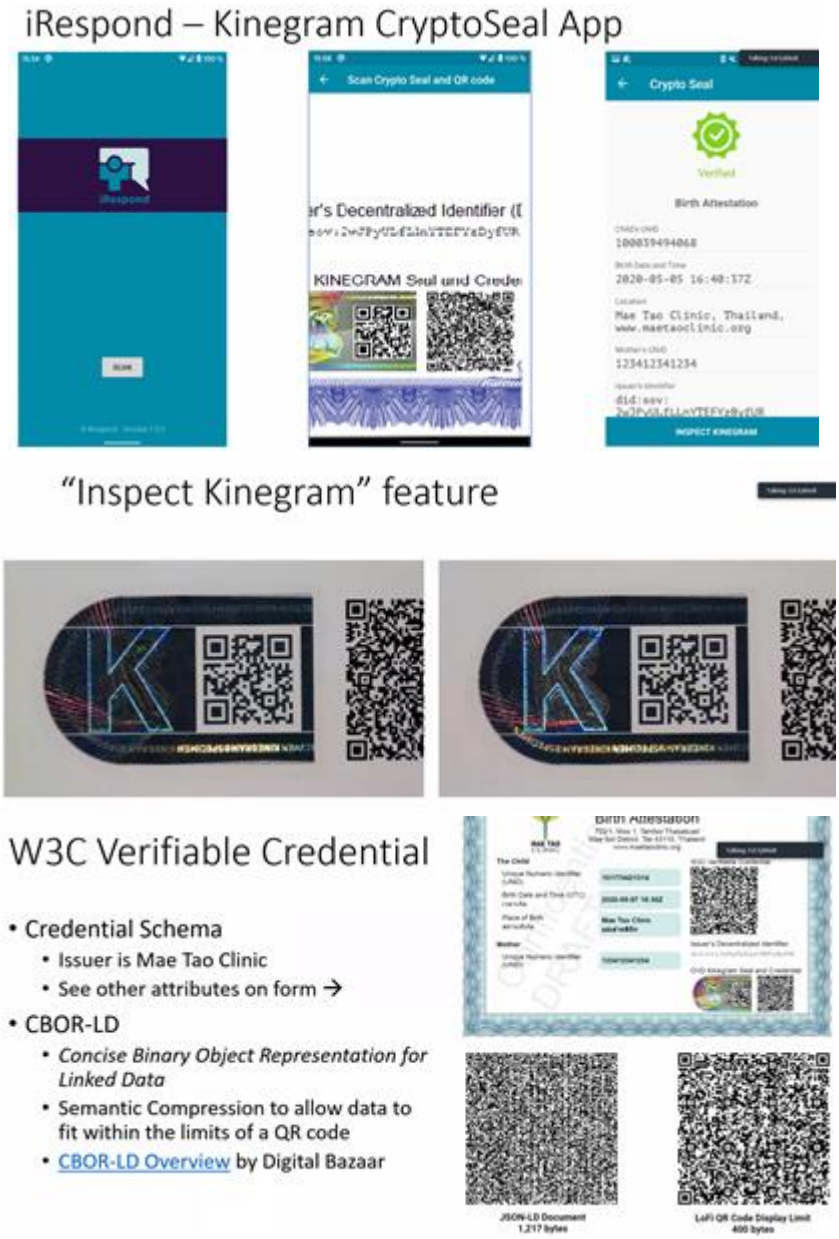
Wednesday 9A
Convener: iRespond / Ed Eykholt
Notes-taker(s): Neil Thomson

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:
This session is being recorded

_____
UNiD Node
Uses (eye) iris camera
Returns a UNiD (Unique Numeric Identifier)
iRespond has a project which is using iris camera to better identify migrant and citizen children born in Thailand (Yay Nam Tao Clinic! / Mae Tao Clinic)
1600 babies born per year in this clinic.
Currently produces a hand-written birth record.
Digital paper (security paper) – as 'minimal device' – essentially bank note paper



The two QR codes, etc. in bottom right are unique per piece of paper, the rest is generated for each birth



Not a live project yet – this birth attestation has not been rolled out. This is in process (software in development)
Has a lot of interest for use of this technique for other identity circumstances.
It is not known if the Government(s) and officials (e.g. schools) will accept these IDs/documents.
Will have to be proactive in working with the governments.
The scope of this pilot was to produce digital and non-digital (linked) identity.
The problem in Thailand is the porous border with Myanmar

The digital document (with minimal data) can also be printed on paper.
Carrying the OVD paper is a digital id.
This is initially just for Birth Attestation to get a Birth Certificate, which is the currently recognized document in both Thailand and Myanmar.
Can we bring them a process and tool

Birth Attestation – Future

- Add verifiable credential types
  (guardianship / immunization records)
- Integrate biometric hardware for infants / children
- Collaborate on SSI Guardianship
  - Issue and revoke
  - Work with governments, international NGOs, ...
  - Understand their needs
  - Educate and enable other credential verifiers
    (e.g. healthcare)
- Add issuing locations (refugee camps and hospitals)
- Explore safeguarding credentials from loss
  (e.g. verifiable credential registries, encrypted data vaults, escrow / trustee / steward processes, signed PDFs docs)

Peter Simpson.
An issue is also document recovery – in case the issued digital paper is lost. Much cheaper if stored digitally to reproduce.
Also an attempt to provide a document recognized by both documents.
Ed Eykholt

Also looking at other Biometric capture tools – iris cameras can be problematic for infants (distance between eyes relative to head.
Need an infant iris camera, but looking at other biometrics tools as well.
Will be different in each region based on the legal systems and government identity systems in each region.
Looking to work with other locations – refugee camps and hospitals

This approach only makes sense if it will be acceptable for life - a long term DID mechanism.

“Proof of existence” a very important. Access to school, immunization, etc. The security of the document is key. They are like passports in the level of sophistication.

Running paper (physical) and fully digital in parallel

Have deployed wallets on a lot of android phones and a lot are not compatible

Why chose iris scan vs,. finger prints

- Non-touch is important
- Iris are very unique
- Finger prints not recorded for 20% of the population in many regions

Chris Raczkowski - Sovrin certainly (Sovrin) interested in fully supporting the project as are many others

Eric Welton - in effectively in a disputed non-state area in Thailand/Myanmar border. The health system is porous on who is who and undocumented is a reality for many people. There is a high resistance to a new process, so the goal is to run in parallel

Comment: Many phones (e.g. android) non-compatible - particularly at the low cost end - with wallets or any applications. This approach avoids that problem and provides a usable lowest common and secure mechanism (paper) in parallel with digital. Sounds like the immediate future. There is a lot to learn from this to apply everywhere (including COVID-19)

Comment: This parallel approach gives a solution that would be pragmatic for many seniors (40% in Canada over 75)) who are not tech-savvy

COVID-19 has slowed things down. Producing a simple physical key with only a focused purpose that can be carried by the person is meeting higher acceptance than a pure digital solution.

Data has value when it flows,

A church in Hollywood has issues with a large homeless population. Issues with a person in late 70’s without any ID (no social security number). Took years without attestation to secure a new SSN. Is a huge problem everywhere.

Refugees and homeless are very suspicious of registries for them - as bad things have happened in the past. This is why minimal information is collected (minimal personal disclosure) to establish identity (e.g. metrics such as iris image).

Goal - create a non-reputable proof of existence - which is acceptable anywhere. Get into the official, local systems (exchange birth attestation for birth certificate/social security card) using a common agreed “root”.

With COVID-19 is more important to have everyone tested and have a traceable record tied to an Identity than to have only those who are officially registered (e.g. has a birth certificate).

This situation illustrates the need for an identity that is independent across borders and technologies and that having a complimentary (non-competing) DID

Question - A barrier can be local administration. What about identifying (and "certifying") and delegating exactly who can generate the birth attestation? This can be important to local authorities.

Sounds like an opportunity to share experiences (e.g. Kiva w iRespond UNiD)

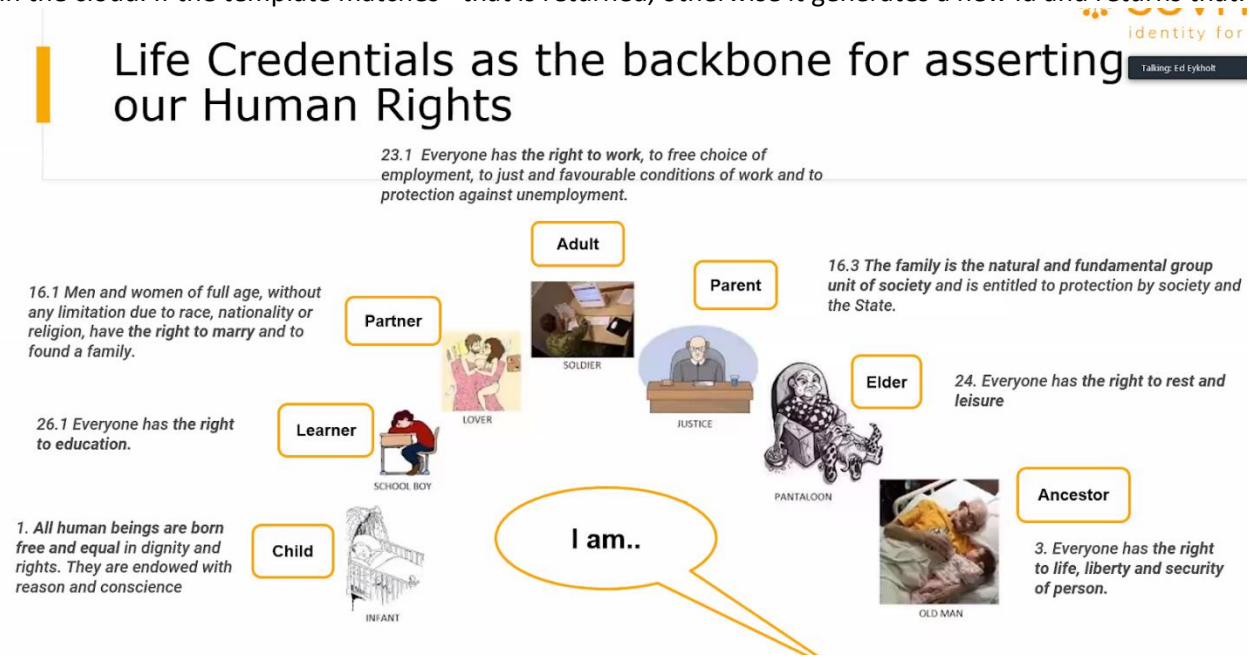
Guardianship - of the Identity vs. supporting the actual guardian (mother -> child) . Who is the ultimate guardian of the (digital) data.

How would the child (as they grow up) use the birth attestation ID, what happens once the QR code is scanned?

The DID of the issuer will aid in the proof of existence - assuming the personal DID and issuer did are on a ledger. If a revocation is needed, the ledger record will also assist.

How does the QR code lead to other information?

How does the iris scan/camera work - it generates a biometric template, which is sent to repository service in the cloud. If the template matches - that is returned, otherwise it generates a new id and returns that.



Have not worked out the "Guardianship" lifecycle (as shown above).

There will be many types of credentials (or identities) including revocations - and where is that recorded (sounds like a personal identity vault).

After birth, immunization records are key to health (second DID contact point).

How to generate QR code to be universally accepted - is CBOR-LD the right way to go?

Concerns with putting a large amount of data into a QR code - which may be difficult to scan - QR codes only as an "introduction" (or a pointer/Digital Link) to other sources of information.

Where is the project going:

- KISS - keep the information essential, but minimal
- Work in progress - learning lots of lessons
- Don't want biometric data flying all over the place.

How to make this a "bearer token" that people can use. Might not be a problem at a hospital. But is this something (like the QR code) that is simple enough to be forged?

There are biometrics readers that are good for verification, but forgery is a known and existing issue.

Education on exactly what this "ID" is intended for and where is it intended to be actually used.

So is the main purpose that this birth attestation is intended to go to an authority that will use it to produce a more "forgery robust" ID (e.g. the paper document is only used for verification into the "official" ID

Secure Scuttlebutt - Peer-to-peer Social Network

Wednesday 9E
Convener: Charles Lehner
Notes-taker(s): David Schmudde

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

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

Slides: https://ssb.celehner.com/iiwxxxi.pdf

Cypherlinks

- Message: header info includes
  - Key: message id (the hash over the value)
  - Value: message number, previous message, signature, etc...
- Blob:
- Feed: a list of messages from a public user (a key)

Pubs

- Servers that serve SSB
- Can send out invite codes for other users to join

Patchwork: Main desktop client
Patchfox: SSB in Firefox

The Principles of SSI

Wednesday 10A
Conveners: Sankarshan Mukhopadhyay, Jasmin Huber, Johannes Sedlmeir, Chris Raczkowski, Joyce Searls, Drummond Reed, Feng Hou
Notes-taker(s): No notes just Chat

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/1ve1bpR7nK6tYyOUjHKYcAB2YZGqKD77OD9ECvpE6JOg/

Complete chat log from the session
From sankarshan : Session notes will be at https://docs.google.com/document/d/1rmPppQwrfPiGVVAaGMJaRdZsa-XegOdTpHs-d0NiQYo/ - hopefully we will have someone to take notes.
From Kaliya Identity Woman : to be fair this is a very SOVRIN centric articulation - there are those who are key leaders in the industry to believe that any permissioned chain is limiting relative to the freedom to "own" your digital identifiers - so it would be great to have a more inclusive frame for articulating these. The BTCR, SideTree, Element and ION are all permissionless
From Tony Fish : ? who's principles and aligned to whose oversight
From drummondreed : @Kaliya, I'll definitely make that point
From Chris Raczkowski : These principles are developed by the SSI community - in a fully open, and collaborative manner. Essentially, these are the global SSI communities Principles of SSI. Sovrin just acts as the convener and organizer for the global community.
From sankarshan : Also, the principles are WIP and the conversation today is part of how we can evolve, refine and make it relatable.
From pknowles : Trust over IP is also much broader than "Identity"
From Kaliya Identity Woman : wait we haven't heard principles yet
From Tony Fish : looking forward to them and how they align to Human Dignity; Subsidiarity; Solidarity; Covenantal; Sustainability; The common good; Stewardship; Equality; Transparency
From Chris Raczkowski : I have to drop - will be back in 30 minutes.
From Kaliya Identity Woman : The essay that first articulated the so called principles was written by one man - he wrote them alone - then "sought input" and when women like me gave feedback on how he framed the principles and the ecosystem - threw how a whole bunch of sexist tropes - and never really got input from anyone who wasn't him. so no Chris it wasn't open and transparent Sovran is not "the convener and organizer of "the global community" there are lots and lots of SSI people who aren not in the Sovrin orbit and don't want to be.
From Tony Fish : +1 @kaliya ; From Jeff Doctor : +1 @Kaliya
From Kaliya Identity Woman : since they have cut off the back channel in our zoom rooms here - please open the rocket chat

From sankarshan : The document being linked to on the slides is at https://docs.google.com/document/d/1YXJEFW2lNuPdhUmXQfO2xQZXwxrskH-lTrHk9pZ_aiM/edit?ts=5f84d3bb&pli=1#bookmark=id.207animqp3le
From mary hodder : So not to defend Chris because he should have done an inclusive process.. but how was that different than Kim Cameron's Laws of Identity? He didn't convene a group.. that I know of.. or it wasn't put out to the community.. and yet this community cites him regularly. How does the community react consistently to things created by one person when they put out something like a list of principles or whatever?
From Kaliya Identity Woman : I was commenting directly on what Chris R. Said above about Sovrin
From Tony Fish : @drummond - rights are not principles; We are all equally entitled to our human rights without discrimination. These rights are all interrelated, interdependent and indivisible. The principles are: Universal and inalienable, Interdependent and indivisible, Equal and non-discriminatory, and Both Rights and Obligations.
From Karen Hand : maybe individuals and organizations?
From Kaliya Identity Woman : I was commenting on two things - one Christopher Allen put his first draft of the post out to about 40 people ; that whole thread went in some weird directions - unsurprisingly - happy to share that whole exchange I have it in a 40 page PDF ; I also was commenting on this from Chris R. "Sovrin just acts as the convener and organizer for the global community."
From PhilWolff : 4th Party Data Fiduciary Powers and Duties : ??
From Dave Crocker : Design Principles should specify a framework for realizing goals. Rights are a type of goal. Design principles are about pragmatics, not ideals.
From Jeffrey Aresty : Rights exist in law; conflicts of laws are where we are wihtout international law stepping in
From Jeffrey Aresty : the mechanism for creating international law is pretty broken
From Kalyan Kulkarni : +1 = Design Principles are about being pragmatic and not necessarily be ideal
From Scott David : How is "their" defined in "their "Personal Data"
From Scott David : Principles, Ethics and Norms
From Jeffrey Aresty : mostly public international law models are we know about - and, to make a right work in an international setting, you need adoption; this is how the Sullivan Principles were adopted (via industry pressure) against S. African apartheid
From Scott David : Duties and Rights must be declared to mutually support
From Jeffrey Aresty : We have taken a stab at this in session 11 - Universal declaration of digital identity
From Scott David : Group behavior is embodied philosophy
From Scott David : We have new blank interaction space in which to work.
From Jeffrey Aresty : It's not blank - the SDGs are there -
From drummondreed : Please feel free to put your hand to queue to talk
From Scott David : SDGs are not enforceable and many remain mutually inconsistent
From Kaliya Identity Woman : Kim Cameron put out the laws one a week for 7 weeks and got intensive community feedback via lists and blogs before he wrote the paper that is referenced. Way different then the process that Chris used just e-mailng a totally complete blog post to 40 people and asking for feedback - which he only very reluctantly listened to a little bit.
Jean F. Queralt : @Tony - Your work is on the same space as what we've been doing at The IO Foundation.
From Marc Davis : a huge challenged here is al it's all personal data and digital identity are relational and therefore subject to join, rather t hsn
From Scott David : PEN - Principles, Ethics and Norms. Different sources, different applications.
From John Court : So for 2. As an example isn't the principle the last part. Personal Data must not rely on a single administrative authority ?
From Marc Davis : typo: joint rather than individual control.
From [TIOF] Jean F. Queralt : @Tony - Was a link shared? (I just joined the room)

From Scott David : Norms arise from “normal” behavior
From Tony Fish : catching up + 1 scott
From Scott David : Ethics arise from humans and apply to humans
From Tony Fish : @jean - no was just a post - will find you on rocket
From Scott David : Principles are aspirational behavior goals set by organizations to guide behavior of components. ; PEN is not set in stone, but is a way to recognize that origins and applications are different and must be accommodated independently.
From mary hodder : But show says what is “normal”.. for example it’s normal in the US govt looking back in history, to redline and discriminate against POC property buyers
From Kaliya Identity Woman : +1 PHil
From Jeff Doctor : Is the SSI “community” aware of
From Scott David : Rights are easy to state. Duties are difficult to adopt.
From mary hodder : that’s not something we want to codify.. but it’s been a norm until very recently
From sankarshan : The document being shared on screen
https://docs.google.com/document/d/1YXJEFW2lNuPdhUmXQfO2xQZXwxrskH-lTrHk9pZ_aiM/edit?ts=5f84d3bb&pli=1#heading=h.3td7cxi237q0
From mary hodder : and still occasionally ‘normed’
Jeff Doctor : Is the SSI “community” aware of related principles such as: https://www.gida-global.org/care
From [TIOF] Jean F. Queralt : @Tony - Rocket giving me a 500.
From Scott David : Yep. Norms include messiness of the past. Just because call them norms, doesn’t mean they are good or aspirational. They are just normal.
From drummondreed : @Scott David: can you speak to that?
From mary hodder : right so how we decide what is a norm is crticial
From Scott David : Be careful what you wish for.
From Tony Fish : @jean cannot find you in the rocket messaging
From Scott David : It is edifying to explore non-self-sovereign-identity as a “negative space” of SSI. Maybe SSI is defined by what it isn’t. From Jsearls : +1 Scott
From Scott David : Delegation questions in representative organizations
From [TIOF] Jean F. Queralt : @Tony - 500 error for me, can't load it.
Tony Fish : there is who is responsible. Back to yesterdays session with @scott. Directors are liable for this, does a director want to be responsible for this? Why as this creates new risk, and risk has to be priced in.
From [TIOF] Jean F. Queralt : Gonna add our UDDR Draft on the doc.
From Bob Wyman : I typically think of a “right” as a thing which is a “side-constraint” that cannot be violated. Many of these “principles,” which are labeled as “rights,” seem to be things which should be provided, but, in many contexts might reasonably not be provided. Example: In many contexts, it is appropriate to forbid delegation. If it can be forbidden, it can’t be a “right.”
From Marc Davis : Since so much personal data and digital identity are relational: declared, observed, or inferred about the data subject by other entities, how do these rights apply to that data?
From Tony Fish : @jean iam@tony.fish - might be faster
From Jsearls : @jean, ask the tech channel to fix your RocketChat. Mine got the error message yesterday, but they fixed it.
From Scott David : I define sovereigns as “entities that don’t need to ask for permission or forgiveness.” They are ALL teleologies to which we can self bind. That is why we grant them the monopoly of legitimate violence in society (Mills). Violence includes non-physical violence such as privacy intrusions, the violence of abstraction, etc.
From drummondreed : To join the queue to speak, just put your hand up using the Participants list
Scott David : We have the opportunity RIGHT NOW to “constitute” sovereign teleologies for the future interaction space. The constitution of the sovereign will include a list of “self-constraints” which is what

ALL constitutions do. They state the limits of power of the organization that is so constituted. Perhaps these principles are photo-constitutional provisions to bind the resulting system itself?
From mary hodder : Rights should be things that cannot be given away, like a human right. I cannot sell my kidney and a company cannot ask me to give them one for some transactional or financial consideration, even if we both want to. It's not allowed. Are the rights things that cannot be taken away?
From Scott David : There are many types of assignable rights.
From Mike Kiser : +1 Mary
From Scott David : Contract rights, etc.
mary hodder : Scott.. understand, but for these rights.. about personal data.. are they rights that you cannot 'lose'
From Scott David : We should identify those rights that are not amenable to assignment.
From Mike Kiser : The term is "unalienable," I would think.
From sankarshan : As we continue with the various perspectives on this topic I'd also like to request that we have some specific next steps we can take with this document and set of principles. As a straw man and WIP - this will require more extensive outreach, inclusion and discussion.
Scott David : Numerically, Most of our identity "rights" at present are contractual, rather than "god given"
From Mike Kiser : And that's likely a different session - would have to think about data dividends / selling your personal data.
From Marc Davis : This list does not include the EU's "right to be forgotten".
From Scott David : This is an awesome discussion. Everyone is a little bit right. Synthesis of all of these consideration is the "constitution" of the future organization
From mary hodder : Scott.. right and that's a huge issue because we are constantly giving them away in TOUs and PPs that we don't even read
From Tony Fish : ownership is framed by your context (geography) and it is not universal.
From Kaliya Identity Woman : I think it is good - to step back and start fresh with principles that are not from the head of one man…(who is highly problematic in how he relates to women and people of color - as evidenced by a string of interactions over the last 5 years) So yeah - I also look for how we get really diverse perspectives of non WEIRD people (western educated industrialized, Rich and democratic).
From Scott David : This is beautiful stuff. We are at the Pupae stage of metamorphosis.
From Karen Hand : In my work we talk about this in relation to an animal - their attributes, the data they generate - where would they fit? Who owns their identity and does it move with the animal - as an example
From drummondreed : @Marc Davis - the EU right to be forgotten is part of #3.
mary hodder : the distance between what is happening and the concept of these 'rights' on screen is huge
From pknowles : Passive items are identified by passive identifiers, a type of identifier that has an association with a cryptographic hash of digital content which acts as an immutable fingerprint to identify a passive non-governing entity, an inanimate object or a static data input. A passive identifier can either be (1) controlled by an active identifier or (2) not controlled.
From Jeffrey Aresty : We can use all the help we can at our upcoming summit, Building the Justice Layer of the Internet, Nov 17-19. Next step is a presentation at this meeting Session 11 - Universal declaration of Digital Identity
From Marc Davis : @Drummond gotcha thx.
From Karen Hand : very relevant in livestock markets
From Tony Fish : individuals, and animals and living things and legal entities and non-legal entities
From Scott David : Living forms are "autocatalytic and entropy secreting" we are among living forms and cannot exist alone. Rights of living forms is associated with limiting how each NIMBYs their entropy exhaust. The SSI
From Scott David : The SSI "constitution" will state responsibilities to other living forms, including humans. Otherwise it is unnecessarily solipsistic. The value add immediately will be for humans to avoid avoidable harms.

From drummondreed : @Jeff Aresty - you should mention your upcoming session before we close this session as it may be of interest to attendees here
From pknowles : It is all about the capacity to govern in the digital realm. Active identifiers identify entities that have the capacity to govern. Passive identifiers identify entities that do not have the capacity to govern (e.g. a cow), an inanimate object (e.g. a passport) or a static data input (e.g. a schema).
From Jeffrey Aresty : The session which Jean (currently speaking) and are running in Session 11 is related to this- Universal Declaration of Digital Identity as a foundation for Universal Declaration of Digital Rights - making it real will require hard work - but it starts here -with the builders of the technology
From PhilWolff : Places can have legal standing. If I recall right, a wild forest/stream was given legal standing so humans could act in loco parentis.
We also need compounded rights, maybe arising from the Agency rights. Families (with various levels of collective identity, delegation), Corporations, Governments, and informal groups (like friends who play a game together).
From drummondreed : @Jeff Aresty - that sounds very relevant to this work
From Scott David : Right now programmers (and their employers) are “sovereigns” - They don’t ask for permission or forgiveness to do this or that thing
From pknowles : In the case of a pet, they would be identified by a controlled passive identifier. A passive identifier (for your dog) that is linked to an active identifier (you, the dog’s caretaker).
From Scott David : That sovereignty is understood by people, who now look to companies to provide vital services, without government oversight. See contact tracing, etc. ; Atheists included
From pknowles : https://humancolossus.foundation/blog/active-and-passive-identifiers
From Karen Hand : Excellent, rights of the community
From Scott David : Nice. Rights of individuals acting in groups
From sheldrake : +1 Jeff.
From PhilWolff : Death. which of my rights survive my bio life?
From Scott David : Beautiful.
From PhilWolff : Can I give up these rights? Surrender them? Or are they inalienable?
From Jeff Doctor : https://www.gida-global.org/care
From Vic Cooper : If I create a thing does it have any right to exist on it's own? What happens if I sell it to you? What happens to the things I create after I die?
From Tony Fish : @phil death of whom, we need to define death.
From Scott David : Hip. Hip. Horray.
From Jeffrey Aresty : @drummondreed - yes, and, this group has the strength to say - this is what we are going to build as a global group and those of us who sign on pledge to work according to these principles in our lives (our day jobs, our volunteer work..)
From Scott David : ALL sovereigns are stories. Not all stories are universally shared. We were one village in East Africa 100k years ago. We radiated around the earth creating different language, food, music, behavior, religions. Now the Internet has brought us together for show-and-tell. Not ever culture is represented.
From Scott David : Not every culture is represented. AND the Internet is commercial.
From Tony Fish : when a pet is in care or abandoned it is under the authority of a legal entity. indeed most birthed pets that are sold are owed by a company and not a person
Scott David : We commodify cultures on commercial internet. What is the “platform” for non-commercialized cultures. Must a culture subject itself to appropriation/enclosure by capitalism in order to survive?
From Jeffrey Aresty : @jeffdoctor - in our program - Building the Justice Layer - Nov 17-19 - we have examples of youth from indigenous culture (Hawaii - Australia) who can benefit from SSI - just one example of empowerment; we need guidance from more people from these cultures and histories

From Karen Hand : Animal's in the ecosystem - their identity and rights will greatly impact how VC's build traceability in food systems
From Kaliya Identity Woman : The next session is European Demo hour ; so we can go past the hour
From Tony Fish : thank you - made me think.
From Vic Cooper : We seem to be are focusing on identifiers. How do these rights extend to connections and communications. Do I have the right to connect directly to anyone? To communicate with anyone. Who can I deny connection and communication with?
From pknowles : It is all about a signing key. If a company identifier requires a signing key to authenticate information, that is covered by an active identifier. A company can be a governing entity (as is a human being, as is a self-certifying IoT device9.
From Jeff Doctor : https://www.culturalsurvival.org/ From drummondreed : Thank you
From Jeffrey Aresty : Session 11 is after demo hour, so our session doesn't start in 17 minutes, but it is the first session after demo hour From drummondreed : Thanks Jeff
Carly Huitema : And pets can be sold to the 'person who cares for the animal' while the other party maintains ownership (common for animal shelters). This way they can recall the animal if it isn't getting care etc.
From pknowles : If you have a very clever dog, maybe they can sign stuff! That dog deserves to be the controller of an active identifier! (Thinking of the clever IIW dog!)
From Tony Fish : +1 @carly
From sheldrake : Jeff, are you in touch with Kaye Maree Dunn re. https://www.ahau.io/ ? … And you may enjoy the session in just over an hour (Breakout G) on generative identity — going beyond SSI.
From Jeff Doctor : yep ; Their work is super cool
From pknowles : KERI can help with the provenance chain re … “And pets can be sold to the 'person who cares for the animal' while the other party maintains ownership (common for animal shelters). This way they can recall the animal if it isn't getting care etc.”
From sheldrake : Jeff …. thought you might be, just checking :-)
From Kaliya Identity Woman : I was just looking up Kaye Maree’s work
From drummondreed : Yes, Generative Identity is really interesting
From Kaliya Identity Woman : to share
From Vic Cooper : My do agrees with you @pknowles
From Jeff Doctor : Me and my team wrote about similar stuff here https://niiwin.ca/ (links to articles at bottom of page) - disclaimer I work for Animikii
From Vic Cooper : My Dog
From Iain Henderson : + 10 Scott, use the Duties
From PhilWolff : In terms of storytelling, consider the Data Seder session. Poets, songwriters, imaginative creatives are welcome.
From Tony Fish : @pknowles - the issue is not provenance and linerage (easy) duties, rights, liabilities, risks and governance appear to be more complex
From pknowles : Oops … gotta run. I’m demoing!
From Carly Huitema : How does the system? description? have a right to change and growth? There will be future use cases that will bring new prinicples
From Vic Cooper : Please come chat with us at the HearRo demo hour!
From Arnon Zangvil : I think this rich discussion is proof that a much larger and more diverse ‘space’ is needed for this discussion\
From pknowles : Tony - Identification is much more simple than that. Can the entity sign or not. Yes = active. No = passive.
From Jeffrey Aresty : @drummondreed November 17-19
From Marc Davis : test the principles on a set of real world use cases. example, personal location data
From [TIOF] Jean F. Queralt : Makes sense to me.

From [TIOF] Jean F. Queralt : For info: UDDR White Paper Draft
https://docs.google.com/document/d/1Id4gIcoDzsZs04EdWZM-5vs5M_nSlheAMb68ZmJwrhs/edit
There's a second document, the UDDR Draft itself
https://docs.google.com/document/d/1y9C-5TPYmRruRQqJq39-HePk3ypWLDpSAEVzuonOH2Q/edit
From Scott David : One approach, that anticipates the contact with existing power structures, is to apply the following general test. For those structures that are “technically feasible” are they also “BOLTS reasonable”. BOLTS is business, operating, legal, technical, social.
From Jeffrey Aresty : @kaliya - thanks!
From PhilWolff : listserv?
From Tony Fish : @scott - with the purpose of influence or to ask for more rules.
From Scott David : Collect practices that are consistent with the principle. Put the practices in a pile and stare at them. Derive best practices/requirements.
From PhilWolff : Example of a practice?
From Scott David : Practices to best practices to standards to institutions then will organically grow into institutions.
From Tony Fish : more rules/ regulation is unlikely to get to where we think we want to be
From Tony Fish : https://medium.com/@tonyfish/power-agency-and-influence-a-new-framework-about-complex-relationships-73f5e97295ef
From Scott David : Practice examples are drawn from BOLTS categories. Like Christopher Alexander work in Architecture
From Katrie Lowe : +1
From Arnon Zangvil : Sounds like a tail wagging a dog :)
From Tony Fish : @scott best practices require maturity …. we are not at ubiquity or known outcomes
From Kaliya Identity Woman : Oh… lets go full post graduate - and work on a pattern language for SSI
From Scott David : It is the tail/dog. Because it is “normative”
From drummondreed : “Pattern language for SSI” <== cool!
From Tony Fish : @marc +1 -1 +1 -1 +1 -1 +1
From drummondreed : “So much data is relational” and has joint rights” <== Marc Davis
From Scott David : @ Tony Fish - That is okay. We can use the old stinky practices as the “Before” picture in the analysis of future practices/duties. Synthesize existing knowledge
From Iain Henderson : Agreed Marc, many of the key data attributes are co-managed.
From Tony Fish : @scott +1
From Arnon Zangvil : @Scott David - tail/dog indeed
From Dan Bachenheimer : looks great... does "CONTROL" include delegation?
From Scott David : Data as Body. Interesting. Autonomy will work well with Hegel and Kant based-identity constructions in EU
From drummondreed : “Data as body” <== Kaliya bringing this as a different “centering point”
From [TIOF] Jean F. Queralt : @Kaliya: I never managed to get an answer from them. ; (Data as body)
From Kaliya Identity Woman : they may be impacted - we need to find resources for marginalized folks and groups to be able to contribute
From Vic Cooper : thanks Drummond!
From Johannes Sedlmeir : @Dan, definitely yes. Many of the design principles rather should be described by "the opportunity to" - like full privacy and full control, but often we may want to relax this by intention
From drummondreed : My pleasure. Thank you to Sankarshan and everyone who contributed to this session!
From Chris Raczkowski : Great work, Sankarshan!
From Melody Musoni : Thank you everyone for this session and all the informative information you shared.
From sheldrake : +1 Scott. Generativity trumps efficiency.
From [TIOF] Jean F. Queralt : Thanks for the session :-D

From Arnon Zangvil : @Kaliya - “Data as body” which I am not familiar with sounds very similar to an embodied media perspective, which is definitely an important perspective that should be integrated into our thinking
From Jeffrey Aresty : Very exciting work - great session
From Jsearls : +1 Scott
From Kaliya Identity Woman : I think these are the notes for the session you are talking about marc - https://iiw.idcommons.net/Metaphors_and_Models_of_WHAT_IS_%E2%80%9CPersonal_Data%E2%80%9D_Implications_for_Policy_plus_Technology
From [TIOF] Jean F. Queralt : @Arnon: Check our Principle I "I am my data".
From Kaliya Identity Woman : maybe this session - https://iiw.idcommons.net/Common_Ontology_for_Personal_Data_Interoperability_%E2%80%93_(Part_2)_The_What_and_How
From Scott David : Good stuff. Thanks everyone
From Jsearls : come to session 11 on generative ssi to discuss what scott was saying about “human scale”
From Arnon Zangvil : Wonderful session! <3
From Tony Fish : you cannot be your data :)
From Scott David : See book “staying with the trouble” (Harriman?). Feminist/ecologist view of identity; Haraway
From [TIOF] Jean F. Queralt : Your data is you. Contextualization.
From Arnon Zangvil : Very much looking forward to session 11!
From Scott David : Complexity and emergence is the action; We are emergent embodiments of “viral promiscuity” through deep time.
From Tony Fish : data is data ….. Heisenberg problem of observation as it creates more data; @scott +1
From sheldrake : thanks Drummond, thanks Joyce, thanks all.

Bypassing eSignature Regulations for SSI Adoption

Wednesday 10C
Convener: Nuttawut Kongsuwan
Notes-taker(s): Catherine Nabbala

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

Thailand is the second country after Canada that officially recognizes Verifiable credential standards.

Thailand has three types of e-signatures

1. Your name, email signatures, scanned handwritten signatures etc that has very low trust level.
2. Using public and private keys (PKI) with medium level of trust
3. Qualified Certificate Authority with high level of trust

    Finema’s approach is to use Hybrid CA/DID model with an approach that has minimal disruption, key rotation friendly as well as prompt DID and VC adoption.
    Advantageous in a way that you can apply Key rotation and use the same certificate.

Eric Welton: VC certificates are the same as X.509 certificates?
Where is the schema for the VC?
How broad is the Government acknowledgement of VC?

Nathan George Has it been approved yet?
Canada is doing the same approach and no need to go through a CA.
We can automate the process and avoid the manual way.
No need to bypass the authorities take an example of digiCert
You can't have a successful holder without preserving transactional privacy
X.509 didn't work very well but there is no way of handling data effectively.

Leah Houston thats the US- DEA, ACGME, NBME
Authorities don't really care about Privacy.They are mainly authoritative.

PBAC 102: Architecting Authorization to Protect Your Data

Wednesday 10D
Convener: Jacob Siebach
Notes-taker(s): Judith Bush, edited by Jacob Siebach

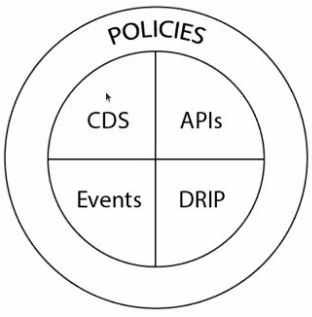
Tags for the session - technology discussed/ideas considered:
Policy-based authorization, attributes for authorization

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

See yesterday: Assuming a domain driven design - domain is the business area and the data in that area. The domain is the authoritative/definitive source.

Policies Protect Data

General Moore's Medallion



Named after Brent Moore, Architect at BYU

Four pillars of IDP: Identification, Authentication, Access management, Authorization

Is the identity attempting to access this resource allowed to do this.

Protect the doman's data. Rely on authorization-important attributes. Does not divulge data (like showing a drivers license to prove authorized to enter an age gated space) Super fast: part of architecture.

How to demonstrate policy compliance without divulging information.

AuthZ Design 1
Must NOT cross domain boundaries

- Tight coupling Eg: to HR database (Nooooo!)
    - Domain that has the data should decide the attribute and not interpreted cross domain from a different attribute
- Security letters

AuthZ Design 2
Invoking the authorization service
Must pass subject, target, client
Must pass policy to be checked
Must allow for other data to be passed

Example: the nuclear lab is the only domain that needs to know principle took safety training, the nuclear lab should be able to provide that to authZ so authZ can make that decision.

From Swapna Radha to Everyone: (11:58 AM): is it a good idea to have a trace on authorization service? To see who accessed what and when it happened? Or, is it a security issue?

AuthZ Design 3
No tokenomics for authz
AuthZ engine lives in trusted network
Engine talks directly to service
Real time

(EG: no one can scan through principles to find a principle that gets the token)

AuthZ Design 4
Attribute Design
Domains created the attributes
Attributes should not be confidential
Business decision, not technical

Compare birthdate to "are you old enough"? Authorization attribute may be derived from PII

AuthZ Design 5
No down-time for domains using authorization
Must be able to update policies in real-time
No redeployment for domain code
Provide authz even when domain down -- domain A depends on domain B attribute; if authZ persists the domain B attribute domains A&B need not be tightly coupled

Challenge by Allan Foster: what about a policy that says “within a 30 days of your birthday” -- is this business logic or authorization? Is the hard stuff now business logic? Now have to couple the domain with the PII pool (the database field) .
Response: is it REALLY the case that that business system wouldn’t have access to the PII to begin with?

Jacob asserts calendaring systems aren’t so much authZ: they are business logic.

The university included a domain for identity. Then the “locker rental” team couldn’t get a list of who has rented lockers because they had to use the ID to look up. So yeah, the locker rental folks could get a self asserted name or a decoupled name, so each domain is responsible for recording the data that it needs for a given identifier. The whole organization maintains the identifiers for each person, but then each domain holds the data that correlates to that identifier for its own business purposes.

(Chuckling over whether a single source of truth is a source of perpetual employment)

Back up to authZ: Jacob asserts the business process that cares about the birthdate . The additional data from the business domain would/could then include IsWithin30DaysOfBirthDate. (But perhaps still better in the business logic to tell user the window of the action)

From Alan Karp to Everyone: (12:14 PM)

Jacob described the authorization process as happening when the request is received. That approach can lead to a confused deputy vulnerability. (https://en.wikipedia.org/wiki/Confused_deputy_problem) It’s better to separate the authorization decision from the request as done by UMA.

Role explosion leads to over provisioning.

Separating access control from authorization is a solution to the Confused deputy problem

An OAuth token with a bunch of scopes is like a role with a bunch of permissions -- if the permissions/scopes are granted based on this policy engine -- it solves a broad set of issues. Alan Karp, poorly paraphrased

What is a “student” vs one domain requiring “in a degree program” whereas another domain “enrolled in X or more hours” -- different attributes

A domain that controls the definition of an attribute does not require other domains to “sign-off” on the definition. This allows an organization to have firm definitions in its policies and bypass the morass of red tape and meetings that come from trying to align attributes for different domains.

Initial Trust

Wednesday 10E
Convener: Micha Kraus, Paul Bastian
Notes-taker(s): Micha & Paul

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

How can we bootstrap trust relationships in a new DID ecosystem?
How can Alice be sure that after scanning a QR Code, she will give her personal data to the right verifier?

In the TOIP triangle scheme only one trust relationship is described.
We look at the different relationship and approaches to establish these connections.

(a) verifier needs to know: Is the issuer trustworthy? (which value do the credentials have?)
(b) holder needs to know: Is the verifier trustworthy? (will the verifier respect my privacy?)
(c) issuer may need to know: Is the holder's wallet trustworthy? How can I prevent misuse of the offered credentials?
Link to document.https://hackmd.io/z-FRlDF6QouUeokp4UT_0g?view

Saved Chat:
From Sam Curren : Governance Frameworks!
From Chris Buchanan : https://wiki.trustoverip.org/display/HOME/Ecosystem+Foundry+Working+Group ; https://wiki.trustoverip.org/display/HOME/Governance+Stack+Working+Group ; https://wiki.trustoverip.org/display/HOME/GSWG+Trust+Assurance+Task+Force
From Vishal Gupta : www.diro.io
From Sam Curren : related to this, but on the user verification side: https://github.com/hyperledger/aries-rfcs/pull/535
From Jim St.Clair : We're working on this in Sovrin and TOIP in a Trust Assurance Framework
From Micha Kraus : https://webgate.ec.europa.eu/tl-browser/#/
From Keith Kowal : https://europa.eu/europass/digital-credentials/issuer/

Ideas to Action: BYOB (Bring Your Own Blockers)

Wednesday 10F
Convener: Scott Harris (Indicio) & Karl Kneis (IDRamp)
Notes-taker(s):

Tags for the session - technology discussed/ideas considered: This session was a "rubber-meets-road" discussion centered on factors that are hindering or slowing adoption.

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

In this session the key takeaway was that the technology is no longer a limiting factor. There have been enough use cases and development to enable useful building and implementation.

The blockers continue to be:

1. Education of both business and technology decision-makers
    1. There is rarely a "simple" story to tell surrounding implementation and understanding of the value propositions. Therefore it is important to focus on problem-solving at the micro level.
2. Competing vision of top-down vs. grass-roots adoption cycles
3. Real world wallet use and interoperability
    1. Making credential holding and use simple for end users in the B2C world
    2. Finding ways to solve for multiple wallets on the same device and credential movement between wallets is important

KERI for Wizards

Wednesday 10G
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:

See slide deck here:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI2_Overview.web.pdf

GS1 Digital Links, Decentralized Identifiers & Verifiable Credentials

Wednesday 10O
Convener: Orie Steele (CTO @Transmute), Kevin Dean (GS1 CA), Phil Archer (GS1)
Notes-taker(s): Margo Johnson (Transmute)

Tags for the session - technology discussed/ideas considered:
GS1 Digital Link, Decentralized Identifiers, Verifiable Credentials,
Supply Chain Applications

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

GS1 Digital Link:

> "The GS1 Digital Link standard extends the power and flexibility of GS1 identifiers by making them part of the web. That means that GS1 identifiers, such as the GTIN (the number in the barcode in almost every consumer item in the world), are now a gateway to consumer information that strengthens brand loyalty, improved supply chain traceability information, business partner APIs, patient safety information and more."
>
> TLDR:
>
> GS1 Digital Links are URLs for exploring linked data related to products that have a barcode or QR Code.

https://www.gs1.org/standards/gs1-digital-link

Decentralized Identifiers:

> "Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity. A DID identifies any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) that the controller of the DID decides that it identifies. In contrast to typical, federated

identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities."

TLDR:

A decentralized identifier identifies a subject, and associates a set of verification methods and services for use related to that subject.

https://www.w3.org/TR/did-core

Verifiable Credentials

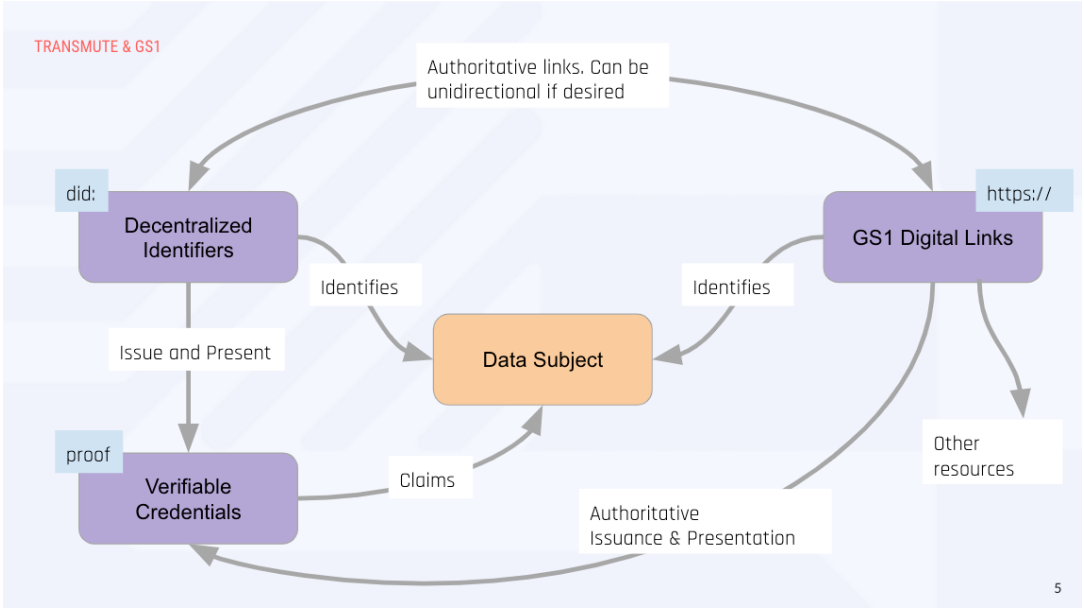
"A verifiable credential can represent all of the same information that a physical credential represents. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts."

TLDR:

A verifiable credential is set of tamper evident, authenticatable claims about a subject. For example: Drivers License, or Board Certified Physician or Certified Organic.

https://www.w3.org/TR/vc-data-model

What is the relationship between these three standards?



-Left side describes relationship between DIDs and verifiable credentials
  -DIDs cryptographically self-certifying, used to present and prove control over keys
  -

-Digital links have authoritative information after the "//"
  -Web resources today make use of this, lots of value here
  -Know that the issuer authoritatively controlled and intended to share access to

-Server is authoritative… and with DL the identifier is authoritative

GS1 DL can be used for authoritative issuance of VCs and VPs
Can create VCs that come from IRI

DID method resolution, example is Universal Resolver… but there are multiple resolvers
-Trusting that multiple web origins will return same DID doc, some trust here

GS1 DL resolution, can also take to multiple resolvers, same opportunity and challenge as DIDs

Question: Verifier missing from this picture… explain in simple terms, how as a verifier do I decide where to resolve a Verifiable Credential.

NOTE: GS1 DL standard also defines a data model and standard for link sets

Verifier reserves right to ignore whatever identifier is presented
Verifier can see either a DID or VC
And can see that they can verify the credential

Kevin: Think of DL as bridge between trusted and untrusted worlds

Question: How different from Certificate Authority?
Different from certificate authority because does not sign public keys
GS1 does issue identifiers, have done so for many years
Now for first time are making identifiers resolvable on the web, including option to link to Verifiable Credentials

GS1 Identifiers clarification: “GS1 is the largest system of identification for supply chains. Orgs, locations, assets, products, shipment. There is a key that may be used to define an individual to a service relationship, but in general - the system is not for the identification of people.” (Gena Morgan, GS1 US).

Right tool for the job? (Assessing pros and cons)

-Digital Link out of the box provides some details about the subject, type information, higher usability with systems today. Disadvantage of correlation.

-DIDs have little trust without Verifiable Credentials. Poor solution for discovery, but higher privacy. Most don’t reveal the type in the DID or DID document itself.

-Verifiable credentials can use both DIDs and Digital Links, VC very useful for confidentiality concerns, presentation and disclosure. Relies on trusting verification method.

TRANSMUTE & GS1

Discovery

GS1 Digital Link: linkType=linkset

```
[
  {
    "href" : "https://example.com/product/ingredients",
    "anchor" : "https://example.com/gtin/614141123452",
    "rel" : [ "https://gs1.org/voc/ingredientsInfo" ],
    "title" : "Ingredients (Ingrédients)",
    "type" : "application/ld+json",
    "hreflang" : [ "en" , "fr" ]
  },
  {
    "href" : "https://example.com/product/pip",
    "anchor" : "https://example.com/gtin/614141123452",
    "rel" : [ "https://gs1.org/voc/pip",
    "https://gs1.org/voc/instructions"],
    "title" : "Manufacturer's description",
    "type" : "text/html",
    "hreflang" : [ "en" ]
  },
  {
    "href" : "https://example.com/gtin/614141123452.html",
    "anchor" : "https://example.com/gtin/614141123452",
    "rel" : [ "alternate" ],
    "title" : "Available links as a Web page",
    "type" : "text/html",
    "hreflang" : [ "en" , "fr" ]
  }
]
```

DID Document

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123",
  "authentication": [{
    "id": "did:example:123#keys-1",
    "type": "Ed25519VerificationKey2018",
    "controller": "did:example:123",
    "publicKeyBase58": "H3C2AVvLMv6…."
  }],
  "service": [{
    "id":"did:example:123456789abcdefghi#vcs",
    "type": "VerifiableCredentialService",
    "serviceEndpoint": "https://example.com/vc/"
  }]
}
```

Notice that DID Document **service** is a gateway to related links.

7

TRANSMUTE & GS1

Verifiable Credentials

```
"credentialSubject": {
    "id": "did:example:456",
    "type": [
      "CertifiedMillTestReport",
      "InspectionReport"
    ],
    "heatNumber": "000005248357",
...

"proof": {
    "type": "Ed25519VerificationKey2018",
    "created": "2018-06-18T21:19:10Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://id.gs1.org/gln/0614141123452#key-0",
    "jws": "eyJhbGciO..."
}
```

```
"credentialSubject": {
    "id": "https://id.gs1.org/gtin/614141123452/ser/12345",
    "type": [
      "CertifiedMillTestReport",
      "InspectionReport"
    ],
    "heatNumber": "000005248357",
...

    "proof": {
        "type": "Ed25519VerificationKey2018",
        "created": "2018-06-18T21:19:10Z",
        "proofPurpose": "assertionMethod",
        "verificationMethod": "did:example:123#key-0",
        "jws": "eyJhbGciO..."
    }
```

Verifiable Credentials rely on trusting a **Verification Method**, which means:

1. Trusting a **Web Origin** and **Transport Layer Security** or
2. Trusting a **DID Controller** and a **DID Method**

8

TRANSMUTE & GS1

Confidentiality

Decentralized Identifiers can be combined with GS1 Digital Link in cases where issuer / subject confidentiality is required.

1. Vendor 1 issues a "Trusted Trading Partner" certificate from their GLN Digital Link, with credential subject being Vendor 2's Decentralized Identifier.
2. Vendor 2 can now prove to Vendor 3 that they are trusted by Vendor 1 without revealing their identity.

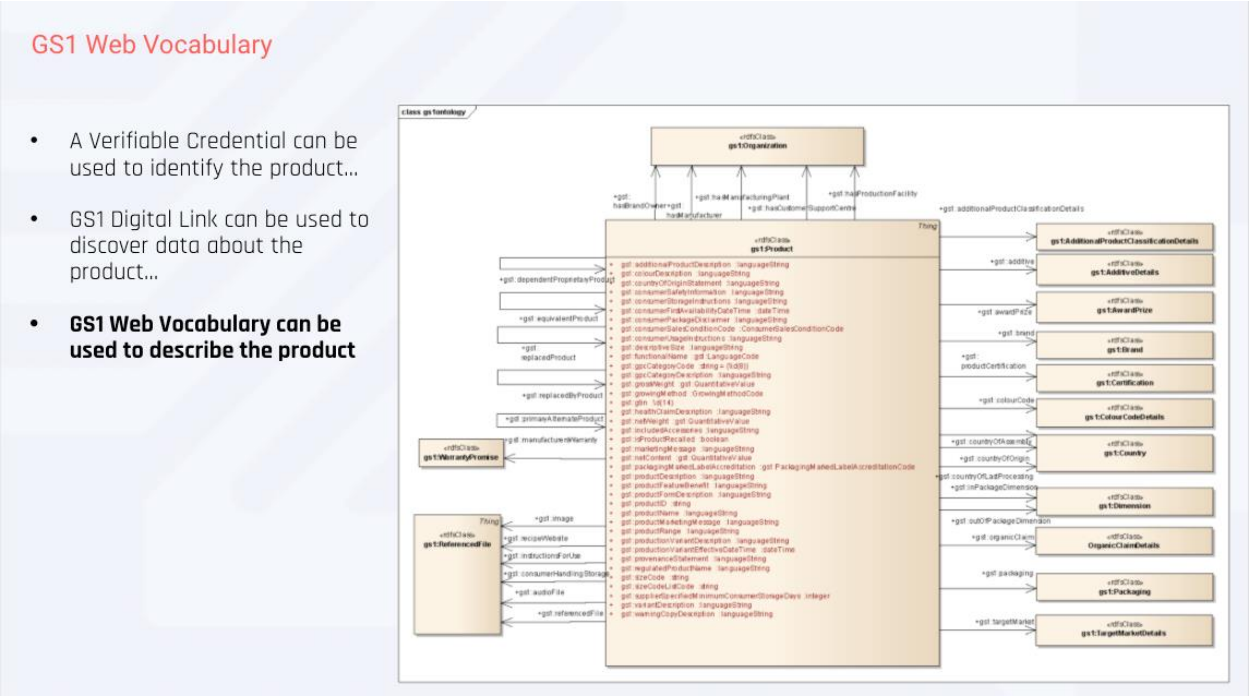
Zero Knowledge Proofs & Selective Disclosure can also be used.

1. Vendor 1 issues a "Trusted Trading Partner" certificate from their GLN GS1 Digital Link, with credential subject being Vendor 2's Decentralized Identifier, with additional property Vendor 2's GLN GS1 Digital Link.
2. Vendor 2 can now prove to Vendor 3 that they are trusted by Vendor 1 with or without revealing their identity (GLN GS1 Digital Link).

9

GS1 Web Vocabulary

- Based on **schema.org**
- Primary focus is **products**, but includes **organizations**, **locations**, **offers**, and **prices**
- Can be asserted as **Verifiable Credentials**



https://www.gs1.org/gs1-web-vocabulary

Links:

- GS1 Web Vocabulary
  - https://www.gs1.org/voc
- GS1 Digital Link Standard
  - https://www.gs1.org/standards/gs1-digital-link
  - https://www.youtube.com/watch?v=9sDrk0bFBN0
- Traceability Shared Vocabulary
  - https://w3c-ccg.github.io/traceability-vocab
- Decentralized Identifiers
  - https://www.w3.org/TR/did-core
- Verifiable Credentials
  - https://www.w3.org/TR/vc-data-model
- Sidetree.js
  - https://github.com/transmute-industries/sidetree.js
- vc.js
  - https://github.com/transmute-industries/vc.js
    - gs1-digital-link/vc.json

Example of Credential:
https://github.com/decentralized-identity/jsonld-document-loader/blob/master/src/__tests__/gs1-digital-link/vc.json

Where to get started for developers with GS1:

- https://gs1.github.io/DigitalLinkDocs/

- https://www.gs1.org/voc/

For deeper notes about traceability go to session notes from yesterday… “Moving Untrusted Data Across Untrusted Parties in Supply Chains” (Session 4, Breakout F)

Enhancement of existing IDs with DIDs
Questions of sensitivity apply just as much to contextualized identifiers (like DL) as they do to DIDs.
Place where public discovery ends

From Chat notes:
From Adrian Gropper to Everyone: Digital Link is a Certificate Authority?
From JC Ebersbach to Everyone: yes, I was also wondering about the security aspect
From naga durga prasad to Everyone: is GS1 better for objects / things than for humans? A muggle asking question here?
From Gena Morgan to Everyone: GS1 is the largest system of identification for supply chains. Orgs, locations, assets, products, shipment. There is a key that may be used to define an individual to a service relationship, but in general - the system is not for the identification of people
From Adrian Gropper to Everyone: q+ to ask about DEA numbers
From Rouven Heck to Everyone: I guess slide 6 includes a lot of statements which are very depending on the context/use-case
From phil.archer@gs1.org to Everyone: Linkset is an advanced Internet Draft we're really hoping becomes an RFC soon https://tools.ietf.org/html/draft-wilde-linkset-07
From Lio Lunesu to Everyone: Q: Could GS1 links be resoled to a DID Doc?(resolved)
From phil.archer@gs1.org to Everyone: q+ to answer Lio
From Rouven Heck to Everyone: + trust in the x509 cert?
From Dmitri Z to Everyone: @naga - that’s a reasonable statement (that GS1 links are better for things and organizations rather than humans)
From phil.archer@gs1.org to Everyone: We're much more concerned with things (products, shipments, railway wagons) than we are people, yes
From Rouven Heck to Everyone: operational security seems like the same in all cases - if you send me your private key/password for your web-resource … :)
From Me to Everyone: https://www.gs1.org/gs1-web-vocabulary
From Dmitri Z to Everyone: q+ to ask about if there’s intentions to integrate with schema.org
From Gena Morgan to Everyone: It is an extension to Schema.org
From JC Ebersbach to Everyone: could you show the credential again?
From Orie Steele to Everyone: https://github.com/decentralized-identity/jsonld-document-loader/blob/master/src/__tests__/gs1-digital-link/vc.json
From JC Ebersbach to Everyone: thx
From Dmitri Z to Everyone: super useful vocabulary, thank you so much
From Orie Steele to Everyone: https://github.com/w3c-ccg/traceability-vocab ; https://w3c-ccg.github.io/traceability-vocab/
From phil.archer@gs1.org to Everyone: https://gs1.github.io/DigitalLinkDocs/principles/
From Simonas Karuzas to Everyone: Have you considered using "did:web"? "issuer": "https://id.gs1.org/gln/0614141123452" could be: "issuer": "did:web:id.gs1.org:gln:0614141123452"
From Melanie Nuce GS1 US to Everyone: DEA numbers are entity/provider identifiers
From Orie Steele to Everyone: Yes, I love did web https://did.actor/ https://did-web.web.app/
From Gena Morgan to Everyone: For those dealing with Class 2 drugs.
From Orie Steele to Everyone: We are working on did:web, but there are a number of privacy issues were are still sorting out in the spec

From Gena Morgan to Everyone: We expect there to be creds from the DEA for those entities, and that will be used as one credential for identity, among many others
From phil.archer@gs1.org to Everyone: https://gs1.github.io/DigitalLinkDocs/
From Orie Steele to Everyone: https://www.gs1.org/voc/ Can someone from my team make the presentation available
From Adrian Gropper to Everyone: q+ to answer about OCA
From Me to Everyone: Most presentation slides and all of the links are in the IIW notes.
From Wayne Chang to Everyone: Just wanted to mention that Adrian has queued himself to add to this. Maybe hand raise?
From Dmitri Z to Everyone: w3c is not english-centric.. it has a ton of internationalization specs; also, JSON-LD specifically (over plain JSON) has excellent internationalization capability
From jonathan holt to Everyone: I should clarify, the vocabularies that we are creating in the w3c DID spec registries are English-focused due to the nature of the contributors. Obviously, w3c in general is very international.
From Dmitri Z to Everyone: @jonathan - yeah.. we should put out a call specifically, for translators etc or just add some PRs with non-english examples
From Leah Houston to Everyone: Come by table 12 to see what we are doing with HPEC!
From Joachim Lohkamp to Everyone: Thank you Orie, Phil and everyone for a great semantified session ;)
From Orie Steele to Everyone: Cheers!
From Swapna Radha to Everyone: Thank you for the great session
From Laura J to Everyone: Thanks!
From Paul DIetrich to Everyone: Thanks Orie
From JC Ebersbach to Everyone: great session, thanks a lot!
From John Walker to Everyone: +1 Orie, very informative
From Dmitri Z to Everyone: thanks Orie!
From JC Ebersbach to Everyone: That's a really great point: enhance existing IDs with DIDs!

Service Delivery and ecosystem management with verifiable credentials (VC), focus on incorporating VC into existing workflows. A discussion of current challenges and opportunities.

Wednesday 11A
Convener: Mike Vesey, IdRamp CEO. Karl Kneis, Idramp COO.
Notes-taker(s): Karl Kneis

Tags for the session - technology discussed/ideas considered:

- Verifiable credentials
- Self Sovereign decentralized identity
- Enterprise and or mass adoption
- Interoperation with legacy Identity Management
- Service Delivery and business alignment
- Ecosystem management

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

Challenges:

- Many ecosystems employ multiple generations of identity systems. Adding verifiable credentials to service delivery is of interest but can appear complicated and expensive.
- Businesses are not eager to replatform identity systems for VC adoption.
- Adoption of many VC solutions generally requires some level of API development and or other skills that are not always easy to procure.
- Many existing services do not support credential verification today.
- Businesses are confused about blockchain capabilities based on crypto currency headlines...Common misunderstandings include the need to re platform, host data on the ledger, and performance is not yet read for production use among others.

Opportunities and IdRamp Product demonstration:

- Education is key - focus on the business problem not the technology. Identify practical business value. Focus on process efficiency, UX, portability and finally security benefits. Avoid technical focus on blockchain unless it is essential to the business problem.
- Focus on interoperability with legacy systems. IdRamp provides protocol translation to incorporate VC into any existing authorization service process.
- Focus on incremental adoption over replatforming. IdRamp provides the ability to issue credentials from any existing data source and add service verification to any relying party bridging interoperability with legacy standard protocols.
- Provide credential management services that do not require developers or special knowledge beyond basic IT service administration. IdRamp provides a user friendly interface that allows service managers to control VC adoption across ecosystems without any special development skills. The IdRamp API provides robust options for ecosystems that want to develop their own solutions but many customers are not prepared for dedicated coding.
- To help harmonize with existing business requirements IdRamps combines VC capabilities with well known capabilities for MFA, Consents, access rules and analytics. This helps business prospects understand how VC can accommodate a wide range of business needs.
- To simplify ecosystem management IdRamp provides segregated trust clients that provide the ability to separate security policies and share service control with other business units/partners. This is more efficient than and easier to manage than traditional federation strategies.

For more information:
Contacts: mvesey@idramp.com, kkneis@idramp.com
IdRamp in action - Service Management Platform demonstration
IdRamp website - idramp.com

Unified Front for SSI/DI messaging

Tuesday 11C
Convener: Juan Caballero, DIF et al

Tags for the session - technology discussed/ideas considered:
#messaging #communications #strategy #ssi #decentralizedIdentity

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

- Introductions
  - Riley - messaging is a blocker for adoption (my session alter)
    - Preaching similar gospels :D
    - Unclear messaging opens doors to copycats
    - Naming session from IIW30
  - Rouven
    - Confusing each other about details and technical definitions (let's kill blockchains! Blockchains are mandatory!)
    - Articulated tradeoffs
  - Matthew Hailstone - BYU, Indy and Aries background, edu-vc projects
    - Spec compliance, platforms, interop - how to zoom out for scoping
  - Tom Jones - User-centricity and UX
    - Dissent
  - Ally Medina - Blockchain Advocacy Coalition
    - VCs and public sector/policy - clearer definitions that aren't controversial in the community ←→ standards-compliance
    - Portability and interop -- too fuzzy
  - Johannes Ernst - IIW regular and cloud liberator - UNHOLY MESS of what it is and what it isn't - just add simplicity - 9/10 of the concepts needs to disappear for a clear common story to emerge
  - David Birch - Digital Identity is what I promote; if I don't understand SSI, how will the general public
  - Karyl Fowler - Difference within the community could be simplified as well - tradeoffs and specializations within the field
  - Sankarshan - I'm going to put the "why I am here" on chat.
    - 20 years ago I was handling "objections" from government departments at India around Free and Open Source Software showing how to evaluate and find the value and user experience. Now, I am doing the same circus around SSI and VC and the somewhat evolving UX does not help. The message needs to abstract what fascinates us and focus on what amazes the intended consumer
- Agenda
  - What do the end-users need to know?
    - Tom: what's the value prop?
    - Riley: Everything in your wallet except the credit card (phone for
    - Dave - functional definition, sure, but what's the link between what SSI is and that? What's diff between VCs and SSI?
    - Matthew:
- Slide 3

- Riley: Market-Terminology dialectic: KuppingerCole uses SSI, SEO/google, Gartner and Forrester-- markets are defined by brands and concepts that can be cut-and-dry
    - VCs and DIDs - not out there in the IAM market yet -- SSI is out there tho
    - Prisoner's Dilemma of branding - no one incentivized to defect!
    - Matthew: Blockchain /DLT/DAG all just "blockchain" outside of specialist circles, the market landed on a dumb, limited set of terms
- Open standards
    - Tom: Incumbent IAM - RAND > open standards :D
    - Bart: Maturity of standards and maturity of products
        - Bickering over VC cred formats - squandering goodwill?
        - Fork in the road: could become PGP or get adoption
- Global final solutions
    - Matthew: Multiple roots of trust, multiple networks - implementation flexibility and standards-driven federation of trust platforms
        - Nuance is in roots of trust
        - Self-regulate on top of that basis
    - Balázs: yes BUT going beyond individual identity and self-representation, lots of other entities have identity needs that would benefit from the same toolkit
        - Self-issued government ID is… silly. Citizenship isn't an opt-in identity system; how to federate L.E.S.S. and the other kinds is important
        - Tom in chat: names on birth certificates is voluntary!
        - Rouven: DID as anchor to which you can bind or unbind data points? Trust platform with multiple poles and power; ID is so much more than a govt ID #
        - Bart: Unbundling credentials - root of trust is already a legacy mental model, perhaps - in general political economy, unbundling seems to shift power from supply to demand (i.e. from issuance to verification/capture/consumption of data);
        - Bart: Every govt wants a DID Method and to own/operate the namespace and have lookup rights on the data; Verifier has more power now
        - Riley: KARYL WHERE YOU AT; some of us are talking about our ENTIRE [human] identities; others are talking about authZ/N (a classic function of IAM); others are talking about B2B credentials; messaging + id cards + b2b creds all in one word?
            - Tom in chat: GS1 is all messaging formats and identifiERS
        - Karyl: Our customers (metals manufacturers, for ex.) - we almost never say id and never say "blockchain"- we talk *business* cases, not use cases
            - Even coming here or working on standards is a code-switch
        - David: people (and govts) want to own DIDs - we all seem to share a vision of all people having 12 DIDs at least; govt cases are a "special" not a "general use" case… contextual privacy & separation of concerns?
        - Rouven: Tradeoffs, not argue for "best solution" or "general solution" - shift the focus from "dids" and infrastructure ownership, to "credential value" - forget whose DID it is, decide what creds you want to assign to it
    - Axis of trackability and decentralized Palantir
        - Kaliya: Keybase problem: aggregation and disaggregation - federating public identities (opt-in aggregation) while preserving disaggregation (private life and personal life)
        - Ally:
    - Bart: Solution focus - Sometimes we sound like two preteens fighting over their toys?
        - Bart: No one wants to manage their keys-- keep our eyes on the prize of making KMS usable and making data governable?

- //Blockchain - huge disruption that opens up new solutions - what does VC enable?
- People will not adopt SSI because privacy - our convenience needs to beat their convenience - what is the Uber-like or Google-like convenience this enables?
- Kaliya Young - Everett Rogers - Diffusion of Innovation (1962) - theory about adoption of tech (written about seed experimentation among farmers) - //Geoff Moore's Crossing the Chasm but more academic
    - 5 stages: knowledge and awareness ; persuasion; decision confirmation ;
    - Bart: I preFer Nunes' Sharkfin model
    - Kaliya: We need to get over 3-sided markets
    - Kaliya: Trialability, observability, Proof-of-conceptability :D
- Kaliya: If adoption is our goal, we need to look at scientific analyses of adoption and innovation
        - relative advantage
        - Compatability
        - complexity/difficulty to learn
        - trialability/testability
        - potential for reinvention observed effects
        - Potential adopters evaluate an innovation on its relative advantage (the perceived efficiencies gained by the innovation relative to current tools or procedures), its compatibility with the pre-existing system, its complexity or difficulty to learn, its trialability or testability, its potential for reinvention (using the tool for initially unintended purposes), and its observed effects. These qualities interact and are judged as a whole. For example, an innovation might be extremely complex, reducing its likelihood to be adopted and diffused, but it might be very compatible with a large advantage relative to current tools. Even with this high learning curve, potential adopters might adopt the innovation anyway.

        - Bart: I feel like we're solving for the old paradigm- individual versus platform barons = legacy problemset; let's look instead at p2p mental models- why doesn't the bank log into me? We are stuck in hierarchies and power assymetries instead of looking at what we can change

- Karyl: I want to hear more about p2p and bidirectional usecases (outside of healthcare?) -
    - David Luchuk: Healthcare (Canadian context) - I go right to Bouma and Jordan's govt svcs delivery - "directionality" of services - each service a node on a network with separation of concerns; DIACC: govt service as good mental model of agencies logging into citizens; reversing the directionality of "onboarding"
    - Bart: My example for Karyl - every service/bank/business that ever sent you an SMS or a letter with a PIN number in it goes away

because they know how to find you, they onboard themselves to you…

- Moi: Secure Channel
  - Bart: What you issue is the secure channel (not technically true but it's true in business-case terms when talking to a sovereign) - i issue you a visa, and that opens a secure channel to you in an emergency abroad
  - Bart: "I just want it to work like WhatsApp" - multisource/threshold credential-based authentication - news governance model opens up right there
  - Bart: P2P governance - this is what people want
- Margo: My house, my rules - if you don't have a house, you don't really have authority to impose rules. SS (in B2C) gives each holder an address for their house
  - Privacy and regulatory
  - In B2B this is easier to understand - they WANT discoverability (partic for M2M and API businesses :D)
  - Find a vector where the power dynamic can be

After OAuth2: ZCAP or GNAP?

Wednesday 11D
Convener: Adrian Gropper, Invited: Orie Steele, Dick Hardt, Alan Karp
Notes-taker(s): Judith Bush

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

Introduction
OAuth2 is expiring - confusing, poor for Zero Trust Architecture
Authorization Matrix

	Store	**Process**
Clear Text	Directory	Lab
Encrypted	Encrypted Data Vault	Intel SGX

Dmitri Zagidulin: "My only request is - please underscore that GNAP is a protocol and zCap is just the data model (is compatible with GNAP as a protocol.)"

See Secure Data Storage Authorization Slide Deck (which explains the relationship between OAuth2, GNAP and zCaps)

Initial Chat:
From Wayne Chang to Everyone: (2:03 PM) See also https://w3c-ccg.github.io/zcap-ld/
https://lists.w3.org/Archives/Public/public-credentials/2018Nov/0099.html
From Sascha Preibisch to Everyone: (2:03 PM) Can this session be recorded?
From Dmitri Z to Everyone: (2:04 PM) @Sascha - Adrian is recording it, yeah
From Sascha Preibisch to Everyone: (2:04 PM) thank you
From Orie Steele to Everyone: (2:05 PM) See also https://github.com/decentralized-identity/secure-data-store Can we get google doc link in chat
From Dmitri Z to Everyone: (2:05 PM) @Adrian - I'd love to say a few words on zCaps + GNAP from our SDS WG slide deck https://docs.google.com/presentation/d/1QEHSs4XJ05yQl2mvpiqbM80-MySxlVI9cNDLPq_XkkY/edit

Adrian gave an introduction -- OAuth 2 ill-suited for institutional users. Projects on smaller scale, less self sovereign -- eg : health care -- OAuth not working

Zero trust architecture has SSI as a building block (NIST definition) (SP800-207)

Adrian asks: How do we work with ZCAP & GNAP given the matrix:

	Store	**Process**
Clear Text	Directory	Lab
Encrypted	Encrypted Data Vault	Intel SGX

Here the values are examples of systems that might meet a system that stores clear text or processes encrypted data (confidential computing).

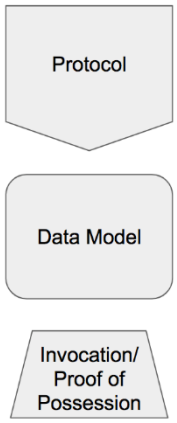
Aaron Parecki - OAuth framework can work in a decentralized space -- eg see IndieAuth (indieauth.net) extension in the IndieWeb ecosystem. (There are ways to adapt it)
https://aaronparecki.com/2018/07/07/7/oauth-for-the-open-web

Chat says Aaron wrote /the book/ on OAuth2 (as well as a fantastic website)

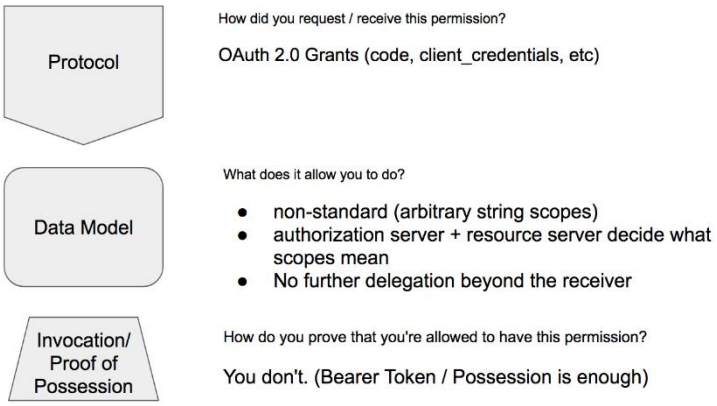
Dimitri starts slides:
https://docs.google.com/presentation/d/1QEHSs4XJ05yQl2mvpiqbM80-MySxlVI9cNDLPq_XkkY/edit

Encryption plus authorization required: neither alone is sufficient.

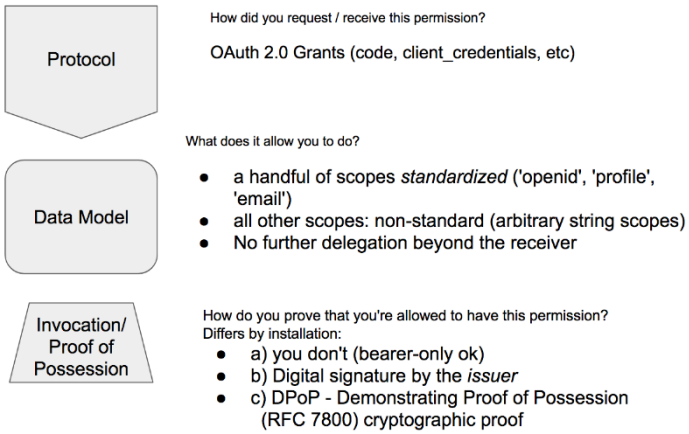
Authorization - 3 components

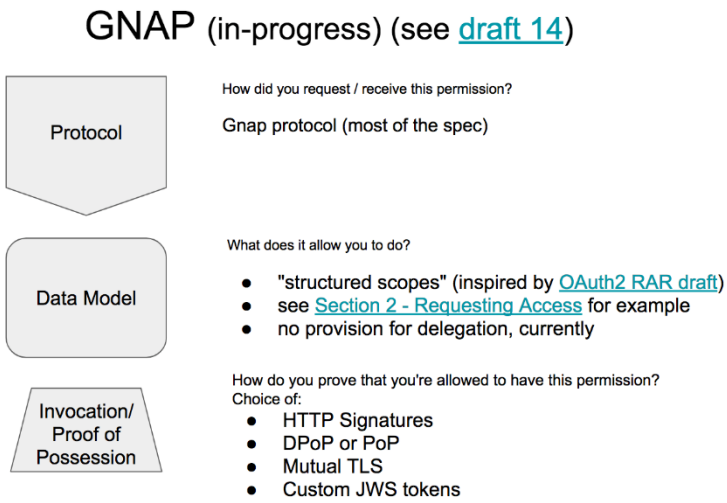


OAuth 2.0 (Classic)



OpenID Connect / Advanced OAuth 2.0





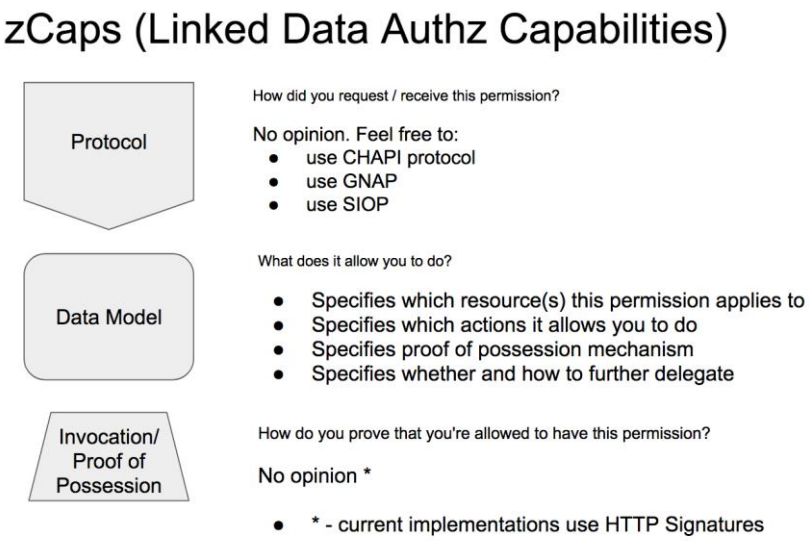
GNAP draft 14 * OAuth2 RAR
Draft 14 was still and individual draft
WG doc is https://datatracker.ietf.org/doc/draft-ietf-gnap-core-protocol/

Example:

```
[
  {
    "type": "example.com/resource-set",
    "actions": [
      "read",
      "write"
    ],
    "locations": [
      "https://server.example.net/resource"
    ],
    "datatypes": [
      "metadata",
      "images"
    ]
  }
]
```

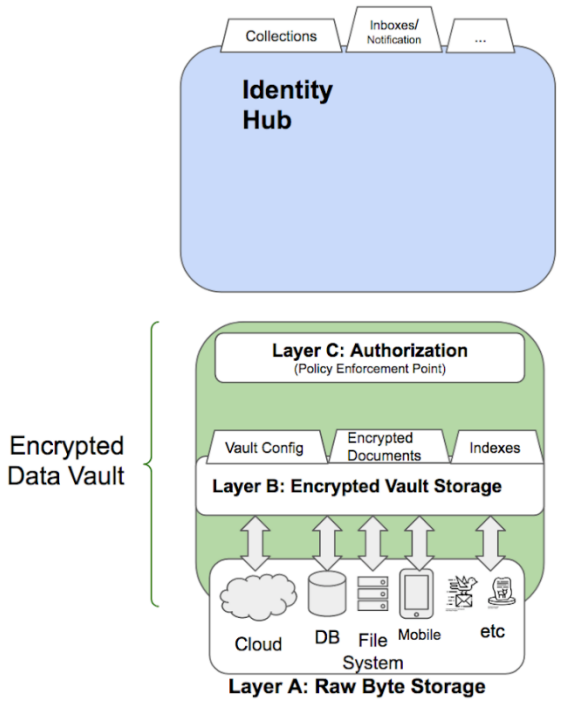
Intent is type can be standardized by different bodies. The three verbs below are NOT part of GNAP/RAR - an example . GNAP and RAR are the same thing. Driven by European FinTech.

Authorization : request phase with list of wanted, response with get



Would verifiable credentials be usable for authorization? This is a data model to attempt to do that.
Example:

```
{
   "@context": ["<security context>"],


   "id": "urn:uuid:....",

   "invocationTarget": "/edv/z4sRgBJJLnYy/docs/zMbxmSDn2Xzz",


   "invoker": "did:example:abcd",

   "allowedAction": ["read"],

   "parentCapability": <optional - this is for delegation>,

   "proof": { … }
}
```



Hub* Permissions:

- Full scopes TBD
- Rich, complex (see Web Access Control spec for example)
- APIs

EDV Permissions:

- Tightly constrained standard scopes
- CRUD on: documents, configs, indexes
- Delegatable
- Portable

Very nice notes

Going back to the very beginning - the sentiment that OAuth2 is "expiring" but in reality - practitioner in large and small projects -- UMA barely registers, SSI and these protocols aren't even hinted at. Unlike SAML (no innovation) there are still innovations occurring in OAuth2. Don't misrepresent OAuth2 "expiring" outside of the "magic bubble" of IIW! -- Vittorio Bertocci

Question: confirming that GNAP just requires type in the RAR object, thus ZCAP can fit in just perfectly. -- YES.

OAuth2 useful -- but perhaps not in the Zero Trust context. Considering Zero Trust as a security architecture … how far can we get **without** SSI?

14:34 EDT (for comparing with chat)

SAML is still the broadly used interop, to keep in mind as we discuss OAuth2 as "dead."

GNAP helps with bootstraping up trust.

Dick Hart - in GNAP we are focusing on authorization, but the grant server can **ALSO** provide claims. What about asking for verified credentials from the grant server.

Sasha: In OAuth2 an issue with scope -- not just permission, but also scopes can influence protocol, switch from default behavior. Eg: openID request can return different data. The scope is used because it's available. Can GNAP help communicate to server to handle a request in a different way than default.

In GNAP, there is a full JSON object so scopes are not the only signal. Another GNAP top level object can extend.

In UMA it was addressed because sometimes the server is subject to jurisdictional constraints independent from authz, … is there a notification channel built in the protocol? The separation of authZ from resource creates a need for the resource server to communicate back that the service had to do something different from what was requested.

One of the reasons to drag OAuth2/OpenID Connect into SSI is because it has ten plus years of experience of implementation -- when DIDs start living in web browsers the OAuth2 community can explain.

Problems “with” OAuth are often problems with the environment, like the browser and app stores, and a new spec can’t solve those issues.

How does secure computing (eg: Intel SGX) -- hosted -- affect?

The client credential solves two different problems.

Why should a resource care about the client app and not the user behind the app? The challenge is phishing or other siphoning off of the protected data. There’s a debate as to whether this is important or not. This was litigated in the API task force of the health care space.

Managing client secrets makes OAuth2 complicated. If you could ignore that it would be much easier. In browsers you can confirm the application with the URL.

Knowing which device (the hardware secure computing) is orthogonal to knowing the application.

GNAP starts backchannel. If you got it, it really was you.

Zero trust - the idea of moving from “clam shell” (firewall the soft area) -- to where authorization very close to the services. “Opposite of perimeter” -- well, the perimeter has gotten very small (eg the pod in kubernetes).

Where are the logs and how do you monitor when there is no “hard outer shell”? When everything authorized as close to the resource as possible, how do you monitor?

SSI vs OAuth -- both are types of credentials, where OAuth is very constrained. SSI and ZCAP (could be verifiable or some other type). OAuth vs GNAP - some of the complexity of OAuth is that not all people have same environment. OAuth has only one type of token - -access (refresh not really). OpenID Connect expands the scopes on the token to communicate more to the server. Hoping that GNAP will address the additional pieces ; not just access, but credentials in a wallet, etc. - David Waite

Orie proposes a hypothetical scenario:

Alice & Bob both have DIDs. Alice wants to access Bob’s sensitive data. Alice only knows of Bob’s authZ server (GNAP). Alice can ask Bob for access to a secure resource. Bob’s access server can grant, Alice can take that grant as a header in a http request and to access the secure resource from a third party.

Would this work?

Dick likes it up to “everyone has DIDs”. How does Bob share with Alice today?

Use the service section of the DID to point to GNAP. DIDs identify subjects. Bob & Alice want identifiers for each other that are independent of third party (like google or facebook).

Adrian's restate: Given the authZ server advertising Some Protocol. Do we have a consensus for how that authZ server interops with Alice, Bob, and the Resource?

Alice and Bob have different GNAP servers. How does Bob's GNAP know who Alice is to provide the authorization? Bob gives Alice's DID to his OAuth token…

Alan Karp asserts this is where we want redelegation -- Bob gets a token to give to Alice.

Alice has to sign the HTTP request -- don't want simply a bearer token.

A BRIEF DESCRIPTION OF THE GNAP GRANT OF CAPABILITY AND TRANSACTION WITH RESOURCE SERVER:

Alice and Bob are identified with DIDs.
Alice and Bob have GNAP servers in their DID Document service section.
Alice and Bob start a romantic relationship, Alice wants to ask Bob for his STD test.
Alice requests Bob's GNAP server for STD Test Resource authorization.
Bob generates an Authorization Capability (ZCAP) to the resource in an encrypted data vault.
Alice invokes the ZCAP via an HTTP Signature to download the STD Test from a 3rd party service provider.
Alice is able to confirm that Bob has been tested, and they are happy together using DID, GNAP, ZCaps and HTTP Signatures.

Bengo asks for a library for auth that has pluggable strategies. Orlie says the PKI / raw digital key libraries are the only commonality.

---------- Comment added by Alan Karp after the fact ----------

Mark Miller is so unhappy about the "do not delegate" feature that he's considering taking his name off the zcap-ld spec. I feel strongly about it, too.

Trying to prevent delegation is futile as long as credential sharing is possible or confinement is not possible. The feature just makes systems harder to use while leading to weaker security. A user with a permission can share a credential, e.g., password or private key, with someone who does not have that permission, which often leads to giving up too much permission. Without confinement, someone with a permission can proxy requests for someone who does not. Both ways of getting around the restriction make responsibility tracking harder if not impossible.

There are extreme environments in which credential sharing can be prevented or users can be prevented from communicating, e.g., NSA. Is it worth penalizing the larger market with a feature that will be widely misused just to support such niche uses?

Instead of a "do not delegate" mechanism, we implemented something we called Voluntary Oblivious Compliance (VOC) that allowed people to obey a policy they had never heard of. In this context "Please do not delegate" translated into a popup that told the user to "Please explain to your manager why you are violating the blah blah blah policy." (Truth be told, our project was cancelled before we built the

popup.) Most of the time, the reaction would have been to not continue with the delegation. However, it is likely that the user would proceed if a $10M contract was on the line.

SAVED CHAT:

From James Manger : Where is ZCAP on the web?
From Orie Steele : https://github.com/digitalbazaar/http-signature-zcap-invoke ; https://w3c-ccg.github.io/zcap-ld/
From Wayne Chang : See also https://w3c-ccg.github.io/zcap-ld/
From Wayne Chang : https://lists.w3.org/Archives/Public/public-credentials/2018Nov/0099.html
From Sascha Preibisch : Can this session be recorded?
From Dmitri Z : @Sascha - Adrian is recording it, yeah
From Sascha Preibisch : thank you
From Orie Steele : See also https://github.com/decentralized-identity/secure-data-store ; Can we get google doc link in chat
From Dmitri Z : @Adrian - I'd love to say a few words on zCaps + GNAP from our SDS WG slide deck https://docs.google.com/presentation/d/1QEHSs4XJ05yQl2mvpiqbM80-MySxlVI9cNDLPq_XkkY/edit
From Dick Hardt : GNAP docs https://datatracker.ietf.org/wg/gnap/documents/
From Vittorio Bertocci : https://docs.google.com/document/d/1u1CmtCZaqbJM8HIdnv9RaXgUEnWOrFoJZpMe4vdq0aI/edit
From JC Ebersbach : https://docs.google.com/document/d/1u1CmtCZaqbJM8HIdnv9RaXgUEnWOrFoJZpMe4vdq0aI/edit
From Adrian Gropper : https://2.qiqochat.com/breakout/14/iiw31
From Dmitri Z : Aaron wrote /tha book/ on OAuth2 (as well as a fantastic website)
From Dick Hardt : OAuth 2.1 is intended to make OAuth 2.0 easier https://tools.ietf.org/id/draft-ietf-oauth-v2-1-00.html
From Dmitri Z : https://docs.google.com/presentation/d/1QEHSs4XJ05yQl2mvpiqbM80-MySxlVI9cNDLPq_XkkY/edit
From Alan Karp : Is GNAP what Justin called OAuth XYZ?
From Orie Steele : Yes, its the next evolution of that
From Dick Hardt : @Alan — yes
From Dean H Saxe : Alan yes.
From Dick Hardt : AKA Transaction Authorization TxAuth ; GNAP -> Grant Negotiation and Authorization Protocol ; The hope is that GNAP requests are RAR
From Orie Steele : @dick hard please que to explain head shaking :) ; Sorry spelling :(
From Dick Hardt : @Orie … :)
From Kevin Dean : Would VCs be an appropriate method for proving authorization?
From Terry Hayes : SPKI
From Wayne Chang : @Kevin would appreciate answers to that question too
From Dmitri Z : @Kevin - great question. So, VCs are basically just the Data Model part of the authorizations. and zCaps are "VCs used for Authorization"
From Wayne Chang : @JoeA if you're around, is this congruent w/your conception too?
From Joe Andrieu : So far… : =_
From Wayne Chang : Is it a fair characterization that zCaps are the marriage of structured authz scopes + RDF?
From Terry Hayes : Because HTTP signatures aren't confusing?
From Joe Andrieu : @Wayne, I'd say delegatable structured authz scopes in RDF as JSON-LD
From Dmitri Z : @Wayne +1, what Joe said
From Alan Karp : I'm not sure that ZCAP has a "whether to allow relegation option." That's a mistake made in SPKI.

From Dmitri Z : @Alan - it does, yes ; (have that option)
From Wayne Chang : I wonder about any widely used production impls of SAML2 using RDF
From Alan Karp : Ouch!!
From Dmitri Z : +1 to what Vittorio said. I think we are all huge fans of OAuth2 here.
From Joe Andrieu : +1 to be careful about the hype. we're in this together.
From Kristina Yasuda : +1 Vittorio
From Dale Olds : Always great to hear from Vittorio!
From Wayne Chang : yay
From Lio Lunesu : bravo
From Aaron Parecki : +1 to Vittorio, and don't forget that there is a lot of experience in the OAuth community to be learned from, otherwise whatever new thing SSI does will make the same mistakes that OAuth made at the beginning
From Harpreet singh : Dynamic OAUTH 2 referesh may to some extent go in space of Zero Trust ; ?
From Vittorio Bertocci : <3
From James Manger : "Zero Trust" is a very generic term … but I'm not sure it has much connection to SSI
From Harpreet singh : agree
From Adrian Gropper : +1 to GNAP helping with Dynamic Client Registration
From Orie Steele : https://mattrglobal.github.io/oidc-client-bound-assertions-spec/
From Dmitri Z : @Dick - Tobias's session on SIOP is very much involved in requesting VCs as OIDC/OAuth2 claims
From Orie Steele : ^ thats the link I just posted above.
From Dmitri Z : there's a lot of good work on that in DIF ; thanks
From Dick Hardt : @Tobias - when is that session? ; @Dmitri I mean
From Kristina Yasuda : session 14 today ; in 3 hour-ish
From Dmitri Z : ^ +1
From Oliver Terbu : "SIOP - progress on the laundry list (wrt DID)"
From Kristina Yasuda : idea is to allow VC/VPs to be sent back in OIDC response
From Dick Hardt : @Dmitri thanks! — I will check it out
From Vittorio Bertocci : +1 Aaron!!
From Dmitri Z : I can answer that (re application id) ; (s' all good, it's a big topic (why client identity etc))
From bengo : as a service provider, I don't want to let anyone use my service, unless I can understand which Clients (apps) are requesting my service at different ratios. It may not be profitable to offer the service unless Client A is blocked.
From James Manger : My browser will run javascript on my PC from any site
From Dmitri Z : let's come back go GNAP etc tho
From Joe Andrieu : +1 for not depending on client validation.
From bengo : PART of the authorization policy is 'what client is the end-user using?'. Let the service provider shape the policy that they need to make their part of the ecosystem sustainable.
From Vittorio Bertocci : This is a very deep rabbit hole, we could easily hijack the entire session
From Harpreet singh : Thanks Aaron
From Orie Steele : Phishing access tokens and exploiting oauth ; Proposed session
From Harpreet singh : There are POP and PKCE standards to prevent phishing to some extent not all use cases
From bengo : It's interesting to have an 'identity' for a person, each of the devices they use, each of the device<->app pairs to prevent tracking, and additionally a delegated keyPair that is only used for the length of one session.
From Kristina Yasuda : pairwise identifiers?
From bengo : yes
From Tim Cappalli : +1 for Wayne's ZT explanation

From Orie Steele : Obviously this guy has never accidentally eaten a pearl :)
From Dmitri Z : lol
From Tim Cappalli : Continuous reauthorization as well.
From Harpreet singh : Continuous re-auth means refreshing Oauth dynamically and silently ?
From Orie Steele : Distributed logging at scale ; Another session topic
From Dmitri Z : many logs. so many many logs. just everywhere.
From Dick Hardt : HAA ; HAHA
From skyberg : I see Zero trust as the reduction of intrinsic trust. Hard outer shell assumes we only need to authorize at that shell, and not internally.
From Dale Olds : Can't quite let the previous discussion go, so here is more. I could not disagree with Terry more. From my perspective and experience, being able to constrain what authorization a user CAN delegate to a particular app is essential -- therefore you need to know what app is asking for the user's authorization. The point is to constrain what the app can get at the AS.
From Tim Cappalli : @Harpreet, not necessarily. CAEP / SSE is being built to reduce the need to reissue tokens in some cases
From bengo : Service Mesh can help detect intrusion without needing logs that contain PII
From Tim Cappalli : *designed, not built
From Dick Hardt : @Dale +1
From Dmitri Z : +1 Dale
From Vittorio Bertocci : +1 to CAEP
From Aaron Parecki : @Dale exactly. there are plenty of cases where that is the case. There are also times where that is not the case, which should absolutely be supported in a protocol as well! (That's what we've done with IndieAuth in fact!)
From bengo : +1 Dale. I want to authorize a Client to read my email address, but not my home address.
From Terry Hayes : Of course you need to know what app is asking the user, but the resource server doesn’t need to know.
From Dick Hardt : GNAP simplifies doing CAEP as the Grant URI can be used to link user, client, and server
From bengo : If I’m operating the resource server, I demand to know for ‘business reasons’.
From Vittorio Bertocci : the client identity as part of authZ was the reason I tried to get a claim in the JWT AT indicating the client verification strength... but no one wanted to play :P
From Dmitri Z : @Vittorio - oh NICE. I so wish we had that! ; what was the claim? ; (let’s resurrect it :))
From Dick Hardt : GNAP — pronounced guh-nap
From bengo : ‘Client app’ is in the realm of the provider’s problem domain, not the protocol. If what Terry is saying is it shouldn’t be ‘required’, I agree with that probably.
From Vittorio Bertocci : @Dmitri few options were floated... if you want to resurrect, the draft just entered IESG review - chime in on the oauth WG! :)
From Aaron Parecki : @bengo depends on the scope of the protocol
From bengo : +1 Aaron ; Loki: Aaron Parecki’s karma is now 1
From Aaron Parecki : if it's just an oauth client to server thing then i agree, but OAuth has grown to encompass RS + AS comms as well, and then it becomes necessary
From Dmitri Z : @Vittorio - do you have a link handy perchance?
From Wayne Chang : @vittorio FranceConnect seems to have made a keycloak extension to oidc that creates different “eIDAS levels” for authz ; https://github.com/InseeFr/Keycloak-FranceConnect/blob/master/src/main/java/fr/insee/keycloak/provider/FranceConnectIdentityProvider.java#L108 ; “ FranceConnectIdentityProvider extends OIDCIdentityProvider implements SocialIdentityProvider<OIDCIdentityProviderConfig>”
From Terry Hayes : @Aaron - if you want a tunnel through the app to allow comms between RS and AS, then that needs to protect in its own right.

From Vittorio Bertocci : @Dmitri the draft is in https://tools.ietf.org/html/draft-ietf-oauth-access-token-jwt-10 ; @wayne thx!
From Dmitri Z : thanks!
From Vittorio Bertocci : got to drop for a conflicting meeting, but will come back to the notes to see if there are followups. thx!
From Aaron Parecki : @Terry that's not what I'm talking about. I just mean that the spec may or may not include definitions of comms between different parties. OAuth started just between client and AS and client and RS, and now has extensions to define AS/RS comms as well, such as that access token spec vittorio just linked above.
From Alan Karp : Mark Miller is one of the ZCAP authors and said, “Cannot be true.” when I told him “do not delegate” was in the spec.
From David Waite : While OAuth does not make the separation directly, you also have a separation in some cases by the accessing client and the authorizing agent - that might be a local browser in code/implicit, a remote browser in device flow, a mobile device and push in CIBA, etc
From Leah Houston : the documents could be fraudulent….
From Dmitri Z : @Alan great point (that Mark Miller & the OCap community has a LOT to say about trying to restrict delegation”
From Terry Hayes : @Dmitri - yes we do! ; From Dmitri Z : :)
From Wayne Chang : did:not ; From Dmitri Z : ::facepalms:: ; From Ken Adler : lol
From Neil Thomson : How does Bob assign the access token only usable by Alice
From Dmitri Z : @Neil not sure how to put it in OAuth2 terms. but something like - Alice will be in the audience / azp claims
From Oliver Terbu : + HTTP signatures when invoked/used
From Neil Thomson : @ Dmitri how to map an audience to Alice in a secure manner (Alices DID as the audience)?
From Oliver Terbu : You could use DIDs for that
From Harpreet singh : Is it the signature of Alice on response to bob’s authorization
From Oliver Terbu : DID -> resolve DID -> public key -> verify HTTP signature
From Alan Karp : @Neil: Bob asks Alice for a public key and creates a new JWT issued to that key.
From Harpreet singh : Thanks Oliver
From Neil Thomson : @Alan - thanks, closes the loop..
From Dick Hardt : @Orie — when you say HTTP Signing — which spec are you referring to?
From Aaron Parecki : good question there are so many!
From Orie Steele : The expired one Justin is partially responsible for at IETF :)
https://tools.ietf.org/html/draft-richanna-http-message-signatures-00 ;Its mentioned in GNAP as well; right
From Aaron Parecki : how does that one relate to the earlier one that is now under http?
https://tools.ietf.org/html/draft-ietf-httpbis-message-signatures-00
From Ken Adler : I always think of an agent utilizes a wallet
From Joe Andrieu : it's a lovely rabbit hole, the wallet / agent discussion
From Dmitri Z : @Aaron - same spec
From Wayne Chang : Could a VP-style presentation be used by a zCap’s invoker for authentication?
From Dmitri Z : not sure why it’s under 2 URLs like that, or which one’s earlier ; @Wayne - yes.
From Wayne Chang : cool
From Colin Jaccino : The second http signature spec was after the draft was picked up by the httpbis working group
From Dick Hardt : IETF process — individual draft’s get adopted as WG drafts
From Joe Andrieu : +1 to trusting the crypto instead of trying to verify a particular software client
From Dmitri Z : -1 to only asymmetric :)

From Orie Steele : Post quantum resistance is one reason you might object to requiring assymetric ; But there will be solutions there as well
From Wayne Chang : https://github.com/WICG/WebID
From bengo : Is it like a hipster thing why I get SSL_ERROR_BAD_CERT_DOMAIN on https://gnap.io ?
From Orie Steele : lol
From Dmitri Z : hahahahah
From Orie Steele : Apparently not ; Because the cert is not mocking
From Wayne Chang : I still propose an example implementation of gnap using a music sharing service called gnapster
From Orie Steele : Its github
From Judith Bush (she her) : yes, thank you!

Components for Aries/Indy Agents

Wednesday 11E
Convener: Andrew Whitehead (BC Gov)
Notes-taker(s):

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

Slides:
https://drive.google.com/file/d/1mnkyR3kbzcZaR0aycoJs3Z2W1BE0G5SD/view?usp=sharing

Dealing with Import/Export Wallets: What about malicious wallets?

Wednesday 11F
Convener: Kyle Den Hartog
Notes-taker(s): Kyle Den Hartog

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

We considered a few different approaches to this problem and still consider it a relatively unsolved problem at this point. Based on our discussion it seemed that the direction of the room preferred the route of a allow list type system (potentially the path of trustmarks via trust frameworks) with the understanding that there's definitely tradeoffs. Probably the most concerning tradeoff is that an allowlist would naturally create a long tail curve distribution which could create centralization based on market dynamics.

Generative identity — for psychological, sociological, and ecological health (aka the dystopia of SSI)

Wednesday 11G
Convener: Philip Sheldrake
Notes-taker(s): Drummond Reed, all contributors to the chat during the session

Tags for the session - technology discussed/ideas considered:
Generative identity, relationships, psychology, sociology, law, problems with SSI, dystopic

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

We are working on a transcript of the session. Philip gave a presentation based on his chapter of a forthcoming SSI book called The Dystopia of Self-Sovereign Identity. The points he made in his presentation are all captured in that chapter and in the rest of the new site called Generative Identity.

The next steps is continued conversations and decisions about how to make many of these key points about the problems with SSI actionable.

Following is the **very rich** chat that went on throughout the session.
11:02:30 From Hunter Cain : 1 in the morning here haha
11:03:15 From mary hodder : record away
11:03:15 From Scott David : No objection
11:03:18 From Bob Wyman : Please record.
11:06:00 From mary hodder : have read and taken grad classes in all of that, but I'm not an =ist
11:06:21 From mary hodder : just interest-ist
11:07:04 From Scott David : SDG goals is nice global inventory of challenges to start with for myriad identity facets.
11:07:30 From Scott David : Need tech and social structures to facilitate horse trading within and among SDG silos.
11:07:56 From Scott David : Fungus did it first?
11:09:29 From Scott David : Tech is hard - humans are soft. Tech is digital - humans are analog. Need harmonic coupling, not smashing. Existential Crumple zone
11:09:58 From mary hodder : Humans are messy. Really messy.
11:10:06 From windley : https://www.windley.com/archives/2020/08/cogito_ergo_sum.shtml
11:10:41 From drummondreed : "Existential crumple zone" <== fascinating, Scott. More?
11:10:44 From Bob Wyman : I don't have a birth certificate. (I have a "consular report of birth") Getting work permits, etc. for living in France was *very* difficult since they couldn't imagine a living human without a birth certificate.
11:10:50 From Scott David : And if we find that "cogito" is situated in language and material culture, the "am" is the group, not the individual instantiation.
11:11:21 From mary hodder : I think we may be in the existential crumple zone right now.. we are well into it.. with the planet.
11:11:36 From Scott David : This is a beautiful presentation.
11:11:58 From Nicky Hickman : +1 Mary - the planet is a stakeholder and we are part of it - Gaia principle
11:12:30 From Scott David : "There is no cure for birth or death - save to enjoy the interval" George Santayana
11:12:33 From Nader Helmy : Ooh didn't think I'd hear Gaia at IIW

11:12:35 From Nader Helmy : Love it
11:12:42 From Brent Shambaugh : Are you your identity, or is your identity your connections?
11:12:52 From Nicky Hickman : we're all one man ;-)
11:13:08 From Nader Helmy : +100
11:13:25 From Heather Vescent : Absolute truth = we are all connected, Relative truth = we are individual.
11:13:31 From RuffTimo : Identity is such a messy term.
11:13:32 From mary hodder : No kidding scott.. every day we face death, we just prefer not to acknowledge and instead work really hard to distract.
11:13:53 From Scott David : This is the dawn of “eukaryotic governance.” Multicellular organization with both scale dependent and scale-independent attributes.
11:14:16 From Scott David : Like holocracy stuff on steroids
11:14:29 From Scott David : Socio-technical holocracy?
11:15:10 From mary hodder : being in a holocracy gets harder and harder every day
11:15:16 From Nicky Hickman : @ Heather - we are also 'dividual' - I might do a session on this. Our identities in many cultures are socio-centric and 'dividual' therefore do not end with physical death as Philip said
11:15:35 From Scott David : Life generates information. Data/perception plus meaning equals information. Life creates meaning recursively merely by maintaining negentropy autocatalytically.
11:15:39 From Nicky Hickman : vs ego-centric and individual
11:16:28 From Scott David : Nice
11:16:51 From Arnon Zangvil : beautiful
11:16:54 From Nader Helmy : Yeah the idea of relative truth centering around the individual is pretty biased to the western lens
11:17:15 From mary hodder : does purchasing count?
11:17:16 From Brent Shambaugh : People only see a fraction of the information available, and the information they see is based on what they have seen.
11:17:24 From Heather Vescent : Well, I am using the mahayama definition of relative truth. So IDK how western that is.
11:17:44 From mary hodder : because online purchasing is a daily dose of identity proofing
11:17:54 From Scott David : Nodes versus edges as source of value?
11:18:33 From Scott David : Value as generative information zones - mind, markets, are reaction chambers where data is exposed to meaning creating information
11:20:07 From Scott David : Static vectors cancel out
11:20:23 From Scott David : It is artifact of “reliability” as a pathway to trust
11:20:32 From Nader Helmy : Relative and absolute truths, sure. Not the idea of relative truth being individual
11:20:34 From drummondreed : Hmmm. The verifiable credential trust triangle is just a description of how transitive trust works.
11:21:44 From windley : trust triangles (not defending name) aren’t about removing trust. They’re about replacing the proximity we have in the physical world with the ability to determine the validity of the credential by ensuring its fidelity cryptographically. But it doesn’t remove the need to being vulnerable in trusting the content of the credential, a process that depends on credential provenance.
11:21:54 From Nader Helmy : Perhaps the distinction here is implicit vs explicit trust?
11:22:10 From Nader Helmy : "Removing the need for trust" == making the explicit implicit?
11:22:21 From Scott David : Trust triangle concept is akin to the notion that brakes on the car don’t make us go slower, they let us go faster. Triangles let us rely, but is that trust. Also, is that reliance justified in complex systems where non-linear behaviors will overwhelm pre-programmed (triangular) structures.
11:22:54 From Scott David : This is fun stuff.

11:23:34 From Terry Newton : Football helmets result in more injuries.
11:23:59 From Scott David : We are taking a “linguistic turn” similar to that of European philosophy in the prior century. From math-based philosophy to “language based” philosophy. Language and narrative provides additional degrees of freedom.
11:24:23 From Scott David : Law is enforceable triangles to help de risk the future
11:24:57 From Scott David : De risking is not equivalent to living. It just mitigates the risk of dying.
11:25:12 From Doc Searls : Is "reliance" a better word than "trust" in this context? Dunno, but I suspect there is a better word than trust, in some other language, for what's being talked about here.
11:25:23 From drummondreed : +1
11:25:47 From Nader Helmy : +1 Doc. Maybe even "dependence"
11:25:54 From Nader Helmy : interdependence
11:26:02 From Michael X Shea : the challenge is always when taking a word with an existing definition. There is always a dissonance that occurs when people take an existing definition and find that it does not quite fit.
11:26:31 From Scott David : Yep. That is why contracts and laws present specific definigions
11:26:40 From Michael X Shea : While it may sound silly, maybe creating a new word, a mashup of segments would help.
11:27:17 From Scott David : The paradox of incommensurables presents reality for our consideration. The absence of paradox is ALWAYS a model. \
11:27:20 From Nader Helmy : the idea of definitions and differing definitions is really interesting in the context of linked data, ultimately an effort to establish shared meaning on the internet…….
11:27:43 From Hunter Cain : I feel like we are trying to put a black and white definition into a world of gray
11:27:57 From Scott David : To resolve paradox is to adopt a model. Better to “manage” paradox, and understand incommensurables as the essence of identity.
11:28:02 From Doc Searls : We could bring in Lakoff and cognitive linguistics here. His case is that all thinking and the conceptualizations beneath thinking, are metaphorical. So we borrow the language of one frame to talk about another. For example, time is not money, but we talk about time in terms of money when we say we save, waste, invest, loose and set aside time. A key fact about this is that all metaphors are wrong, and that's one reaons they work.
11:28:45 From drummondreed : I disagree that SSI is “noun-like”. Some may see it that way, but ironically the peer DID pattern is highly verb-like.
11:29:07 From Doc Searls : I think SSI may be noun like if you look only at the corners of the triangle, but it is all verb in use.
11:29:08 From Nader Helmy : Metaphors are blunt force weapons. Huge assets but ultimately by definition imperfect
11:29:14 From Nicky Hickman : Sorry I disagree with persistence as a founding principle of SSI
11:29:23 From Nicky Hickman : Hello - I am not a techie
11:29:31 From Nicky Hickman : Je suis Muggle
11:29:37 From drummondreed : As an aside, “persistence” was not one of the principles discussed in the Principles of SSI session this morning
11:30:04 From Nicky Hickman : +1 drummond, the immutable ledgers are simply enabling tech
11:30:17 From Nader Helmy : "persistence" sounds like a remnant of the 2017/2018 blockchain hype days of SSI
11:30:18 From windley : Allen used persistence for identifiers, not for identity.
11:30:29 From drummondreed : +1
11:30:32 From Nicky Hickman : +1 phil
11:30:44 From windley : Its about identifiers being non-reassignable, not being forever.
11:31:06 From Nicky Hickman : +1 phil, identity itself is a function of context

11:31:19 From Scott David : Studies of sovereignty are really interesting here. Because “sovereigns” are all narratives/teleologies, you “cannot look directly into the face of God”. Sovereign power is maintained until it is exercised, at which time it reveals itself to be banal and human based, i.e., worthy of awe. (See current US politics for example of that corrosion)
11:31:39 From windley : Identity isn’t an object. There’s no artifact called an identity
11:31:44 From Nicky Hickman : SSI simply suggests you can control it not own it
11:31:51 From RuffTimo : +1 Phil. Need to distinguish identifiers, which are self-sovereign, from identity, which is far more complex and not entirely self-sovereign.
11:31:53 From Doc Searls : Am I wrong that the only thing one can be said to own in SSI is one's private key?
11:31:56 From drummondreed : Sorry, but identity is NOT an object in SSI. Read the Sovrin Glossary Appendix A.
https://docs.google.com/document/d/1gfIz5TT0cNp2kxGMLFXr19x1uoZsruUe_0glHst2fZ8/edit?pli=1#heading=h.8bjtfwpx6fwe
11:32:08 From drummondreed : Correct, Doc.
11:32:42 From Bob Wyman : Do you own only the private key or the key pair?
11:32:50 From RuffTimo : @Doc Yes, plus the agency to share the credentials if/how you want, connect and revoke connections, etc. What you do with what's been issued to you by 3rd parties.
11:33:28 From Scott David : Here are a couple of sovereignty references. “Violence and the State” (Ed. Killingsworth), “the end(s) of community” (Nichols), “The notion of Authority” (Kojeve), “Handbook of Tyranny” (Deutinger),
11:33:28 From windley : You control both keys and in KERI or Peer DID world can rotate them out from under the identifier to give persistence.
11:33:59 From RuffTimo : This comparison proves a fundamental misunderstanding of SSI. Like I concluded after reading his paper: it's an issue of terminology confusion, IMO, which those in the SSI space already readily acknowledge. My $.02.
11:34:02 From Arnon Zangvil : The point is that identity, as we think about it as technologists, as radically different than the concept of human identity as a continuously constituted construct The responses of this group, rest my case, so to speak :)
11:34:16 From Nader Helmy : Don't know if the concept of "ownership" applies to public keys
11:34:31 From Doc Searls : Actually, agency is not fully defined or understood in this, or any context. It's been around since Rome, (in Latin, agere means to do). I think of agency is the ability to operate with effect in the world. One has agency when one speaks, or drives a car. One lacks it when one is a pinball in some company's machine. Or when we have no choice but to "agree" to unfriendly terms.
11:34:33 From windley : Control is a better word than own
11:34:34 From Scott David : Verb like architecture corresponds to identifying and normalizing attributes of edges (versus nodes)
11:34:44 From Arnon Zangvil : He’s saying ‘social animals’ and we see ‘public key’ LOL
11:34:53 From drummondreed : +1 to avoiding “ownership” when it comes to data, period
11:34:59 From Scott David : There is no feral identity. There is no feral consciousness
11:35:02 From RuffTimo : Ironically, after we leave the abstract and get to a discussion of practical implementation, we'd likely discover that we all agree, and that it's just the words that have gotten in the way (again).
11:35:25 From Nicky Hickman : +1 drummond, data is like knowledge. Once shared it can't be reclaimed and you can't rent it
11:35:48 From drummondreed : I agree with Philip on this - “data subjects” is my least favorite term from all of GDPR
11:36:00 From Doc Searls : "data subjects" is what the GDPR reduces "natural persons" to. I'm not aware that anyone in SSI talks about people only as "data subjects.

11:36:06 From Scott David : Rhetorical artifacts of prior power systems. That is why we need to define or redefine usage. Or use new nonsense words (apple=computer?!?) as “positioning” of new concepts
11:36:11 From drummondreed : Agreed, Doc
11:36:16 From Nicky Hickman : I like this distinction a lot
11:36:21 From Doc Searls : Good point, scott
11:36:23 From windley : I don’t like it either, but when you actually start to build a real thing, you run up against pesky things like regualtions
11:36:46 From Doc Searls : Can one not construct a rhizome out of SSI interactions?
11:36:58 From windley : Yrd
11:36:59 From Scott David : We need a “self-regulatory” structure among all humans. COVID exposes our fundamental biological connection
11:37:00 From windley : Yes
11:37:27 From Scott David : Rhizome a la Deleuze?
11:37:46 From Doc Searls : I suggest that what's on the left sides of Philip's charts is what he hears being said in and around the SSI conversation, and not necessarily what's being designed or built. I confess to having the same problem.
11:37:48 From Nicky Hickman : Agree that SSI is relational identity
11:38:57 From Scott David : Yep. We inherit artifacts of prior power narratives as givens. Data plus meaning equals information. We inherit meaning structures (aka institutions).
11:39:27 From Jsearls : +1 Scott
11:39:48 From Daniel Hardman : Many of the characterizations of generative identity that Philip is proposing are the very things I’ve been claiming about SSI for years. The contrast that I’m seeing is between a degenerate SSI and the real thing, which is emergent and multidimensional and relationship-oriented and mediated by negotiations with agency.
11:40:20 From drummondreed : Well said, Daniel.
11:40:21 From RuffTimo : +1 Daniel
11:40:23 From Scott David : We see this as terrifying, but we have a vast opportunity in exponentially expanding interaction space
11:40:30 From Nicky Hickman : +1 daniel
11:40:32 From RuffTimo : +1 Scott
11:40:38 From windley : Yes, Philip has created a straw man SSI and then he’s knocking it down. But none of us working SSI recognize it.
11:40:43 From Nicky Hickman : key point is the edges not the nodes
11:40:49 From RuffTimo : Bingo, Phil.
11:40:54 From Scott David : We need to liberate ourselves from our prior paradigms/language and constraints. That is tough.
11:41:37 From Nicky Hickman : + 1 scott - a new language of trust
11:41:38 From RuffTimo : Again, ironically, when we peel back all the language barriers, we're all in agreement here.
11:41:54 From Nicky Hickman : +1 violent agreement
11:42:04 From drummondreed : Philip has a good point about the fact that digitizing something can wholly change it
11:42:09 From Scott David : The technology is an artifact of the solutions to common patterns. See Chris Alexander “pattern language”. Human identity touchpoints are “patterns” of dealing with human problems
11:42:15 From Doc Searls : I think what matters most is where Philip is coming from, and not the specifics of critiques.
11:42:26 From Wip : +1
11:42:35 From RuffTimo : +1

11:42:41 From drummondreed : I use the wallet metaphor to get across the basic ideal of digital credentials, but not the whole of “SSI”
11:42:53 From Jsearls : SSI is not a technical problem, it’s a spiritual problem.
11:43:12 From Scott David : Passion is always creative. Synthesize and then synthesize and then synthesize. We Bayesians all!
11:43:15 From drummondreed : Though after this session I definitely plan to provide a MUCH broader perspective on what “SSI” really is
11:43:28 From Scott David : Law and power are enforceable philosophy
11:43:29 From Michael X Shea : +1 Scott
11:43:38 From drummondreed : “We Bayesians all!” <=== ++++1
11:43:57 From RuffTimo : Great comment and question, Heather.
11:43:58 From windley : Sovereignty isn’t about “I”. It is, necessarily about relationships and boundaries.
11:44:02 From Bob Wyman : I’m not a verb, I’m a gerund. I’m not “live,” I am “living.” A gerund is a verb-form that acts like a noun.
11:44:37 From Scott David : Synthesize all human intelligence as “Synthetic intelligence” as a body of knowledge AND as a system of knowledge generation.
11:45:21 From Jsearls : +1 Arnon
11:45:27 From drummondreed : +1
11:46:05 From Scott David : SI will offer us some existential coherence in light of the coming STORM of insight from AI. Humanness will be sandblasted if mere “insight” is see as value. Each insight produces a shadow intrusion. We need to balance insight and intrusion in enforceable narratives.
11:46:46 From satikusala : Have a question… has there been any people-research completed on the adoption of these technologies?
11:46:47 From Scott David : This is a first step to that inclusion
11:47:17 From satikusala : I’m looking for SII Technology Adoption Studies and understand that factors that are influencing people’s adoption of these technologies.
11:47:29 From satikusala : Has anyone come across any studies of this nature?
11:47:45 From Scott David : This is an awesome entropy engine! The bigger the gap, the better the information efficiency (see Carnot).
11:48:42 From RuffTimo : +1 Heather.
11:48:51 From mary hodder : This is part diversity issue, and part inclusion, but also it’s about translation between people in interdisciplinary and multidisciplinary (they are different) groups
11:48:53 From Scott David : We all come to this stuff with our own situational awareness. We are co thinking and identifying paradoxes that reflect realities of which we were previously unaware.
11:48:59 From Brent Shambaugh : @heather made me think of something. If it is not pushed to github is it less valuable?
11:49:14 From Scott David : I love my ignorance. It is my best quality!
11:49:15 From RuffTimo : This slide attacks the word "sovereign" for all the same reasons we all dislike it. :)
11:49:50 From mary hodder : in other words we have a lot of trouble understanding each other.. between the sociologists, who look at the same word one way, and the anthropologists who see it another, and psychologists who see it in yet other terms.. and then .. how to talk to lawyer and engineers and product makers?
11:50:09 From Jsearls : We’ve seen exactly this from ALL disciplines. Graphic artists were not brought into the design of early design software. Retailers were not involved in the design of ecommerce software. Bookeepers were not brought into the design of accounting software, etc. etc. It’s only getting worse as we are starting to create software systems that really affect human systems.
11:50:47 From Scott David : +1 to Joyce

11:50:59 From Judith Fleenor : @Heather sometime “just” philosophical discussions are valuable, just to inspire thought. Thus, not everything needs to be “actionable” That’s the delight of IIW for me.
11:51:33 From Heather Vescent : Oh, I get that Joyce, and I have had many of these philosophical discussions, but I am pushing for something more!
11:51:47 From Heather Vescent : I meant @judith in previous message, sorry!!
11:53:14 From mary hodder : you can’t ‘move fast and break things’ and be inclusive and suss through the learnings on usability side
11:54:07 From Scott David : Information technology has been more about the technology than the information.
11:54:34 From Scott David : Information is ONLY produced with meaning. Meaning cannot exist without an observer
11:54:36 From Doc Searls : Great one-liner, Scott. Critical point by Joyce.
11:54:36 From mary hodder : scott.. yes
11:54:40 From Heather Vescent : Sure did Joyce.
11:55:10 From Nader Helmy : I have a question that's been plaguing me for a long time. How does Doc's call to make systems "open to participation" and "not intermediated by trusted companies" reconcile with decentralized peer to peer DIDs and the privacy focus of consumer-facing SSI?

I keep coming back to the fact that we haven't as a community yet solved the "decentralized social discovery" problem
11:55:11 From Scott David : Our shovels started talking to us. Technology got smart
11:55:34 From Doc Searls : On the bookkeeping topic, https://medium.com/@dsearls/the-second-coming-of-double-entry-bookkeeping-786bc47113b4#:~:text=Luca%20Pacioli%2C%20the%20priest%20and%20mathematician%20who%20taught,double-entry%20bookkeeping%2C%20which%20he%20learned%20from%20Venitian%20merchants.
11:56:03 From RuffTimo : Well, "dystopian" roughly equals "sucks"
11:56:06 From Scott David : SSI or any other solution will be transitory. Change is constant. Question of the perfect and the good.
11:56:22 From Doc Searls : Whoops, better link: https://medium.com/@dsearls/the-second-coming-of-double-entry-bookkeeping-786bc47113b4
11:57:31 From Nader Helmy : In other words, how do self-sovereign individuals organize and create collectives that are human and social?
11:57:49 From Nader Helmy : I don't think the answer is built into the technology we're relying on
11:58:21 From Scott David : Don’t drive over a bridge designed by a lawyer. Don’t sign a contract drafted by an engineer. We need to work together to render socio-technical systems reliable. Once they are reliable, they should be recognized for what they are - Interaction de-risking spaces, not existenaial narrative spaces
11:58:45 From Doc Searls : By the way, that "second coming" didn't happen, far as I know. The wisdom embodied in double-entry bookkeeping that was developed by Venetian traders and written down by Pacioli in 1492, has remained largely lost as every bookkeeper and accountant's mind is trapped inside of Quickbooks.
11:59:06 From RuffTimo : @Nader IMO it emerges organically as we connect with one another, forming the web of trust that's been sought after for a long time. I think it'll be very much like the webs of trust that exist in meatspace.
11:59:22 From Scott David : At least the Venetians came up with some great window shade solutions!
11:59:55 From drummondreed : :-)
12:00:11 From Nader Helmy : @RuffTimo I want to believe that things will organically "meet in the middle" between consumer and commercial SSI but I'm not convinced it won't happen without a concerted effort

12:00:29 From Nader Helmy : One side of the equation is driven by funding and commercial interests, the other side is driven by humans
12:00:38 From Nader Helmy : Which does history tell us will win out?
12:00:51 From Nader Helmy : **which side
12:01:00 From Scott David : It is hard to critique behaviors of people and organizations where there are no shared narratives of duties of care
12:01:08 From drummondreed : Good point, Nader. We need to give the humans all the help they can get.
12:01:26 From schmudde : JPL has an important place in art history dating back decades. They have been a model that few people have taken note of, unfortunately.
12:01:36 From schmudde : David Em is probably the most famous artist that worked at JPL.
12:01:58 From Doc Searls : A grace of Tim Berners-Lee's original design of HTML was that rendering was almost entirely up to the reader. That got lost as everyone wanted the publisher to be in charge of fonts and styles.
12:02:00 From windley : This post describes a use of SSI that was not about commercial interactions, but about connecting to people I knew and validating who they were (despite the digital distance). https://www.windley.com/archives/2019/06/did_messaging_a_batphone_for_everyone.shtml
12:02:43 From drummondreed : Also, Phil, there's your post on how SSI is all about relationships…
12:03:00 From windley : https://www.windley.com/archives/2020/07/relationships_and_identity.shtml
12:03:09 From drummondreed : That's the one
12:03:13 From sheldrake : tx
12:04:41 From Nader Helmy : @Doc I never knew that bit of history about HTML. Do you know where I can read more?
12:05:20 From Jsearls : +1 scott, "construct is a form of violence"
12:05:32 From mary hodder : male engineers
12:05:48 From mary hodder : no permission no forgiveness asked
12:06:01 From drummondreed : Ouch! But true…
12:06:09 From Nader Helmy : move fast etc
12:06:39 From Arnon Zangvil : Interesting book: "What Tech Calls Thinking" https://tinylink.net/36mkJ
12:07:03 From Doc Searls : A priest to me at the Camoldoli monastery: "You're taking this stuff literally? Look, Jesus spoke in paradox. You need to look below all that, at the mystery." When I asked him what the mystery was, he said, "If I knew I wouldn't be here."
12:07:28 From drummondreed : HA! That, Doc, says it all.
12:08:20 From Doc Searls : @Nader, not sure. But I'll look around for some source documents.
12:08:50 From Nader Helmy : thx :)
12:08:56 From Scott David : Nice. Heather - Step into your power to use it for good
12:09:39 From windley : Just note that CSS didn't exist originally. Came along 1998ish? We used to do a lot with chopped up images and tables to get a particular look
12:09:57 From Scott David : The only absolute trust is that there is no absolute truth.
12:10:16 From Scott David : Except for mathmaticians
12:10:35 From Scott David : Except for Godel
12:10:39 From Nader Helmy : Every truth is subjective. I think the best we can do is to gather enough context to incorporate many subjectivities at once
12:11:00 From Doc Searls : Yes. All the additions to basic HTML were necessary in retrospect, but something in the original simplicity—that rendering should be up to the reader—was lost. Perhaps unavoidably.
12:12:28 From Nader Helmy : I think what I struggle with in terms of avoiding past mistakes in the history of the internet is the idea that scaling inherently and inevitably erodes individual autonomy and agency
12:12:39 From Nader Helmy : That seems to be an unavoidable fact, regardless of technology

12:12:46 From drummondreed : I LOVE this chat. Truth and the evolution of HTML side by side, blow by blow ;-)
12:13:56 From drummondreed : Nader, I'd say that our primary goal here at IIW and with the evolution of SSI is to have that NOT happen with THIS particular evolutionary step of technology AND society. Let's get it right for one.
12:13:57 From Doc Searls : @Nader, that's why I like working on kinds of scaling of individual agency. Example: https://medium.com/@dsearls/customers-need-scale-f8e045b90304
12:13:58 From drummondreed : once.
12:14:05 From Nader Helmy : What if instead of scaling the growth pattern was horizontal adoption?
12:14:08 From drummondreed : +1 to Doc.
12:15:01 From Nader Helmy : @Drummond totally. Hope is a beautiful thing, All of the previous efforts were hopeful too..
12:15:31 From drummondreed : Yes, but I'm talking less about hope and more about determination.
12:15:38 From Heather Vescent : Thanks Philip. And all for the conversation and presentation. Thank you for receiving my hard ass comments and pressure.
12:15:41 From Nader Helmy : @Doc yes! thanks
12:16:15 From drummondreed : Good idea
12:16:46 From Nader Helmy : @Drummond love it. determination & persistence will keep us going

Universal Declaration of Digital Identity (UDDR/UDDI)

Wednesday 11H
Convener: Jean F. Queralt (TIOF), Jeff Aresty (IBO)
Notes-taker(s): ?

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

Reference documents
UDDR White Paper Draft
https://docs.google.com/document/d/1Id4gIcoDzsZs04EdWZM-5vs5M_nSlheAMb68ZmJwrhs/edit

UDDR Draft
https://docs.google.com/document/d/1y9C-5TPYmRruRQqJq39-HePk3ypWLDpSAEVzuonOH2Q/edit

UDDR Concept Brochure
https://drive.google.com/file/d/1JwdOelW8hzFJROpbPqvknzN_OrTD0UZT/view?usp=sharing

2019 DRAW Booklet
https://drive.google.com/file/d/1LK6n1XbSKvTyNUg0ZgL4jFUTF3085dww/view?usp=sharing

Contact Information
Jeff Aresty & Jean F. Queralt JFQueralt@TheIOFoundation.org

How the regulations related to technology can be incorporated into life. For example, GDPR is top down, and, ultimately for its enforcement to work, people who are subject to the law need to understand it and be willing to be subject to its governance in all forms.

How Digital Identity can lead to digital rights - maybe the starting point is the rights of the data. In order for data to have value of any sort, it needs to be contextualized. Once the data comes from a source, the link can not be severed. If we can define rights from a global perspective, and, that it can be described in a global standards way, we can both protect the data and the user.

From an individual perspective, if I am my data, then most democratic jurisdictions will have certain rights and duties of care with respect to that data. And, whether they are a positive or a negative right, the government will have a role to play to protect the data of their own citizens.

The first iteration of this is a Universal Declaration of Digital Rights - link above.

Is digital identity for use in the digital world or the real world?

Has there been a conversation anywhere about SSI is intersecting with disinformation - we have a huge challenge with what is real and what is not real - how do you enforce sanctions against untrustworthy information?

Unedited Chat -
From [TIOF] Jean F. Queralt to Everyone: 12:38 PM Heya
From Tony Fish to Everyone: 12:39 PM i am hiding :)
From Tony Fish to Everyone: 12:58 PM Humans move in and out of relationships and our mental and legal models worked within this conceptual framework. Digital contracts, tracking, consent notices, risks and use of data survives all users engagement. This is a change in the fabric. which fabric are you creating right for? tony pain in the ass fish why do you need a secure ID ? rules, governance and principles are connected via the risk framework - if the risk framework was built for the old system, how will it identity risk in the new digital first world? .. "identify" risk how would the individual ever understand the risk It's all data until I attach it to my identity at which point it becomes information If I trust you (with information), then I increase my risk and decrease privacy in a one to one relationship If I increase security (by gating my information), then I decrease risk and increase privacy in a one to many relationship Trust and Security are actions that I can take. Risk and Privacy are consequences of those actions Identity is the spider that spins the web
From Tony Fish to Everyone: 01:01 PM Spider web is very strong, yet also delicate and fragile Just like these relationships predicated on data Identity: A personal context that can be attributed to data Trust: The quantity and quality of identity attributed data that I actively share with you Risk: The expected negative consequences of you doing something with my data Security: The processes that I put in place to control the data that I share with anyone Privacy: The level of control I have to generally reduce negative outcomes of data sharing
sorry for my rambles
Music - so when the fabric changes those who want the old may not survive. the new is emerging. digital first
From Jeff Doctor to Everyone: 01:02 PM I'd prefer not to be recorded
From [TIOF] Jean F. Queralt to Everyone: 01:04 PM Thanks everyone for coming to the session.
From Trev Harmon to Everyone: 01:06 PM Hi everyone. Has a link to the doc being shown been shared?
From [TIOF] Jean F. Queralt to Everyone: 01:08 PM UDDR White Paper Draft
https://docs.google.com/document/d/1Id4gIcoDzsZs04EdWZM-5vs5M_nSlheAMb68ZmJwrhs/edit UDDR

Draft https://docs.google.com/document/d/1y9C-5TPYmRruRQqJq39-HePk3ypWLDpSAEVzuonOH2Q/edit UDDI Draft https://docs.google.com/document/d/1Z8X_jB_P40fHjii2a4_GrUETi7x7Ty8V-RavjhK42jk/edit?usp=sharing Note: The UDDR is a pokemon evo from the UDDI. So to speak.
From Trev Harmon to Everyone: 01:08 PM
Thank you!
From Jeff Orgel to Everyone: 01:14 PM
Far more persistent online so arguably far worse...!?
From Melody Musoni to Everyone: 01:15 PM
I am still new in this field. Perhaps you may start by defining what Digital Identity is. Where do we draw the line between what we consider to be part of Digital Identity and what shouldn't. Thank you.
From Trev Harmon to Everyone: 01:17 PM
If data has severed, independent rights, in the case of redress, who has standing to bring that into the courts?
From Tony Fish to Everyone: 01:19 PM@melody Digital Identity like risk, beauty and trust - it all depends on the eye of the beholder.
From Jeff Orgel to Everyone: 01:19 PM 3 Jeffs, wow!
From Jeff Doctor to Everyone: 01:20 PM Can never have enough jeff
From Me to Everyone: 01:20 PMDigital Identity definitions are all over the place.
From Tony Fish to Everyone: 01:20 PM is data and digital interchangeable in this document ?
From Me to Everyone: 01:22 PM I try to separate them out into sectors: legal identity is one specific form of digital ID, but not the only one there are medical and financial identities reputational identity - both social and skills but ultimately, each piece of identity can be looked at as a data attribute which needs to be contextualized
From Tony Fish to Everyone: 01:22 PM can digital exist without data? can data exist without digital ?
From Me to Everyone: 01:23 PM And, then governing how that data is created so that it can be trustworthy to those who 'own' it, or ultimately, 'rely' upon it - in a global sense - is what we are working on
From Melody Musoni to Everyone: 01:24 PM @Jeffrey, thanks for the clarity. I think a working definition is very important particularly for most African countries here as digital rights are usually overlooked. I can imagine the same goes for digital identity and less protection being afforded to certain digital identities, apart from the legal DIDs
From Lisa LeVasseur to Everyone: 01:25 PM I know a lot of you were in the session where I shared this yesterday, but for those who weren't, we've started to catalog digital harms here: https://me2ba.sharepoint.com/:x:/s/LivingDocuments/EcqGrfGY8qJEiioT-RpuNb4BxSIPpzWzWFl7nfTN1cbl8w?e=S1rfS4 can also find it a www.me2ba.org/resources
From Jeff Orgel to Everyone: 01:25 PM Really great effort!!!
From Jeff Doctor to Everyone: 01:25 PM Has this work taken into account UNDRIP ? https://www.un.org/development/desa/indigenouspeoples/declaration-on-the-rights-of-indigenous-peoples.html or even ILO 169? https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C169
From Lisa LeVasseur to Everyone: 01:26 PM @Jeff D thanks for those links
From Jeff Doctor to Everyone: 01:27 PM United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) - C169 - Indigenous and Tribal Peoples Convention, 1989 (No. 169) (ILO 169)
From [TIOF] Jean F. Queralt to Everyone: 01:27 PM @Jeff: The concepts reflected do not specifically tie to existing Rights. The reality of data (which doesn't care if it represent me, you or anybody else) is substantially different.
From Tony Fish to Everyone: 01:27 PM @lisa +1

From Jeff Orgel to Everyone: 01:27 PM I very much appreciate your clarity and focus on the language/translation layer bringing HR concepts to IT ethics design. You phrase a strange space very well in y opinion.
From Jeff Doctor to Everyone: 01:28 PM I strongly recommend looking into Indigenous Data Sovereignty principles - https://www.gida-global.org/resources
From Tony Fish to Everyone: 01:28 PM thanks @jeff D
From Lisa LeVasseur to Everyone: 01:29 PM so interesting @JeffD--are you also aware of this work: https://standards.ieee.org/project/2890.html
From Jeff Doctor to Everyone: 01:29 PM Yup I'm in that working group, but I haven't had much time to participate
From Lisa LeVasseur to Everyone: 01:30 PM <thumbs up>
From Tony Fish to Everyone: 01:30 PM since data is by its nature, non-rivalrous and non-excludable. how can data have rights?
From [TIOF] Jean F. Queralt to Everyone: 01:31 PM @Tony: It's a working framework. It may not adequate to traditional definitions, possibly.
From Tony Fish to Everyone: 01:31 PM non-rivalrous nature of data plays havoc with modern notions of ownership and rights
From Jeff Doctor to Everyone: 01:33 PM Whose traditional definitions :)
From Tony Fish to Everyone: 01:34 PM @jeff D the ones that satisfy confirmation bias
From Jeff Orgel to Everyone: 01:35 PM You are the ONLY other person I have heard say that! What about VR impact upcoming. Where is driving school for these peope?!
From Lisa LeVasseur to Everyone: 01:36 PM
I'm a big fan of the UDDR. The UDDI is new to me and I echo Melody's earlier questions regarding "Digital Identity".
From Tony Fish to Everyone: 01:37 PMif your future is a fully autonomous driving future - there is no driver.
From Jeff Doctor to Everyone: 01:41 PMArticle 5 - not everyone has a country @Melody - 100%
From [TIOF] Jean F. Queralt to Everyone: 01:41 PM UDDR Brochure
https://drive.google.com/drive/u/0/folders/1RnvAgFyfKbUUQgdd8S5GRGrNgDlQ2n41
From Lisa LeVasseur to Everyone: 01:42 PM
@Jean, can you change that to a public link? [love that diagram]
From Tony Fish to Everyone: 01:42 PM @lisa can you add assumption/ harm " that the data gathered can provide a model of the subject"
From Lisa LeVasseur to Everyone: 01:43 PM
@tony - YES! I actually want to get even more specific around OCEAN profiling, too.
From [TIOF] Jean F. Queralt to Everyone: 01:44 PM One event we ran as a first step: 2019 Digital Rights Awareness Week, in Malaysia. It has some summarized diagrams.
https://drive.google.com/drive/u/0/folders/1SAR651w2PVnhq8sXWNq7I9ghX-XapE2T
From Tony Fish to Everyone: 01:44 PM @lisa also forcing staff to work on data/ algorithms that they the employee considers unethical or immoral @ lisa will find you
From Lisa LeVasseur to Everyone: 01:44 PM@tony--thx, please do
From [TIOF] Jean F. Queralt to Everyone: 01:44 PM@Lisa: You having issues with the links? They are supposed to be Public already.
From Lisa LeVasseur to Everyone: 01:45 PM
that uddr brochure asks for perission
From [TIOF] Jean F. Queralt to Everyone: 01:46 PMSorry, I gave away the wrong links.
UDDR Concept Brochure
https://drive.google.com/file/d/1JwdOelW8hzFJROpbPqvknzN_OrTD0UZT/view?usp=sharing
2019 DRAW Booklet

https://drive.google.com/file/d/1LK6n1XbSKvTyNUg0ZgL4jFUTF3085dww/view?usp=sharing

From Tony Fish to Everyone: 01:47 PM love this, sorry have to run, shame not recorded. however please do put the chat into the open doc - thank you
From [TIOF] Jean F. Queralt to Everyone: 01:48 PM @Tony: Links are on the Doc. Can always share later on too.
From Tony Fish to Everyone: 01:50 PM thank you
From Nicky Hickman to Everyone: 01:50 PMI think there are some sessions on surveillance capitalism and something on deep fakes which could be interesting
From Lisa LeVasseur to Everyone: 01:51 PM
https://fixfake.com/ Kathryn Harrison usually presents here....not sure if she's here this time.
From Jeff Orgel to Everyone: 01:53 PM The surfacing of the values and the effort you are putting behind it will help find a dovetail for its place in helping this issue out. And starting with the kids is great!
From Lisa LeVasseur to Everyone: 01:53 PM also tru.net
From Nicky Hickman to Everyone: 01:53 PM Thanks Lisa
From Lisa LeVasseur to Everyone: 01:53 PM https://www.tru.net/
From billaal to Everyone: 01:54 PM Project lockdown
From Trev Harmon to Everyone: 01:54 PM Part of the issue with balkanization is that society isn't punishing bad information, but is instead encouraging it.
From Jeff Doctor to Everyone: 01:55 PM Y'all really need to consult with more Indigenous Peoples
From Jeff Orgel to Everyone: 01:56 PM@Trev, I believe that is human nature being played towards agitation for the sake of engagement/click dollars. This effort would help to roll that over I believe.
From Trev Harmon to Everyone: 01:57 PM@ Jeff Doctor +1 @ Jeff Orgel I agree. I was noting a result of the cause that you brought up.
From Jeff Orgel to Everyone: 02:01 PM @ Trev - Ya, sad/scary stories fuel challenges of managing the idea of "the others". Social Net atomizes it into every possible space...
From [TIOF] Jean F. Queralt to Everyone: 02:01 PM @Billaal https://ProjectLockdown.world
From Lisa LeVasseur to Everyone: 02:03 PM I like that git idea
From billaal to Everyone: 02:05 PM Jeffs' and trev, If I hear you correctly, There is a contradiction between indigenous rights of cultural "self definition", and a need for challenging the breakdown of humanity that might occur that with balkanization….
From Jeff Orgel to Everyone: 02:07 PM I would hope we can have a self that we can associate. I hope the options for association are broad enough to consider all facets, as well as fit into larger information needs (like identification).
From Lisa LeVasseur to Everyone: 02:10 PM Thanks for sharing this work! Good discussion, looking forward to ongoing work/discussion.
From Melody Musoni to Everyone: 02:10 PM Thank you everyone. I look forward to this document. @Jeffrey, I would love to know more about the work you are doing in Zambia. Thank you
From Jeff Doctor to Everyone: 02:10 PM https://www.iwgia.org/en/malaysia.html
From Me to Everyone: 02:11 PM@melody - jeffaresty@internetbar.org
@melody - let's be in touchFrom Trev Harmon to Everyone: 02:12 PM
@bilaal, I'm not attempting to compare indigenous rights and culture with the balkanization in social media. I'm going to think on your comment, though.
From Jeff Doctor to Everyone: 02:12 PM twitter: @jeffadoctor

Overlays Capture Architecture (OCA): Global Semantic Harmonization

Wednesday 11K
Convener: Paul Knowles @pknowles
Notes-taker(s):

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

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.

A database model shows the logical structure of a database, including the relationships and constraints that determine how data can be stored and accessed. Common kinds of data models include Hierarchical database model, Relational model, Network model, Object-oriented database model, Entity-relationship model, Document object model, Entity-attribute-value model, Star schema and Object-relational database model. The data semantics across these common database models can be harmonized using OCA.

Everything is documented in the slide deck which is available here.

Related blog post: https://humancolossus.foundation/blog/cjzegoi58xgpfzwxyrqlroy48dihwz

The Thoughtful Biometrics (un)Conference Coming in January - Sharing Ideas [Thoughtful Biometrics Conference]

Wednesday 11L
Convener: Kaliya Young, John "Jack" Callahan, Asem Othman
Notes-taker(s): Kaliya Young

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

We talked about the vision we have for the Thoughtful Biometrics (un)Conference. January 2021

Solving the problems.
Sharing 101 learning.
MITRE people could they show up? Chris Buchanan asked

To what affect?

Matriculate the ideas and concepts - via all of the biometric related people - who work with governments
Have to "win over" the MITRE engineers.

Daniel Bachenheimer - see what we are doing here in this space similar to what ICAO has done for their digital document (ePassport credential).

What are the biometric images / standards ?
What are the IAL requirements involved?
What are applications of pseudonymous biometric technology? (i.e., identify someone in a population) - see Doddington Zoo references in the literature
How do we handle morphing?

Some of it is use-case driven similar place to ICAO
Images and templates

When including biometric identifiers in credentials as a Verifiable Claim (e.g., an ICAO ePassport) we should consider:

- What mode[s] is [are] required, versus optional
- Photo capture process [e.g., live or not; professional or amateur], glasses [or not], quality [quality algo used]
- Identity Assurance Level [e.g., NIST 800-63-3]
- Format: Image, template [incl templ algo], hash [incl hash algo]
    - Images are not dependant on proprietary templates or hashes and typically out-perform standardized templates
- **Informed Consent**: biometrics are considered ***sensitive*** personal data per GDPR and should be handled accordingly. When shored through informed consent, how will the info be used, by whom, for how long, etc.

George Fletcher - What problem(s) are we trying to solve.
Let's enumerate use -cases already being used.

Todd Gerhke - id2020 work with iRespond in Bangladesh
Jeff Kennedy - Kiva work in Sierra Leone with single digit fingerprint
Chris B. - MITRE - new Social Justice team with interest in biometrics
John "Jack" C - new DIF Biometrics SIG

AUTHtung! Can digital identity resist authoritarianism?

Wednesday 11M
Convener: Phil Wolff
Notes-taker(s): Dave Huseby

Tags for the session - technology discussed/ideas considered:
#wedgethreshold #surveillancebydesign #tor #cci #covidcredentials #SSI #meaningfulconsent #TikTok #TikTokBan #Resist #revocableconsent #sovereignty #privacy

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

- What is it about technology that empowers individuals against government and corporate power?
    - Telegram allowed teens to coordinate their actions in an undetectable way to disrupt a Trump campaign event.
- There is a threshold, a "wedge" threshold, where a technology becomes such a large part of a society and empowers individuals while resisting corporate/government takeover through decentralization where those in power are forced into a choice between holding onto power and keeping the internet on.
    - Wedge technologies follow:
        - The Principles of User Sovereignty
        - The Unified Theory of Decentralization
- Master data controllers based on consent receipts can be used to empower users against government power to use that data.
    - Can also form the basis for government regulation of private entities through establishing a standard in which private systems can be judged.
    - Proportional safeguards can serve as a means for doing revocable, consent-based architectures.

From the chat:

From David Huseby to Everyone: 11:31 AM

- my article on the principles of user sovereignty:
    - https://uxdesign.cc/the-principles-of-user-sovereignty-515ac83401f6
- my article on a universal theory of decentralization:
    - https://medium.com/swlh/a-unified-theory-of-decentralization-151d6f39e38?source=friends_link&sk=b2a71917dcb5ce948196887c7ff48fde
- another article on how the web was never decentralized:
    - https://medium.com/design-warp/the-web-was-never-decentralized-bb066138c88?source=friends_link&sk=4359fd30d172cb49c14f7bb73174e5e3
- I'll be publishing my article on the wedge threshold next week
  a wedge, when in flight. a bank of swans when on the ground

From David Huseby to Everyone: 11:55 AM

- Six principles of user sovereignty:
    - Absolute privacy by default.
    - Absolute pseudonymity by default.
    - Strong, open source encryption always.
    - Open and standard protocols and formats for all data.
    - What, not who, for authorization.
    - Revocable, consent-based power structure.

About notice and consent receipts

- Rough iiw history - working on this topic - Identity Trust Charter @Identity Commons
- Digital Ledger Consent LifeCycle (specification we are working on @ Aries -)
- Part 1 - Operational Privacy Notice - Human(social), Legal, Technical Layer
    -
- (the unofficial draft in progress - check it out first week of Nov) AdvCIS - V1.2 Notice + Consent Receipt - Spec levelling for ISO 29184 and ISO 27560

- Combining it into one doc - working on it this week
  - Consent types - Hackathon for master data controls -- is being updating consent receipt types
  - for master data controls - (for revoking consent - etc)

Kantara Cr v1.1 (the old version 2017)

- (now being adopted by ISO 29100 and 29184 -- called ISO 27560 - Consent record structure - which we can use to make things,)

41st ICDPPC Tirana 2019, Open Session Panel I, October 23

- G. Greenleaf panel - including China/Japan - (the front lines of "All hail the emperor")

Full Session - Description -

- This session aims to inform a global understanding of MyData governance

3 layers

- Common language about governance landscape
  - Governance /Regulation
    - International Law - CoE 108 +1
  - Standards (international)
    - ISO 29100 - 29184
  - Best Practice -
  - Business

Interoperability

- Use standards

KERIfying DID Methods & KERI for Interop

Wednesday 12A
Convener: Sam Smith, PhD
Notes-taker(s): Ajay Jadhav,

Tags for the session - technology discussed/ideas considered:
KERI, cryptography, public/private keys, key event logs, decentralization

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

Dmitri Z: What is did:un method?

- CHarles: Indirect mode - it gets more complicated
- Charles: Delegated identifiers and multiple public keys in resolution?
-

Dmitri: Are there features you want to see other methods assume?

- Sam: Being able to easily and interoperably establish trusted communications across methods is the target end state--various ways of getting there

    - More brownfield approach - bootstrap various existing tech at once
        - Existing, hardened, legalized crypto > new stuff
            - Best crypto foundation using today's hardened tech is KE logging
            - key event logs and hash-chained microledger
    - Trust spanning layer for the internet
        - It is based on the old crypto
    - Using key event logs, you're building tooling which is [already] interoperable

Drummond: Indy method evolution - proliferation of variants (indy interopathon)

- Pu
- One of the key decisions was to use did:indy:subnetwork method
- We could reserve a namespace for KERI's SC identifiers
- KERI masquerade
    - Using KERI for trust basis
    - As it is agnostic to the namespace

Zoom Chat logs:

From Me to Everyone: Wizards ++
From Dmitri Z to Everyone: wot is this "blockchain" business. will never catch on.
From By_Caballero to Everyone: CAGE FIGHT CAGE FIGHT CAGE FIGHT! (I joke)
From Joe Andrieu to Everyone: =)
From Xavier Vila to Everyone: No you're not ;)
From Joe Andrieu to Everyone: btw, +1 to covering did:un a bit
From Dmitri Z to Everyone: +1
From By_Caballero to Everyone: requirements gathering
From Xavier Vila to Everyone: +1
From By_Caballero to Everyone: if only we had some kind of requirements engineera legendary one, ideally

From drummondreed to Everyone: I know a Legendary Requirements Engineer ;-)
From Joe Andrieu to Everyone: lol
From By_Caballero to Everyone: it undoes did methods if you're not careful
From Me to Everyone: :D
From drummondreed to Everyone: There is an evolutionary path for KERI adoption among existing DID methods
From David Huseby to Everyone: careful, might start looking like IPv6 addresses
From By_Caballero to Everyone: ^ !!!
From David Huseby to Everyone: did::::::::::::::::::::
From By_Caballero to Everyone: I wanna hear more about that analogydid:indy:deu:nrw:biele:keri:v4:
From Kumaravel N to Everyone: is the session recorded please?
From RuffTimo to Everyone: @Juan halting and then reversing the proliferation of DID methods is one of the desirable outcomes of KERI growth. :)
From By_Caballero to Everyone: ^ in my Bielefeld example, there was only one DID method-- just a very balkanized namespacedeu is SSI4Deutschland (one of the new indy ledgers using the same method)
From drummondreed to Everyone: I've suggested to SAM that DID methods that want to incorporate KERI just use the :keri: namespace inside their namespace. Example: did:indy:sov:keri:did:indy:indy:keri:oops, that was supposed to be did:indy:indy:keri:
Ah-ha, it's autocorrect! One more time: did:indy:findy:keri
From Joachim Lohkamp to Everyone: so the sequence matters… not sure if I understood Drummond correctly saying did:indy:un(keri): so it would be rather did:un(keri):indy:Is that right?
From drummondreed to Everyone: No, it's putting the KERI identifier namespace INSIDE the DID method namespace.

From Joe Andrieu to Everyone: Drummond, I'm pretty sure it's in the method-specific-identifier, not the method part
From drummondreed to Everyone: So if the DID method name is “did:indy:network”, then the KERI namespace under that network would be “did:indy:network:keri”
From Steve Todd to Everyone: did:un ~ urn, did:indy:indy:keri ~ url?
From drummondreed to Everyone: No, they are both URNs
From Joe Andrieu to Everyone: those DID's all have a method name of "indy" @drummondOh... they aren't dids? They are a URN that uses "did" as a URL scheme?
From Steve Todd to Everyone: But the the latter actually helps you locate the log whereas the the former is a name without any ability to locate the log.
From Joe Andrieu to Everyone: that seems wrong
From drummondreed to Everyone: Joe, those are just the examples I was using. Here’s another one: did:btcr:keri:or did:eth:keri:
From Joe Andrieu to Everyone: yes, the method is btcr
From drummondreed to Everyone: Right, the idea is that KERI can be “tunneled” inside any DID method
From Joe Andrieu to Everyone: the keri part is part of the method-specific identifier, not part of the method (which by ABNF ends at the colon)
From drummondreed to Everyone: Correct. It’s subnamespacing within the method-specific identifier
From Joe Andrieu to Everyone: I'm just correcting the language you used to describe it. I totally agree that any method could use KERI within its method-specific string. That's just not part of the method name.
From drummondreed to Everyone: Sorry, I didn’t mean to imply that the subnamespace was part of the DID method name

From Joachim Lohkamp to Everyone: Looking at the slide what Sam proposes it would be one: did:keri:ethr: or did:keri:btcr:
From Joe Andrieu to Everyone: the "un" is the method here, which is did:ethr:keri as a pattern
From Joachim Lohkamp to Everyone: I see
From drummondreed to Everyone: Just to clarify, “did:un:” (which I personally believe Sam and the KERI community should call “did:keri:” would be the “native” KERI DID method.I have a question for Sam for how that will work.
From By_Caballero to Everyone: uh.....
From Dmitri Z to Everyone: +1 to drummond - I do think did:keri: will be clearer
From Joachim Lohkamp to Everyone: +1
From By_Caballero to Everyone: could Joe answer that one? :D
From drummondreed to Everyone: So use a DHT as the global discovery mechanism
From Dmitri Z to Everyone: ok but like, DHTs are not panacea, right ; they’re just one tool in the toolbox (with clear engineering tradeoffs)
From David Huseby to Everyone: I have suggested to Sam that a DHT isn't low enough in the stack and that maybe this should be something that runs at the IP level like BGP nodes.
From drummondreed to Everyone: I have to jump to another session shortly, but from my POV, the key questions about the relationship of KERI to DID methods have been answered here. Are there any others that I can help with before I go?
From Steve Todd to Everyone: BGP is pretty analog to a DHT, imho.
From David Huseby to Everyone: @Steve Todd, it isI'm thinking more like how the DHT is built
From Steve Todd to Everyone: And BGP runs on top of the IP layer
From David Huseby to Everyone: if the KERI discovery DHT relies on DNS then it is suceptible to attack
From Joe Andrieu to Everyone: @By_Caballero you mean can did:keri work? Sure. that could be its own meta-method.
From By_Caballero to Everyone: I meant who needs DID methods for anything once there's did:KERI

From RuffTimo to Everyone: ^^ my question as well, other than the path between now and then...
From By_Caballero to Everyone: and Bernhard!
From Joe Andrieu to Everyone: I expect KERI fails when a definitive "current" document is a requirement, but as Sam has pointed out, that may not be a strong requirement for many uses
From By_Caballero to Everyone: ^ This question has come up in multiple places, I'd love to hear some discussion of this point
From Joe Andrieu to Everyone: The biggest rebuttal is that even DLTs like bitcoin never have finality, so the purist in me is trying to be open to the option of having a "good enough" establishment of the authoritative version of the DID Document.You still have to check the witnesses
From By_Caballero to Everyone: Hmm

Current & Future Adoption of Verifiable Credentials - How We Get From New Tech to Ubiquitous Adoption

Wednesday 12B
Convener: Riley Hughes
Notes-taker(s): Carlos Rodrigues

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

SLIDES: link to slides

(Copy-pasted from a markdown editor. Sorry)

Current & Future Adoption of Verifiable Credentials - How we get from new tech to ubiquitous adoption

- number of credentials issued has gone from 200 to 52K between Jan and Sep 2020
- many current use cases are low-volume (doctors, etc.)
- lots use cloud wallets (instead of device wallets)
- bcgov has 2.5M+
- barriers to production
  - perceived complexity (solution: simplify. sell business solution and not tech)
  - lack of business case (solution: innovate, productise)
  - lack of safety (getting more than early adopters. Solutions
    - find lighthouse customers, incentivise early customers
    - provide whole products
  - user experience
    - lack of great wallets
    - dance of protocols
    - solutions: find alligator bites problems (big problems that people will swap inconvenience for the solution), "warts and all" customers

  - slow moving firms/issuers
    - patience
    - start with small severe pain points
  - execution
    - solutions:
      - be systematic in product development
      - find operators (not just protocols)
  - governance
    - too much
    - too little
    - solutions:
      - ToIP
      - pilots
  - standards paralysis
    - setting standards intstead of implementing
    - what techs/standards to use?
    - solution: mitigation strategy
  - too advanced a technology
    - solution:
      - target customers. find your target-market
      - future proof your solution
  - funding
  - just takes time (education, standards, etc.)
  - SSI purity and idealism
- feedback: all are irrelevant
  - except finding business, funding
- SSI is the focus, but what we are building is so much more, it's a more general and secure digitisation
- Need more data that can be presented to potential customers
  - adoption
  - ease of use
  - benefit to business/industry
  - cost savings
- Problems
  - Selling technology
    - Sell solutions, not technology. Solve a business pain. Start small.
  - Chicken-egg problem
    - need high adoption to provide value (network benefit)
    - create own eco-system
  - Talking past each other
    - selling ID to authorisation customers
    - clarify the problem set
    - SSI solves big problems, also needs to solve small ones (the business's, what is their problem?)
  - selling the dog that doesn't bark
    - SSI gets rid of problems (fraud, etc.). It's benefit is taking problems away as opposed to provide a concrete, present benefit
- When is VC going to take off?
  - 3-5 years (standard CTO planning horizon?)
- How to overcome the chicken-egg network problem?
  - ecosystem approach (50% of respondents)

    - build an ecosystem with issuers and verifiers, then grow the ecosystem
    - targeting existing ecosystem that is using credentials
    - building an ecosystem around a solution/problem set
  - single-sided market approach (50% of respondents)
    - find one customer, sell solution to the customer, solve the company's internal problem, then open up the solution to others
- Trinsic is holding a webinar next week speaking to 3 businesses who have made and shipping a product using VCs

Feedback
- issue: who owns the wallet? They set the experience, control of the experience is set by who owns the wallet
- issue: not offering a brand new, disruptive technology(i.e. they have an identity solution (inferior, but still a solution))
  - solution: need to offer an ecosystem solution
  - but how to set up the ecosystem?
  - have to start by building a single-sided solution, with the faith that an ecosystem will build-up later
- issue: selling all the features and bells and whistles, but the customer still has to accept/become familiar with the basic package
  - stress that we are managing data, and we have a solution that works and can add additional value to the customer (now, or later,)
- issue: have to make sense of data coming from an orginisation that we do not control
  - need reliable issuers who give us hallmarks of credentials that everyone needs (e.g. IDs)
  - will help wider adoption (especially outside of just the one organisation)
  - this assumes an agreed symantec operablity (e.g. everyone understands and agrees with what is meant by an attribute named "name")
    - what about using schema.org? using that as a pseudo-standard for attributes
  - governance would help
    - but who will govern/standardise it until VC usage is more common/widespread/demanded?
  - when should standards be set/followerd?
    - once standards are set, that itself can be a barrier
    - maybe we should start implementing the solutions now and set/adopt standards later
- Adam McCarty: issues occur where theory ends (classic Physisc quote? I misquoted. Sorry)
  - need experimentation, pilots, etc., to start setting a path and trying solutions
  - build the tech, then the standards (else standards get set by the first-mover/solution (e.g. QWERTY keyboards vs DVORAK/whatever keyboards))
- Keith Kowal:
  - Higher education (in USA, at least) has been working on CLR standards, Learner Records for years. Worth refering to their work. Higher education is also possible target for VC in the US Market.
  - OpenBadges could be another vector. OpenBadges are being rolled into VCs as demand for sharable things (accomplisments, skills, etc.) has grown
- John Court
  - Problem: we want to make wallets, not be issuers/verifiers. So need to go out to build the ecosystem so that we can build wallets! There just isn't the usage out there at the moment to see what wallet-techs work.

CHAT:
From Brent Shambaugh to Everyone: unique kind of credentials? unique issuer?

From Margo Johnson to Everyone: Number of distinct credential templates used for issuance would also be a valuable metric in the future.
From Andre Kudra to Everyone: Margot, this also can be queried directly from the ledger
From Neil Thomson to Everyone: How does that not apply to BC?
From Andre Kudra: Public DIDs Schemas Credential Definitions All countable on the public ledger.
From Jeff Orgel to Everyone: Thanks Riley!
From Jonathan Laut to Everyone: thanks riley, cool insights! is there anything planned to present your interview results in research or something?
From Lynn Bendixsen to Everyone: link to slides?
From Riley Hughes to Everyone: Yes, probably a blog post or something I can make these into slides and share them in the notes Lynn
From Ken Adler to Everyone: +1
From Jonathan Laut to Everyone: any formats appreciated :) Looking forward to it
From Lynn Bendixsen to Everyone: Was one of the reasons related to "Trust"? Which number was that?
From Riley Hughes to Everyone: “Safety?”
From Karyl to Everyone: I **LOVE** that you’ve given this concept a term re: standards paralysis.
From Bob Wyman to Everyone: One risk of a premature focus on solutions is that the tech may become solution-specific, not general and useful for a variety of unanticipated solutions.
From Lynn Bendixsen to Everyone: yeah, thats close, what number was that?
From skyberg to Everyone: @Bob, very true! What’s our confidence that the VC space is “well enough” defined to safeguard against that?
From skyberg to Everyone: SSI runs the risk of looking like customer disintermediation. That’s bad for business that monetize their customer base.
From Bob Wyman to Everyone: @skyberg I don’t have an answer to that question. One way I’ve dealt with this problem with other tech is to define a set of solutions and then apply the tech to all. If the set is diverse enough, you can be confident that the generality of the Tech has not been overly constrained.
From skyberg to Everyone: @Bob +1
From Thomas Schwarz to Everyone: Less dependency and less external trust, I'd say. :)
From Karyl to Everyone: HR Credentials right?
From Bob Wyman to Everyone: Can we design a system that does not provide compelling value to single-sided use? Or, *should* we design it in this way?
From Karyl to Everyone: maybe it’s closed ecosystem vs open ecosystem vs consortia (a more open ecosystem linked together by same infrastructure choice)
From Riley Hughes to Everyone: 👍
From Ken Adler to Everyone: I like that … open vs closed
From Riley Hughes to Everyone: Closed loop vs open loop vs self-contained?
From Karyl to Everyone: ^^yes. for open loop, interoperability is the key IMHO.
From skyberg to Everyone: The cost of dealing with the trust framework in an “open” ecosystem is large.
From Karyl to Everyone: I think it’s actually very similar. When I say “open” I simply mean, the ecosystem actors can share credentials even if they aren’t all on the same infrastructure or issuance app. Whereas closed would be the consortia play - which is a harder sell because instead of individual infrastructure choices, peer-to-peer contracts and agreements, you have to negotiate the infrastructure choice and trust agreements at the ecosystem/consortia level.
From skyberg: How does the anticipation of “critical” credentials (e.g. DMV issued) impact opportunity?
From Me to: Is someone taking notes? I see that the 12B doc is empty. I have notes that I could add.
From skyberg to Everyone: Thanks, Carlos!
From Karyl to Everyone: please add Carlos! thank you!
From Me to Everyone: K.
From Karyl to Everyone: we can copy/paste the chat too at the end.

From skyberg to Everyone: +1, great job, Riley!
From Neil Thomson to Everyone: Why is solving people getting on airplanes, going to sports events or movie theatres as recently COVID tested not a perfect opportunity? The airlines are saying they are out of business without the testing and the proof on boarding solution.
From Karyl to Everyone: shameless plug: https://jsld.org/ linked data + interoperability can help solve the challenge Andre poses
From Mahesh Balan to Everyone: And add to covid testing covid vaccines
From Karyl to Everyone: and re: neil - it is an accessible use case to consider, but there are so many ethical implications being explored as we speak: https://ethics.harvard.edu/immunity-certificates
From Neil Thomson to Everyone: @Karyl - ethics or trust? And is that a US problem?
From Karyl to Everyone: disclosure: I am not a trained ethicist/don't currently work in healthcare/data
I think both depending on your definitions
From Ken Adler to Everyone: GLEIF is a good example
From Neil Thomson to Everyone: @Karyl, fair enough...
From Karyl to Everyone: definitely a US problem, although I suspect other regions are facing it too
From Ken Adler to Everyone: (Global Legal Entity Identifer Foundation)
From Bob Wyman to Everyone: What could be a use of VC that would usefully address a problem of every corporation today? A use that would be the wedge to push into every system?
From Riley Hughes to Everyone: Bob if you can answer that question, and answer the incentives to get it adopted, you'll be handsomely rewarded by the free market :)
From Karyl to Everyone: ^^exactly lol
From Ken Adler to Everyone: @Bob…. Regulation
From Eric Weber to Everyone: @Bob removing passwords
From Bob Wyman: Imagine that LinkedIn used VC and allowed issuers of credentials to certify "resume" entries in LinkedIn profiles. Would this make LinkedIn a preferred provider of employment history and make it easier for companies to avoid resume fraud? Then, if all new employees came into company with VC behind them, would it be reasonable to suggest that VC be used for login, etc. in the company?
From Ken Adler to Everyone: https://en.wikipedia.org/wiki/Legal_Entity_Identifier
From Karyl to Everyone: I've gotta hop; thanks all for my fav discussion at this IIW so far!
From Eric Weber to Everyone: not sure linkedin would add trust to your claim you worked somewhere
From Andre Kudra to Everyone: LinkedIn could issue credentials for confirmed data. I.e. a former employer endorsed the position. I.e. a colleague / peer endorsed a skill.
From Riley Hughes to Everyone: Link to our webinar: https://trinsic.id/making-money-with-ssi/
From Andre Kudra to Everyone: So it would just act as an issuer for confirmed data.
From Eric Weber to Everyone: why would these people not directly issue the VC
From Bob Wyman to Everyone: LinkedIn might start with schools who would certify graduation, etc. for alumni who could verify via their email addresses…
From Andre Kudra to Everyone: Because natural persons without public DID on a ledger cannot issue publicly Verifiable Credential.s
From skyberg to Everyone: They could. But LinkedIn could act as a kind of force multiplier to bootstrap the credential type.
From Eric Weber to Everyone: in real life trust is created between directly, not need for sb to stand next to you and know their head
From Andre Kudra: Correct, Eric Companies with public DIDs can issue testimonials to there employees.
From Eric Weber to Everyone: if we decentralise, everybody should be able to issue
From Riley Hughes: https://www.usv.com/writing/2018/10/the-myth-of-the-infrastructure-phase/
From Bob Wyman to Everyone: Sounds like an ex-DEC guy if he was in both OSI and AltaVista. (I was also with DEC. Was ALL-IN-1 product manager…)
From Andre Kudra: Need to run as well. Thank you, Riley and all, for an excellent & rich discussion.

From John Court to Everyone: DECnet OSI then DEC Research :-)
From schmudde to Everyone: Glad we have a few DEC folks here. Battle-tested network folks.
From Ken Adler to Everyone: Certified VAX System Manager here
From Bob Wyman to Everyone: DEC folk: Remember back when we used to wonder why we were the only ones who seemed to think that networks were valuable?
From Margo Johnson to Everyone: Really good point Keith re: Open badges and learner records. Defined schemas are a wonderful starting point for VCs!
From Ken Adler to Everyone: I saw a PDP-11 still in production at the Tribune Printing plant in Chicago… within the last 5 year

SSI & IoT (moved from this morning)

Wednesday 12C
Convener: Michael Shea
Notes-taker(s):

Tags for the session - technology discussed/ideas considered: IoT, SSI,

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

Sovrin SSI & IoT: *https://sovrin.org/library-iot/*

Contact: *info@sovrin.org or michael.shea@thedinglegroup.com*

Whitepaper announcement
https://sovrin.org/the-sovrin-community-releases-new-ssi-iot-whitepaper/

Whitepaper (44pp) https://sovrin.org/wp-content/uploads/SSI-in-IoT-whitepaper_Sovrin-design.pdf

From Nicky Hickman to Everyone:
- +1 I heard of a hack that came via aircon
- it killed the enterprise security

From Brent Shambaugh to Everyone:
- Silly side question. Ed25519 and secp256k1, used frequently with ledgers, are only available on some cryptographic co-processors. I have a co-prcessor with a p256 curve. Can I embed its public key in a DID document on the sovrin ledger?
- sure

From Nicky Hickman to Everyone:
- + 1 security and especially identity are iot hot topics, especially as is part of physical security , national infrastructure security and bio security

From Brent Shambaugh to Everyone:

- It was informative. I had trouble getting crypto software on my microcontroller. arm chip, esp32.. I used a p256 atecc508a to experiment with because sparkfun made a breakout oard. I am just getting started.
- I hadn't thought about the processor deeply. It was an issue with having enough memory to holding the libraries.
- *for

From Me to Everyone: to lookup: IETF ACE WG.
From Thomas (Evidence) to Everyone: Thanks !
From George Fletcher to Everyone: https://datatracker.ietf.org/wg/ace/documents/
From Nicky Hickman to Everyone: definitely need to focus on specific challenges that IoT can solve sorry \ssi can solve +1 - be careful of those dishwashers :-) Dave +1 paul there are things in every ecosystem
From Me to Everyone: How do IoT people think about digital identity differently than most of us?
From Brent Shambaugh to Everyone: iot is heterogeneous. ockam seems to be helping making things more streamlined across crypto chips and protocols with secure channels. lots of heterogeneous platforms too. the raise hand feature seems to be buggy.. ...look forward to more...thanks...gtg
From Nicky Hickman to Everyone: @ Phil, a lot of them don't think about it at all
they think about identifiers
From Me to Everyone: SSI for IoT hobbyists? running on Arduino and pi?
From George Fletcher to Everyone: I think there are a number of levels of security in IoT devices. Attestation could be key but may not require SSI.
From Nicky Hickman to Everyone: there has been serious thought, analysis and discussion with many from leading IoT Security folks +1 Paul plus the cryptography doesn't need to be device side, especially ALL devices Welcome to westworld
From Bruce Conrad to Everyone: @Phil, as an IoT person, I'm constantly seeing things around me and wondering, "What interesting things could happen if that thing was identified and had some kind of presence/surrogate/digital twin on the Internet?"
From Geovane Fedrecheski to Everyone: @Bruce +1
From Nicky Hickman to Everyone: I have a dishwasher that has a sticker on the back that says 'Marie 1203' it was probably made by a 90% automated industrial process. If that machine blows up, am I going to blame Marie 1203 or am I going to blame the brand - my point - every machine has human relationships and consequences. If some problem is found in the future with one of my washing machine's components, who will tell Marie 1203 that her health is at risk?.....
From Bruce Conrad to Everyone: @Nicky yes, once a thing is identified one can begin to imagine a whole complicated life cycle for that thing. In the end, what does Marie 1203 (or whoever replaced her on retirement) do when your machine ends up in a landfill or junkyard
From Brent Shambaugh to Everyone: there be dragons. :)
From pknowles to Everyone: I agree, Nicky. Even with an organisation, I would suggest that the company would be identified by a controlled passive identifier. The company has a vLEI identifier (GLEIF), a passive identifier. That identifier would be controlled by an active identifier (human being, e.g. CEO). The provenance chain for "Marie 1203" should lead right back to the CEO of the company that produced the machine. You can sue the organisation but the buck stops with an active governing entity - the CEO.
From Nicky Hickman to Everyone: yup - new SOX or IoT for IoT
From Me to Everyone: IoT folks seem to have much more interest in 4th parties. lots of data middlemen as a service that aggregate your fleet data, manufacturers that preprocess your devices' data, and fleet/asset management tools.

From Nicky Hickman to Everyone: are you talking about relationships between things, people and organisations? I think we might have something that could help with that sir. I think you made the key point Michael - it looks good on paper - we need a WG to demonstrate / prove it
From pknowles to Everyone: Inputs Domain WG @ Trust over IP … but that group doesn't exist yet!
From Brent Shambaugh to Everyone: fwiw my IoT hobby project was over at demo table #

Does SSI need DIDs?

Wednesday 12D
Convener: Dick Hardt, Phil Windley
Notes-taker(s):

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

SSI definition references:

http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

https://www.windley.com/archives/2020/06/what_is_ssi.shtml

Custodial/Guardianship Agencies - Hosting Agents on Behalf of Agentless Users

Wednesday 12F
Convener: Ken Ebert, Indicio Tech; Sam Curren @telegramsam
Notes-taker(s):

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

•Range of Technology
•High … Low … None
•Won't, Can't
Agents and Agencies
•Fiduciary Responsibility
•Keys
•Custodial Agents
•Where personal data is stored
•Recovery vs Backup/Restore
•Portability

•Bring your own agent
Best Practices

Scaling Issues
Number of end-users
Concurrent active users
Transactions per day

Degrees of Decentralization
Coexistance with Legacy Systems: Integration
Evolutionary vs. Revolutionary
When shouldn't a system be called "decentralized"?

Legal Layer for the Internet & IEEE 7012 Machine Readable personal privacy terms

Wednesday 12l
Convener: Lisa LeVasseur - Vice Chair IEEE 7012, Mary Hodder - Technical Editor IEEE 7012
Notes-taker(s): David Schmudde, Lisa LeVasseur

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

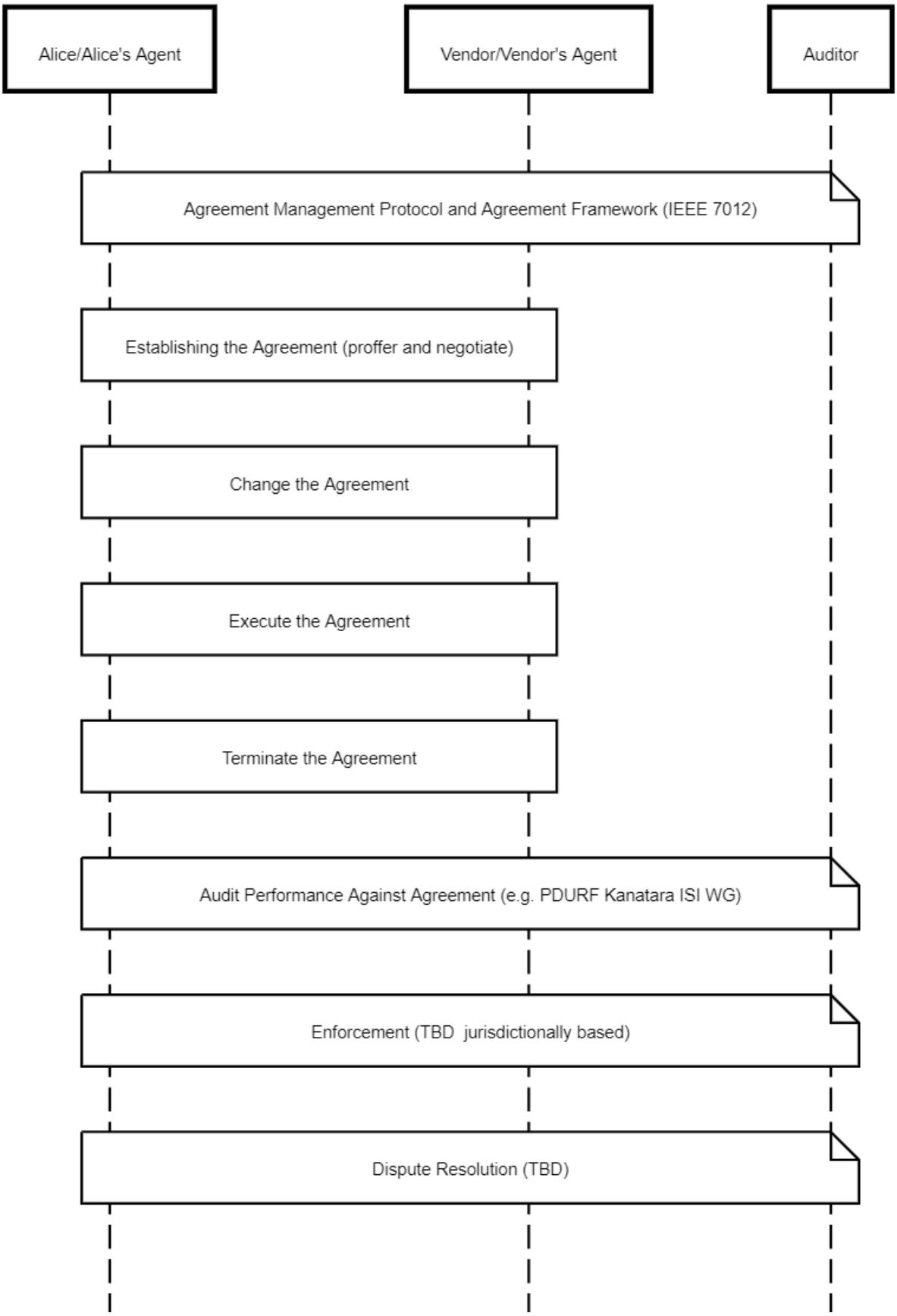
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

1. Agreement management,syntax, and recording (this is where the focus of IEEE 7012)
    a. Proferring
    b. Negotiating
    c. Executing
    d. Changing
    e. Terminating

    2. Auditing Performance Against the Agreement (and supporting technologies like information accounting: Personal Data Use Record Framework (PDURF) in Kantara ISI WG)
    3. Enforcement of the Agreement
    4. Dispute Resolution Activities

Agreement can be made by
1. Notice and consent
2. Contract
3. License (trying to accommodate in the machine readable document)

A Legal Layer for the Internet



Jeffrey Aresty: How do you create adoption by creating an access to opportunity? We're working on a music project to pursue this.

Mark Lizar: We need freedom from services. We need an international standard. The front lines are in China and Japan. ANewGovernance.org has recently convened some work around this, apparently.

Q: Can there be an international standard?

Shared a draft Information Sharing Agreement framework from which ISA profiles can be generated. The current ISA Base Data Model illustrates the minimum data fields needed to convey an ISA.

Marc: does the current schema include the content of the agreement--it looks like mostly metadata?
Lisa: It will include content of the agreement--it's light on that right now. Main content is the Data Grant Record which is the heart of the permissions.

Lisa LeVasseur:

- What we're trying to build is governance-neutral. It isn't about a particular regime, it's agnostic. It supports the private agreements.
- The Accord Project (Linux Foundation Project) is a core project. IEEE is creating an extensible schema that can support any kind of information sharing agreement that we will then translate using the Accord Project syntax to see if it works for our needs.

Scott David: Rights can be stated in contract and/or public law. Duties can be described in contract and/or public law. Foucault.

Also spoke briefly about the Global Privacy Control org and spec building the Do Not Sell/Share header bit in the browser.

If there's desire to work on the high level personal agreement/legal layer framework, let's find a place for it. (Could do in the Me2BA Policy and Legal WG).

Call for folks to get involved: IEEE, Kantara, W3C--see links towards end of chat.

Chat Window:
From Scott David to Everyone: Arc of legal process - nice.
From mary hodder to Everyone: How technology can be applied through a legal arc and the life cycle of that. Private agreement legal process.
From Scott David: Legal process at different levels simultaneously; Personally preferred and proffered privacy policies for people. PPPPPPPPPP. ; Knit together layers with shared meaning making process.
From Me to Everyone: (I'm also involved in W3C, Kantara ISI WG) and Scott's BOLTS
From Scott David to Everyone: Law as rhetorical engineering problem ; Consent is overused. Broken for expanded function. Okay for some stuff. ; Spam metaphor
From Marc Davis to Everyone: Are "private agreements" the same as "legal contracts" or something else?
From Kaliya Identity Woman to Everyone: are u recording the session?
From Scott David to Everyone: M2M - machine readable only? If you are the host, are we the parasites?

From mary hodder to Everyone: IEEE 7012 ; Group on privacy terms.. just the eng layer but needs to have a functional legal layer ; worked from Kantara and Customer Commons work on User Submitted Terms ; now called “proffered terms”
From Scott David to Everyone: Life cycle of legal process is embedded in life cycle of larger interaction process. Larger process of non-legal characterizations and meanings of the interactions. Contract formation has specific choreographies of offer and acceptance (and counter offer, etc. etc.). Those will correspond to the characterizations noted here. Auditing performance is generally referenced or described in the agreement.
From Doc Searls to Everyone: Sorry to be late. Stuff going on.
From Scott David to Everyone: Like when agree to “auditing” of performance via courts, versus arbitration versus mediation, etc.
From mary hodder to Everyone: Other groups are also pointing to legal layers without at all defining them; the hand wavy expectation is that there will just be something to point to with all the things you are mentioning Scott: the choreography steps
From Marc Davis to Everyone: Is the goal only machine readable? Back in 2012-2013 we proposed a “Personal Data Rights Language” (PDRL) that had three layers: machine readable; lawyer readable; and human readable (i.e., easily intelligible to a non-lawyer).
From mary hodder to Everyone: Recording and registering should also be there
yes.. Marc: the engineering and human readable is coming along nicely.. but the legal layer is not well definied 7012 is all engineering
From Doc Searls to Everyone: Actually, Zbynek Loebl is big in that space (and without him we wouldn't have met @Jeff), but he's in Prague and could only be here in the morning
From Michel Plante: Does the european GPDR provide privacy terms in machine readable form?
From Scott David to Everyone: Here is a copy of a data sharing agreement checklist. It is only directed at agreements the subject of which is data sharing, but it calls out elements of contract that may be helpful in “grouping” of issues in Standards contexts working on agreement
From Doc Searls to Everyone: @Michel, the GDPR unfortunately does not provide terms individuals can proffer. Instead it considers individuals "data subjects," while responsible parties with full agency are the data controllers and processors. it does say that a natural person can also be a data controller, but nothing more than that.
From Scott David to Everyone: Oops. Ignore the link. I messed it up.
From Michel Plante to Everyone: @Doc, thanks!
From Doc Searls to Everyone: That said, I don't think the GDPR (or the CCPA in California) foreclose terms individuals can proffer. We are still in early days. (Or daze.)
From Marc Davis to Everyone: “Computational Contracts” work at Stanford:
https://conferences.law.stanford.edu/compkworking201709/wp-content/uploads/sites/40/2017/07/WhitePaperDraftfordistroApril32018.pdf
From John Walker to Everyone: Have you looked at the work in the Accord project?
https://accordproject.org/
From Doc Searls to Everyone: Yes, there is a lot of interplay between this work and Accord. Jim Hazard is active in P7012, and other conversations in this space.
From Jeffrey Aresty to Everyone: Our PeaceTones project was part of the Accord Project in their early days - before they got bought up by, I think, Legal Zoom
From Mark Lizar to Everyone: +! +1 = risk assessment
From Doc Searls to Everyone: I didn't know Accord Project was bought by anybody.
From John Walker to Everyone: @Jeffery - I believe the Accord Project is open source;
From Doc Searls to Everyone: I thought it was an open source project within the Linux Foundation.
From Jeffrey Aresty to Everyone: That's my memory as well
From Me to Everyone: Me too

From John Walker to Everyone: Yes that is my understanding - it is under the umbrella of the LF
From Scott David to Everyone: GDPR is not sustainable. It treats all data as equally valuable/damaging. Also, it substitutes attention to the instrumentality rather than the agent of the instrumentality. We don't have duties to make hammers soft. We make hammers hard and have a rule not to hit people with hammers. Data plus meaning equals information/insight=hammer. Need enforceable duties defended with neighborhood watch, not GDPR frozen data concepts from last century. CCPA, HIPAA, GLB, GDPR don't enhance security. At this point they at best provide "safe harbor" duties of care for organizations. Individuals lose once again.
From mary hodder to Everyone: We've been playing with Accord Project.. but then wondering also how does the registry of agreements, the process and the various legal sublayers: PP/TOU and proffered terms, the jurisdictions and points in time and place how does it work?
From Doc Searls to Everyone: Note to the host (Lisa, I assume): this is one of the sessions with a chat that can only be saved by the host. So you might want to save this off.
From Scott David to Everyone: Rights-Duties-breach-causation-damages-liability-insurance-reinsurance. Legal algorithm. Must move from left to right. Accord-ian repair.
From mary hodder to Everyone: Scott: totally agree re the GPPR and other laws you pointed out above.. they are not making privacy or security
From Doc Searls to Everyone: I also think data is a necessary but inadequate consideration, or way to frame things. Brandeis' "right to be let alone," for example, says nothing about data. The "right to be forgotten" in the digital world does require consideration of data, but the spirit of it is very human and non-data-ish.
From mary hodder to Everyone: thats a good point doc.. the 'data' may only be the agreement not to be known but then how much data is in there? the more there is the more the agreement makes you known
From Scott David to Everyone: Maybe this isn't so much the legal process (a big scope), but rather a pathway to construction of a specific rights regime, based on contract, that accommodates human interests. Existing legal regimes elevate group concepts of power from the past (with all of its imperialism, misogyny, and other wonderful features.
From Doc Searls to Everyone: I think, Scott, in your left-to-right structure, that there is in what we're talking about, a right to proffer toward a contract. What would you call that? (IANAL) We actually don't have that in the client-server world—yet.
From Marc Davis to Everyone: Is this the MIT work Mark Lizar was referring to? https://law.mit.edu
From mary hodder to Everyone: Scott.. maybe, it's definitely process, but also by creating various things like registries and agreements, we need to avoid the pitfalls of the past power paradigms
From Mark Lizar to Everyone: Yep
From Doc Searls to Everyone: The GDPR and the CCPA presume a client-server framework, in which only the server side can proffer terms, and keep records. It's crazy, but there it is.
From Scott David to Everyone: Fresh rights statements. Fresh duties statements. Fresh breach statements. Fresh causation chains. Fresh damages structures. Fresh liability allocations. All made fit for function for exponentially-expanded interaction space (5th order effect of Moore's law)
From Doc Searls to Everyone: Good, thanks, Scott.
From Me to Everyone: I'm going to ask us to stop chatting quite so much. Hard to keep track and attend.
From Scott David to Everyone: GDPR and CCPA are also FIPPs and based in 1970s technologies. Well meaning, but ultimately ineffectual.
From mary hodder to Everyone: And the individual, worse, cannot anticipate the effects of their decisions even if they do understand
From Mark Lizar to Everyone: Ok - :-)
From Scott David to Everyone: Bummer
From mary hodder to Everyone: That doc isn't opening
From Doc Searls to Everyone: Same here. won't open

From John Phillips to Everyone: Great conversation guys, really interested in the discussion and its potential for improving the way some things are happening here in Australia (particularly the Consumer Data Right act https://www.cdr.gov.au/) but I've got to go - I'll check out the recording and notes and probably reach out later. Sorry for chatting Lisa! ;)
From Me to Everyone: Marc I see you--you're next
From Scott David to Everyone: Rights can be stated in contract and/or public law. Duties can be described in contract and/or public law.
From Doc Searls to Everyone: To @Marc, I think our consideration began at the meta lrbrl, in the sense that a standard form contract could be pointed to. (As Creative Commons has standard form licenses that can be pointed too.) Since then we've moved to the latter, as Lisa is explaining.
From Mark Lizar to Everyone: @Scott - W3c DPV (Data Privacy Vocabulary Controls) https://www.w3.org/community/dpvcg/ Which is really legal ontology not vocabulary
From Me to Everyone: Human rights or legal rights?
From Marc Davis: @doc good to hear because I think what is needed are standardized computational contracts with mutually negotiable terms an dot do that you needs a computational semantics and syntax for the contracts themselves in which you could ideally parse a natural language legal contract into the computational form and translate the computational form back into natural language. typo: “and to do that you need” @doc I translated my long sentence from the original German ;-).
From Doc Searls to Everyone: Phil Malone (then at Harvard Law, now at Stanford), who brought the federal lawsuit against Microsoft way back when, once told me the one thing that matters in law is harms. "If you don't have harms, you don't have a case." Something like that.
From Scott David: The source of prohibition on organ sales is state and federal law, not human rights
From mary hodder to Everyone: scott.. yes.. i figured it was state based but i’m also saying on a human level, it’s immoral that others would for someone to sell a kidney for some reason
From Mark Lizar to Everyone: Human to Infrastructure — Notice based (humans are universally individuals) so without notice based governance / compliance / (AKA notice and consent) legal layer - Social Gov - then contract is based on the Social Governance Agreement -
From mary hodder: so can moral rights be a part of this? oops for=force up above.. force sale of kidney because much of our objection is the immorality of what we experience now in digital
From Scott David: Existential entrepreneurship Individual publicity rights are a pathway forward
From Me to Everyone: Civilizing the Digital World
From Scott David to Everyone: Sorry Lisa. I cannot resist
From Jeffrey Aresty to Everyone: We are calling it the "justice" layer so that we incorporate the human rights folks, the people we are serving who do not have access to justice; and, the legal layer is one piece of the justice layer
From Me to Everyone: Yes, I really like that Jeffrey and appreciate it.
From Scott David to Everyone: We screw the other guy and pass the savings on to you!
From Jeffrey Aresty to Everyone: We are going to be so far ahead with the work you are doing - it's exciting to connect Scott - who are you working for???? (-;
From Scott David to Everyone: Internet is a shopping mall - private space Private for corporations I am working for my mom
From Jeffrey Aresty to Everyone: @scott - then you are working for the right lady
From Scott David to Everyone: Formally I work at the University of Washington Applied Physics Laboratory
From mary hodder to Everyone: This is the old info: https://kantarainitiative.org/confluence/display/archive/UST+Project+Scope human and legal layers on No Stalking and also Intentcasting:
From Me to Everyone: globalprivacycontrol.org
From mary hodder to Everyone: (also quite old) https://kantarainitiative.org/confluence/display/archive/User+Submitted+Terms+--+UX+and+Interface+V.1

From Me to Everyone: https://github.com/privacycg/proposals/issues/10
From Doc Searls to Everyone: customer commons' #NoStalking term, which has human and lawyer readable layers, but lacks the machine one: http://customercommons.org/home/solutions/tools/terms/p2b1/ Opt-out is pure client-server, where the terms are always set by the servers, and there are a zillion of those, meaning a zillion opt-outs. which is, by design, fucked.
From Marc Davis to Everyone: +1 Doc
From Mark Lizar to Everyone: https://www.w3.org/community/dpvcg/
From mary hodder to Everyone: https://globalprivacycontrol.github.io/gpc-spec/
From Mark Lizar to Everyone: https://wiki.trustoverip.org/pages/viewpage.action?pageId=66469
https://kantarainitiative.org/confluence/pages/viewpage.action?pageId=125469251
From Me: publication of private facts paradox of the internet: no place is private, no place is truly public
From Marc Davis to Everyone: @Lisa exactly: no private residences, no public squares. @Lisa that is why we still live in an online political economy of "Digital Feudalism" in which there were no private and no public spaces for serfs, all spaces were owned and controlled by the lord of the manor.
From Doc Searls to Everyone: Blackstone item: https://medium.com/@dsearls/the-castle-doctrine-45c9abc147e8 "the castle doctrine" in that case.
From Mark Lizar:
https://openconsent.atlassian.net/wiki/spaces/IHD/pages/768245803/Consent+Type+Profiles+for+Privacy+Rights
From Doc Searls to Everyone: Should we have a session tomorrow on Scott's rights challenge?
From Mark Lizar to Everyone: https://github.com/smartopian/OPN-aNG-Accord
From Marc Davis to Everyone: My "homepage" running on a server in my "home as castle" was the original "private" space of the internet we have now lost.
From Scott David to Everyone: Go forth and kick ass! (From a rights perspective)
From John Walker to Everyone: +1 on the Rights challenge
From mary hodder to Everyone: yes
From Scott David: List rights and harms (harms are things that we can have rights to not be subject to)
From Marc Davis to Everyone: Awesome session and work Mary and Lisa. Thank you!

Rolling Back Surveillance Capitalism: Part 2: What are the Obstacles and what Assets can be used?

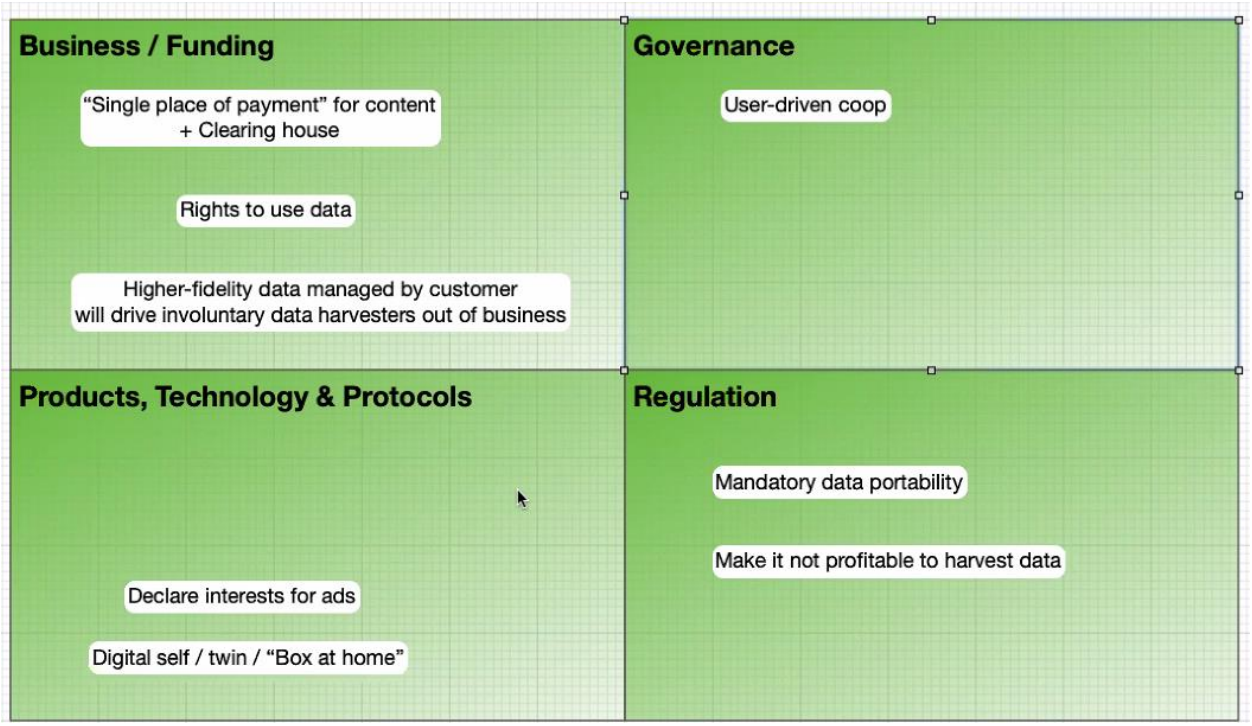
Wednesday 12J
Convener: Johannes Ernst

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

Begins with a recap of previous session
Suggestion - a Data Collection "Credit Report" where a consumer could find out what data different data collectors/brokers have on them?
Some not-promising data points:

- CA law allows consumers to do this

- Nobody does it, including privacy experts
- The processes don't work well, take a very long time
- Data is often provided in a way that's not useful



US centric - I don't care if I am surveilled. How do we raise awareness?
Can we do a data release - show how much data they have on people?
Currently possible in California - process is slow, buggy, doesn't actually work. People haven't really done this. Data being released - some are clearly obfuscating the data, or dump so much data to make it useless.

What are the elements of positive future - what can we possible do to 'get there'.
The market size of surveillance capitalism is on the order of several trillion dollars a year

Hypothetical - what if we took over one of the major telco providers (AT&T, Verizon, etc.) and offered high quality 5G, but didn't allow data collection by vendors on our network.

It would lose money. How much? What parts of it would work? What lessons could we apply to a more workable solution?

Reality - would take at least 2 or 3 friendly billionaires to do the semi-hostile takeover. They would get a less-than-market return for a time due to lack of deals with commercial interests.

Would it even be effective in preventing data collection? Probably not.

What about data poisoning? Could an appliance like a PiHole disrupt data collection?

Need to recognize that there are benefits to directed ads at some point - would rather look at 3 toasters than 3000s.

Curation is already happening on some sites & forums; targeted ads allow the highest payer to get their stuff in front of me but curation by people whose opinions we respect is acceptable. Example - BoingBoing gift guide at Amazon.

What are the obstacles to getting the world to work in the curated model? Monetary loss for vendors - they may not sell stuff you didn't really want that got pushed into your browser by paid ads. Need to determine how to identify & trust "trusted personas" to make recommendations."

Entrepreneur perspective - could have a category where you promise to handle consumer data well (or not collect)? Doesn't make sense for VCs to invest because other companies who offer the same services can monetize consumer data and make more money. VCs could have special-purpose vehicles to fund non-surveilling companies.

Organic food example - you don't have to convince the whole market that organic food is better; if you convince 1% it may become viable.

Need to come up with a business model that would enable companies to operate without dependency on consumer surveillance.

Indie Hacker podcast - lot of examples of startups (https://www.indiehackers.com/podcast). Also Zebra community

Me2ba.org - Me-to-B alliance - describes harms inflicted by surveillance capitalism.

My Data organization in Helsinki, Finland has a good bit of support from the Finnish government. Seems like maybe that's a more receptive environment to resistance to surveillance capitalism. Scandinavian countries, Germany - have a different tradition towards what constitutes society & business.

Possibilities in developing world? People working health care, have seen opinion that USA is one of the most difficult places to introduce social innovations. Entrenched interests are less entrenched in the developing world, dealing with real challenges, more open to innovative solutions. There is interest in SSI, which seems correlated with resistance to surveillance capitalism.

Surveillance capitalism has moved into all categories of life -social media, IOT, walking down the street, etc. - can the market be partitioned to reduce the damage? Mastodon experiment in social media - went quite well in early phases of adoption but never went mainstream.

Equivalent of a VPN or proxy to take on a different persona? For example, sometimes prices are raised based on the customer having a profile of being wealthy. There is a community of people who exchange grocery store loyalty cards.

Getting people to care - just need to tell stories - lots of creepy stories to use.

What are the tools we need to counteract surveillance capitalism? Big ideas in silicon valley don't work, b/c your new company is subject to the same commercial pressures that drove everyone else to surveillance capitalism.

Competition - if Facebook had a lot of competitors, some of whom did better job with customer data, that would drive better behavior.

Data portability - makes it easier to switch providers, would help. Also interoperability, if everyone is on facebook and you can only talk if you are also on facebook it doesn't matter if you move your data

Make it expensive to keep personal data - fines for breaches, etc.

Technical solutions - PiHole example. Raspberry Pi playing white noise over Alexa speaker until the codeword to unlock the RasPi is heard.

Some of these only suitable for techies.

GPDR rulings against big service providers like MIcrosoft create a huge opportunity for newcomers esp. Amid the covid-19 situation and need for remote schooling.

Relationship with service providers should be more like what we have with a maid service - they are highly trusted, have a key to our house, can get into every room but if we decide to switch providers it's very fast and easy to do so.

Local social networks - e.g. run by a school - would allay fears of letting kids onto Facebook. Also could have the whole school community on it, so there's no real reason to join Facebook.

Surveillance now pervasive in schools with use of Google classroom, etc.

In the past in small villages, other people in the village would know your life history and several generations of family history, but you could move away. Today, the history is collected and is global. But in the village you were much more community oriented and working often towards community goals.

JSON-LD Signatures BBS+ 101 Plus Status Updates*

Tuesday 12L
Convener: Tobias Looker
Notes-taker(s): Tobias Looker
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Discuss BBS+ Digital signature, their application to technologies such as Verifiable Credentials and the progress that has been made in the past 6 months with the initiative.

Link to slides - https://docs.google.com/presentation/d/12uZUgNfcMu4-14VocC6DpXbv88Qef1ap-NWdbjh8eM8/edit#slide=id.p2

Great general presentation with lots of interesting questions and feedback.

Sidetree Updates & did:elem Progress

Wednesday 12O
Convener: Orie Steele, Daniel Buchner
Notes-taker(s): Orie Steele

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

https://identity.foundation/sidetree/spec/
https://staging.element.transmute.industries/workbench
https://staging.element.transmute.industries/api/docs/static/index.html
https://github.com/transmute-industries/sidetree.js
https://github.com/decentralized-identity/sidetree
https://github.com/trustbloc/sidetree-core-go

https://github.com/trustbloc/sidetree-fabric
https://github.com/trustbloc/trustbloc-did-method/blob/master/docs/spec/trustbloc-did-method.md

Recovery
https://github.com/decentralized-identity/fuzzy-encryption/tree/master/src/python

What is sidetree?

Sidetree is a scalable architecture for building truly decentralized identifiers.

What are we looking at for the next 3-6 months?

We are looking at hardening and shipping v1!!!!!!!

January is looking like v1 final for the spec and reference (plus other implementations)

We have a couple items left to cover, and hoping to lock things down.

Sidetree is technically what's known as an "embarrassingly parallel" system:
https://en.wikipedia.org/wiki/Embarrassingly_parallel

There was lots of discussion, you covered how sidetree works, as well as did:ion, did:elem, and did:trustbloc…. We covered go and typescript integrations, gave a demo of did:elem, and discussed future work for sidetree that we are excited about.

Defending the Human OS: Augmentation vs Displacement

Wednesday 13A
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:

Orienting Towards Positive Augmentation of the HumanOS (Human Nature) vs Invasive Displacement of the Same.

This session is designed to contemplate and consider all peoples of the world based on the shared root of our ancient and genetic Human Nature.

Until we can find handles to adjust or state of digital presence (Real-IT), or be respectfully treated by default (Me2BA), we are in the currents of events well beyond most anyone's ability to holistically manage digital experiences at the internal, personal level.

Premises of discussion

Human Nature has been met by code written to "optimize" the Human OS.

- Togetherness, mute children speak, lame children can run…
- Omnipresent information to feed curiosity, R-IT.Voyeurism, R-IT.Self-Aggrandizement = ego-casting
- Price of admission to be present with most of one's familiar community Especially for tween-teen ages as they strive to find their social place. **
- Information is heightened, as well as diminished, by "the Cult of the Amateur" as Andrew Keene would put it.

** exacerbated by C-19

Real-IT: Understanding the relationships we choose to have, or not have, with information technologies. Our Real-IT will reflect into our Reality

1. Our HumanOS is generally unprotected from this layer of insult. "Good tech is invisible" so who can even tell until stuff starts growing on your digital presence?
2. Our Sensor package is over-clocked = stress… Who has been honest and open until…now?! (Social Dilemma, etc.) ...about this when it mattered most? Who's talking about VR?
3. IIW.29 – The Gravity Wars: VR v Real World. Who trains people on dealing with the vortex of other idyllic worlds for the socially uncomfortable or narcissist
4.

As people (we) step into a gamed space…

- Advancement of brain science allows "the house" to have an extraordinary ability to impart and extract not only data, but experiences; nudging of emotional ups and DOWNS (x6+)
- Brain Science and platform motives (often dealing with profit first) rules SocNet like "the House" rules (and adjusts on the fly) to a tilted gamble regarding the COST
- As a Parent; the competition from a device optimized to engage my kid is a great offense to my opportunity to raise my child with fighting psy-op science trying to win my kid's head and time

away from the world around, but maybe more importantly, away from the person she would have been under the influence of the local priorities and tasks which lay before her…

! - Much socially based platform code has been written to optimize clicks. Clicks are optimized when we're upset. Dry cleaner 10 good for every bad, cause angry person tells 10 people, happy person tells 1

! - Twitter fallacy spreads 6X faster than truth.

! - Notable vulnerable communities: Parenting, Elderly, Uninclined to IT risk, do not love tech, people who find machine relationships alien to their Human Nature.

CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability

Wednesday 13B
Convener: Deepak Maram, Harjasleen Malvai

Tags for the session - technology discussed/ideas considered:
Legacy-compatibility, key management, bootstrapping, sybil-resistance, privacy

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

A lot of the discussion focused on our previous work, DECO, which we use as a building block in CanDID. DECO allows a client to prove statements about a TLS session in zero-knowledge, using only cryptographic trust assumptions. Another solution is to use TownCrier, which allows the same functionality, using trusted hardware.

Overall, we showed that various problems get swept under the rug in most identity systems, including bootstrapping, key-management, Sybil-resistance and privacy-preserving and decentralized mechanisms for regulatory compliance. We also show various mechanisms for solving each of these problems.

Link to paper: https://eprint.iacr.org/2020/934

Link to DECO: www.deco.works

Survey of Aries Frameworks PLUS Announcing Two New Mobile Native Frameworks

Wednesday 13C
Convener: Alexis Falquier
Notes-taker(s): Alexis Falquier - Google Doc of session

Tags for the session - technology discussed/ideas considered:
Frameworks, interoperability, aries, wallets, agents

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

Slides for framework document:
https://docs.google.com/presentation/d/1rZJMyPlIFuwQNhIlJshf12Ezu22as25L7vm0GwmN-8I/edit#slide=id.g74b8820553_46_868

An SDK Approach for Issuing Credentials

Wednesday 13D
Convener: Michelle Dick and Nate Sulat (michelled@kiva.org and nates@kiva.org)
Notes-taker(s):

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

Presentation on credential issuance: https://docs.google.com/presentation/d/19VBC0WXvx0-yS7oj8OseuSfAaU-n30gZt2_R2E4NnAM/edit?usp=sharing

Presentation on credential verification:
https://docs.google.com/presentation/d/1WwcGfMnIThZAzZk3cJyfDXPZl0whktDSJLDfVmPlJMM/edit

Open-source repo: https://github.com/kiva/protocol-common

DIDn't: did:un and Overlap Between DIDs & KERI [DIDnt, how KERI and DIDs overlap]

Wednesday 13E
Convener: Charles Cunningham

Tags for the session - technology discussed/ideas considered:KERI, DID Methods, DID Resolution

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

Current document is here:
https://github.com/decentralized-identity/keri/blob/master/did_methods/un.md

DIF: Presentation Exchange, Progress Updates!

Wednesday 13F
Convener: Gabe Cohen & Daniel Buchner
Notes-taker(s): Gabe Cohen

Tags for the session - technology discussed/ideas considered:
DIF, VCs, Presentation Exchange

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

Slide/Presentation provided by Gabe Cohen:
https://identity.foundation/presentation-exchange

The discussion was a high-level overview of the specification as we near v0.1.0. Daniel Bucher discussed future ZKP and other format support. We encourage all to attend and join DIF and contribute on the GitHub. We intend the specification to be used by a wide number of companies on different tech stacks and we have taken care to support as many use cases as possible.

Kim Duffy raised a point about considering prior art and hesitation around "re-inventing" generic selection language. Daniel responded stating we heavily leverage JSON Path, and JSON Schema, and have looked at a number of open source alternatives, none which quite met the case. Gabe responded that we are open to improvements, suggestions, and change if there are better alternatives.

The Rising Tide of Deanonymization: The consequences of Self-Sovereign Identity in the context of "organizing the world's information and making it universally accessible and useful."

Wednesday 13G
Convener: Chris Buchanan @ MITRE

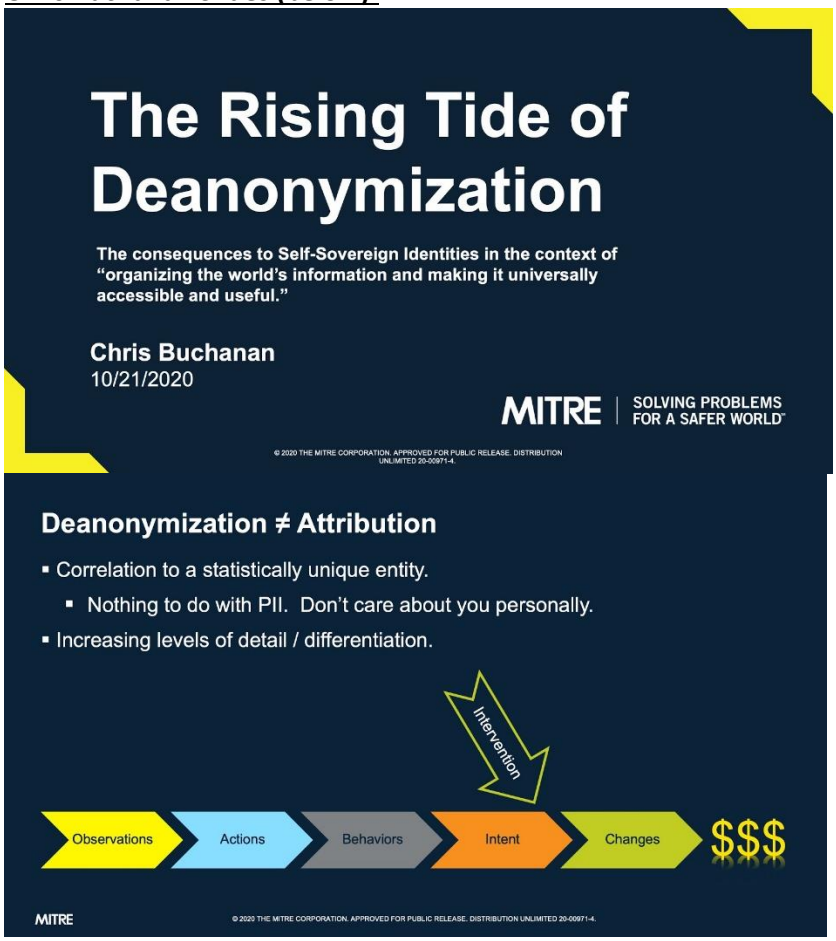
Tags for the session - technology discussed/ideas considered:
Anonymization, Deanonymization, SSI

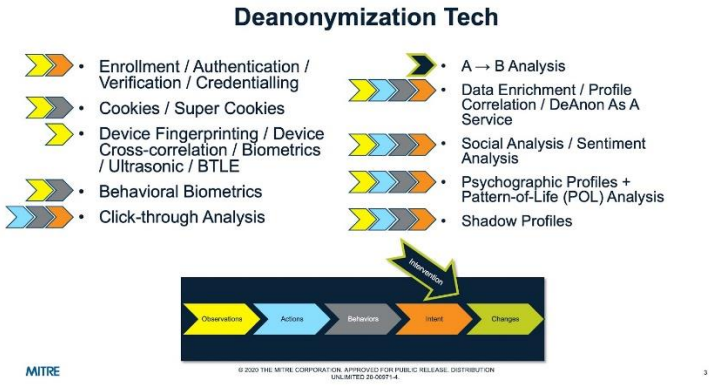
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Chat:
From By_Caballero to Everyone: silly question but will this be recorded? I am triple booked but this session is very relevant to multiple projects I'm working on :D
From Chris Buchanan to Everyone: We will record.
From By_Caballero to Everyone: if people are ok with recording, someone just has to claim host with code "232323" and select "record to cloud" thank you so much! look forward to that clearinghouse that Trev mentioned, and listening to the recording later :D
From Adrian Gropper to Everyone: It's the way Apple Google does COVID
From David Huseby to Everyone: any form of centralization is an attack point. be it a company or a domain name or central servers.
From RuffTimo to Everyone: And yet Facebook purges 3+ billion fake accounts annually...
From Shigeya Suzuki to Everyone: Where to create the account... (I mean, not from home, right?...)'
From Scott Harris to Everyone: From a burner phone? I'd like to try that experiment
From Jim St.Clair to Everyone: @shigeya, try a TOR router :)
From David Huseby to Everyone: Purism's Librem 5 phones have hardware switches for disabling radios and has a removable battery.
From Shigeya Suzuki to Everyone: Right...
From Jim St.Clair to Everyone: WiFi automatically turns back on when it detects a known network
From David Huseby to Everyone: the baseband radio is isolated as a peripheral usb device so it has no direct access to I/O devices and memory and cpu. https://puri.sm/products/librem-5/ and now Purism has their own MVNO so you can get cell service from them directly
From RuffTimo to Everyone: Love the premise that SSI creates a "regulatory pathway". Great job, Chris! Gonna go catch another preso… Ciao!
From Chris Buchanan to Everyone: Thanks Tim
From Jim St.Clair to Everyone: 800-63
From Trev Harmon to Everyone: It's going through a revision right now, as well. That's worth watching.
From Jim St.Clair to Everyone: correct Trev You feel ok, Adrian?
From John Phillips to Everyone: I think you could use a Chinese response to the question of whether Adhaar has done more good than harm.... "to early tell" (this was a response to a question of whether the French revolution was a good thing) ^too early to tell (sorry, typo)
From Eric Weber to Everyone: So now we self-sovereign hardware and self-sovereign internet?
From Adrian Gropper to Everyone: https://indianexpress.com/article/india/new-digital-health-id-will-be-used-in-covid-immunisation-says-pm-modi-6795239/lite/
From John Phillips to Everyone: I'm getting images of wearing an Apple cloak of invisibility - but don't we need to address accessibility? Not everyone has, or can afford, Apple devices
From Gabe Cohen to Everyone: https://github.com/derrumbe/spartacus-as-a-service

From Salvatore D'Agostino to Everyone: so i think you want to improve the range and force of the right to privacy as a driver for laws..
From John Phillips to Everyone: Great discussion, thanks Chris et al
From Steven Wilkinson to Everyone: Thanks!
From Shigeya Suzuki to Everyone: Thanks
From Jim St.Clair to Everyone: thanks!!

Chris Buchanan Slides (below):





Rough Assessment of Accessibility (if exists / non-holders)

Type of Data	Individual	Corporation	Government
Enrollment / Authentication / Verification / Credentialling	🟠	🟡	🟢
Cookies / Super Cookies	🔴	🔴	🟢
Device Fingerprinting	🔴	🔴	🟢
Biometrics / Behavioral Biometrics	🔴	🟡	🟢
Click-through Analysis	🔴	🟠	🟢
A → B Analysis	🔴	🔴	?
Data Enrichment / Profile Correlation / DeAnon As A Service	🟢	🟢	🟢
Social Analysis / Sentiment Analysis	🟢	🟢	🟢
Pattern-of-Life (POL) Analysis	🟢	🟢	🟢
Psychographic Profiles / Shadow Profiles	🔴	🟠	🟡

MITRE

To test your anonymity, try being someone else

- Create a synthetic ID (don't steal)
  - Do not utilize any email or phone number already associated to you or another real person (including by the phone company).
  - Supporting data can be real if it doesn't resolve to an individual.
- Create a Facebook account utilizing the synthetic ID.
- Create a Google account utilizing the synthetic ID.
- Keep them alive for a month.

MITRE

Designed for Deanonymization

- Smart phones do not have user profiles.
  - Cell-phone → Wireless Plan → Credit Check. → KYC Regulations
- Turning off Wi-Fi and BTLE is difficult for the user.
- GPS receiver cannot be turned off.
- Push to higher authentication mechanisms (biometric).
- Battery not removeable.
- SIM not removeable.
- Cellular networks converged.
- AI/ML built into device to pushing computation costs to the user.
- All other devices interoperable with smart phone.

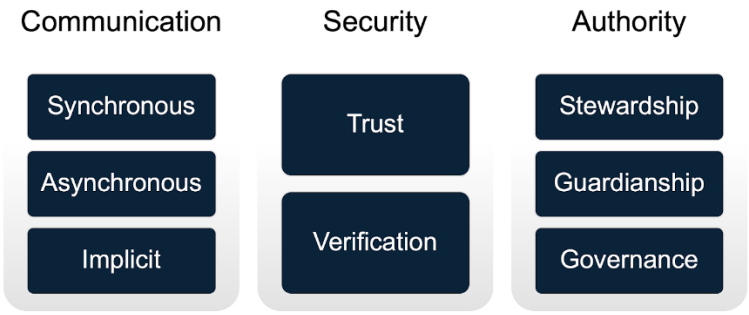
MITRE

What changes with SSI?

- Enrollment / Authentication / Verification / Credentialling ← Nonrepudiable
- Cookies / Super Cookies ← Nonrepudiable (w/NR session)
- Device Fingerprinting / Device Cross-correlation / Ultrasonic / BTLE ← Nonrepudiable (w/NR session)
- Biometrics / Behavioral Biometrics / Environment
- Click-through Analysis ← Nonrepudiable (w/NR session)
- A → B Analysis ← Nonrepudiable (w/NR session)
- Data Enrichment / Profile Correlation / DeAnon As A Service ← Elevated Assurance
- Social Analysis ← Nonrepudiable and cross-correlated
- Sentiment Analysis ← Nonrepudiable and cross-correlated
- Psychographic Profiles + Pattern-of-Life (POL) Analysis ← Nonrepudiable and cross-correlated
- Shadow Profiles

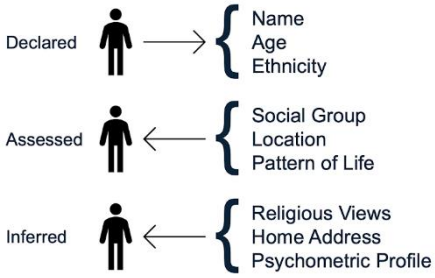
MITRE

Identity is for Transactions



MITRE

Identity Described: Correlation as a Directed Graph



We have no rights to prevent others from assessing, inferring, or transmitting our identity information.

What is the harm?

MITRE

3

Digital Identity is Not Equivalent to Physical Identity.

- **Transience**
  - Most physical identity transactions are transient and quickly forgotten.
  - The internet never forgets.
- **Retransmission**
  - The physical world is severely limited in its ability to transmit and consume data and must therefore be selective.
  - The internet's entire purpose is efficient retransmission of data.
- **Degradation**
  - Physical world data degrades in both quantity and quality over time and when it is retransmitted.
  - Digital information is perfectly preserved in storage and retransmission.

MITRE

The Accumulation of Digital Identity Artifacts

Because digital identity lacks transience and degradation but has perfect retransmission, the accumulation of digital identity artifacts creates a window into psychographic and behavioral details for which **it is impossible to gain the conscious consent of the subject**.

- **Privacy is not about property.**
  - Soldal v. Cook County (1992)
- **The privacies of life must be protected against arbitrary power.**
  - Carpenter v. US (2017)
- **But… this is not a constitutional issue. It's an issue of standing (locus standi).**

MITRE 5

What is the Harm in the Accumulation of Digital Identity?

The intentional creation of an imbalance of power in the information domain which is utilized to consolidate power in the economic and political domains.

Specifically:

- **The surreptitious creation of detailed biographic or psychographic data regarding users or groups of users.**
- **The algorithmic biasing of information delivery for the purpose of monetizing users' attention.**
- **The tapping of biological processes without the consent of the user or against their best interests.**

MITRE 6

Combatting Accumulation with Regulation

Define identity data to include declared, assessed, and inferred identity.

Regulate

- *Transience* as temporal minimization.
  - Data may only be collected or kept if it is necessary for follow-on transactions with or on behalf of the user.
  - Only necessary data may be retransmitted to a third party.
- *Retransmission*
  - User must explicitly agree to any identity data retransmission.
  - Data may only be retransmitted to another entity *n* times where *n* is defined by the user.

Encode *Degradation* via differential privacy mechanisms

Outlaw

- Surreptitious user profiling.
- Attention optimized information delivery.
- Algorithmic manipulation of biological processes against user consent or user interests.

Limit the use of digital identity to transactional activities.

MITRE 7

Chris Buchanan
cjb@mitre.org
@MITREcorp
linkedin.com/company/mitre

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

ToIP Interoperability Profiles

Wednesday 13H
Convener: Drummond Reed (for Dan Gisolfi and Darrell O'Donnell)
Notes-taker(s): David Luchuk

Tags for the session - technology discussed/ideas considered:
Session called by ToIP Technology Stack Working Group to discuss recent announcement - first ToIP Interoperability Profile (TIP)

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

Link to the ToIP Foundation blog post.

Link to the slide deck from the ToIP Technical Stack Working Group (see especially slides 11-14).

Trust over IP - evolving concepts and applications of a dual (human and technical) stack that has four layers - Utilities, Peer-to-Peer, Data Exchange, Applications

Technology Stack WG - convergence toward interoperability of elements on the technical side

Governance Stack WG - models for interoperability on the human side.

ToIP Standard Specifications (TSS) - fully standardized components of the stack, specifications that have broad community adoption

Filling gaps in the stack, where TSS do not yet exist, requires custom specifications to achieve top-to-bottom interoperability that meet the needs of a specific set of vendors and use-cases in a trust ecosystem. This is what we call a ToIP Interoperability Profile (TIP).

Because there are no TSS yet, current work on TIPs by the Technology Stack WG requires pulling DID specs into the stack to test what can work interoperably.

Saturn V TIP - first published implementation of the stack … adopted as a draft deliverable of the Technology Stack WG. Link to the blog post about the Saturn V TIP.

WG has taken on the task of completing a Saturn V TIP and use this progress to, in part, put together templates for other TIPs that can then be tested and implemented to produce adoption metrics for vendors.

Saturn V TIP achieves cohesion top-to-bottom but is not necessarily geared toward a specific market use.

Purpose of the recent announcement is to encourage vendors to be part of the next stage of testing for the full-stack implementation.

WebID: The Web Platform, Privacy and Federation

Wednesday 13J
Convener: Sam Goto, Dick Hardt, Vittorio Bertocci, George Fletcher, Aaron Parecki
Notes-taker(s): George Fletcher

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

[Sam will share his slides used for introducing the topic]
https://docs.google.com/presentation/d/1rnFtThP-drlMKdDDcxknWI1BcswcFZ0LrTMqODoMJrM/edit#slide=id.g831751c125_1_829

Premise: federation is good, we want to preserve it, it's certainly better than username/password.
Framework for evaluating priorities

- User's first
- Developers second (RPs and IDPs)
- Frameworks third (browser engines)
- Technical purity fourth
    - ?Where does compatibility with existing processes come in?

Current federation is built using browser primitives like iframes, cookies, redirects, popups, etc. Browsers need to apply the lowest common denominator policies to these primitives.

Tracking on the web has also been built using these primitives.
E.g. facebook comment widgets on different blogs mean facebook knows all the blogs you visit

Goal is to prevent RPs colluding to track users, and also prevent IdPs from knowing everywhere the user logs in.

In regards to privacy… even "users" need a gradient of protections as implemented by the browser. Maybe use an opt-in model as opposed to an opt-out one.

RP tracking problem:

- Use directed identifiers
- Separate authentication and authorization (don't combine them as OIDC/OAuth do today)

Options for solutions

- The permission-oriented variation
    - Browser provides interstitials to ensure the user wants to use that IDP and the browser can also inspect the user data flowing back through the browser to provide help to the user that globally correlatable identifiers are being shared
    - If user agrees to interstitials, the rest of the UI is under the control of the IDP
- The mediation-oriented variation
    - No IDP UI, browser managed the UI
    - Browsers can control defaults
    - Browsers only mediate in the exchange of the tokens but not in the authentication of the IDP

    - User authenticates to IDP without knowing where the user wants to login (no knowledge of the RP)
- The delegation-oriented variation
    - Not covered in this session

Online JWT Interactions (QR Codes/Buttons For Claiming and Sharing VCs)

Wednesday 13K
Convener: Jace Hensley
Notes-taker(s):

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

https://github.com/hellobloom/online-jwt-interactions

Talked through the spec.

Talked about another use case where the user/wallet may want to initiate the share flow. Where the user presents/sends a QR code or link and the verifier can fetch the VP and get the shared credentials. Use case could be where a boarding pass is issued to a user but the user won't have internet access at the airport so they want to store a VP/VC at some link that the gate agent can scan and verify, without the user needing to be online (at least not at time of share/verify)

SSI for COVID 19: A Comparison With Alternatives

Wednesday 13N
Convener: Kaliya Young Identity Woman, Lucy Yang
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:
SSI, covid, corona, pandemic, public health
CARE principals for data: https://www.gida-global.org/care

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

- The general goal of this session is to collect input from session members on what are the alternatives to Verifiable Credentials that are being applied to address the health information challenges within this pandemic.

- Alternatives to test result delivery VC's:
    - In person - face to face
    - Test results communicated via a telephone call
    - Text message
    - Email delivery PDF document delivery of test results
    - Sending to a third party on your behalf.
    - Employer Testing on site.
    - Direct Access to Health Records - for decision making about COVID travel.
    - Government keeps a database of test results relative to a national ID number
    - Mobile phone app authentication
        - In the Ukraine
        - Install of the app for authentication
        - Intermittent checking from a government authority on location
        - Once tested-intermittent feedback fr government on test result status
- Alternatives to Vaccination Records
    - Yellow Cards
    - Child Vaccination systems today track who has been vaccinated in the state level in databases.
    - National Level Database of people's name addresses and status.
- Problems
    - Fraud - easily faked
    - Theft
    - Malicious disruption (county where defence workers - your test came back clear - ok to go to work)
    - Impersonation
    - Damage to the artifact
    - Loss of phone
    - Binding
    - Closed source code is a threat vector so you can't see it.

People who don't have conventional forms of ID

- No state ID / health care number / birth records
- No stable address / phone number / email address

Attacks and failures are at the edges.
Fax Machine is core to the healthcare system today.
Infrastructure - verify signatures with public keys is 50 years out?

Johannes - gorry details of COVID apps.
Failure scenarios - what if the subcontractor of your official app snuck in some code that benefit the contractor (actual case)
Failure scenarios are whole system

- Operations
- Governance
- Technology

Authenticity

Goals	Updatable/Revocable	Who sees the data?	Verifiable (crypto Signatures match and come from assured place)	Binding	Durable	Secure (at systems level?)	Portable	Interoperable	Scalable	Shareable
Goal Definition					Tamper proof?					
CommonPass	?	Trusted intermediary	80% yes Trust framework	Yes	Yes	Encrypted central database	Yes	No. Only within the network	Limited?	Yes
Phone calls	No	Parties on the call	No	?? (subjective - dependant on the call participants	No	No	No	No	No	No
SMS	Multiple delivery possible	Sender / Receiver	No	No	No	No	No (point to point)	Yes	No	Yes (forwarding)
Fax/Mails		Lab - person - whoever they send it to.	No	Hard (name match?)	no	No	no	NO	Yes (works at scale today)	
Paper f2f	No	Lab - person - whoever they share paper with	No	Hard (name match) photo? fingerprint)	Paper can get wet & lost	No	Yes	Anyone can read it	Yes	Yes
Email	No	Lab - person - whoever they e-mail	limited		No					
Centralized Database	Yes	Data base owner (they also see who pings DB)		depend	yes	depends	no		yes?	hard

Web Portal (With weak Authentication)	Yes	Lab whoever upload the information Probably lab has a database								No Unless you want to share the authentication
Work place testing	-	The employer		Yes			Yes	No	No	No
Verifiable Credential JSON-LD	In theory.	Lab - person.	Yes	Name Match possible	Yes	Yes	Yes	Yes - It is based on an open standard	Yes	Yes
Verifiable Credential with ZKP	In theory.	Lab - person.	Yes	Name Match possible	Yes					Yes

Verifiable Trust Bases: How To Make The Web Of Trust New Again With KERI

Wednesday 14A
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:

See slide deck here:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERIVerifiableTrustBases.web.pd

SIOP: Progress on the Laundry List (wrt DID)

Wednesday 14B
Convener: Tobias Looker, Oliver Terbu, Kim Cameron, Kristina Yasuda
Notes-taker(s): Kristina Yasuda

Tags for the session - technology discussed/ideas considered:
Self-issued OpenID Provider, OpenID Connect, CHAPI, DIDAuthn, OIDF, DIF

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

Agenda

1. What is SIOP/did-siop & WG in OIDF
2. SIOP requirements list
3. Laundry list update/deep-dive & from IdPs to IdSPs
4. PWAs and SIOP

1. **Intro Slides:** https://docs.google.com/presentation/d/1K9jlC17uDC-JYiomcJI8cbZX8pXJwJZcr5Y8M_9c1T0/edit?usp=sharing
    1. SIOP is in session 7 of OIDC spec
        1. No OP needed
        2. Identifier represented as asymmetric key pair controlled by the user
        3. Limitations: crypto, etc.
    b. DID SIOP - spec version 0.1 in DIF (https://identity.foundation/did-siop/)
        1. Id_token used to prove user control over a DID
        2. Adds new claim to id_token
        3. Challenges: incomplete for iOS and desktop

    Work done in OIDF

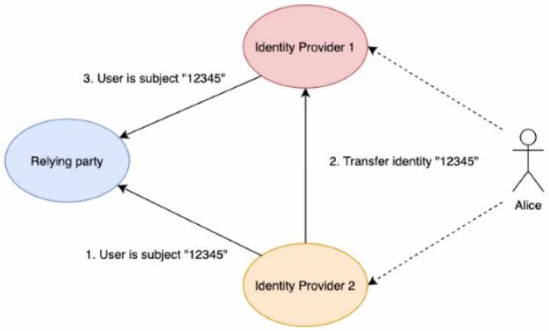
2. **Requirements List for SIOP:** https://bitbucket.org/openid/connect/src/master/SIOP/siop-requirements.md

3. **Laundry list update:** https://docs.google.com/presentation/d/1mNkseYBxOs90whrgDonYyVZj3SqA2QGsn_pp-JpLapY/edit?usp=sharing

- 3 Problems SIOP attemps to solve
    1. Portable identifiers between providers
        1. Sub / sub_jwk claim
    2. The NASCAR Problem
        1. openid:// scheme
    3. Dealing with different deployment types of OP

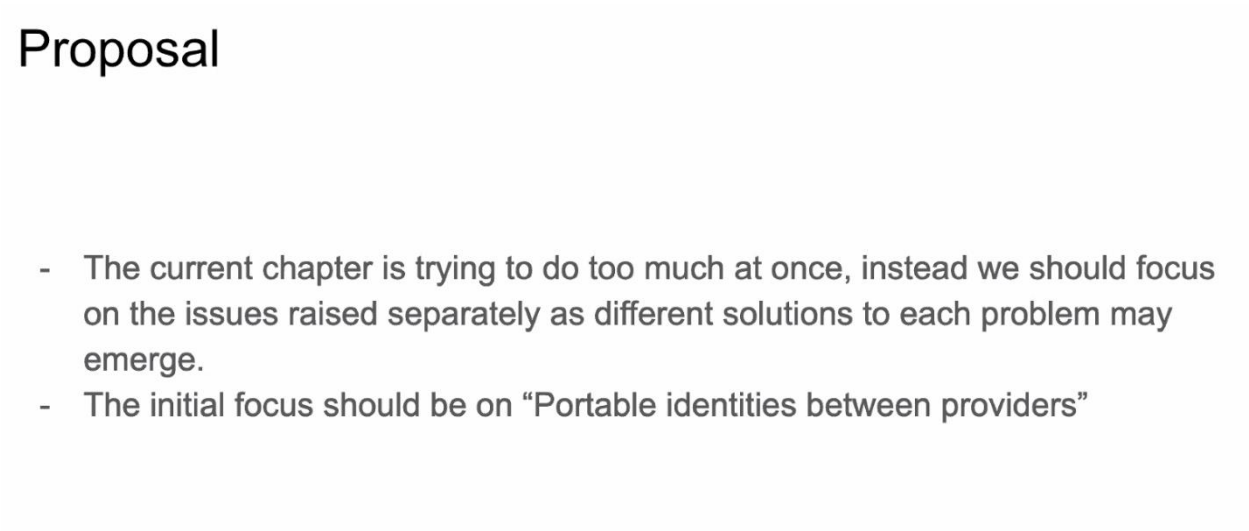
Enabling portable identities between providers

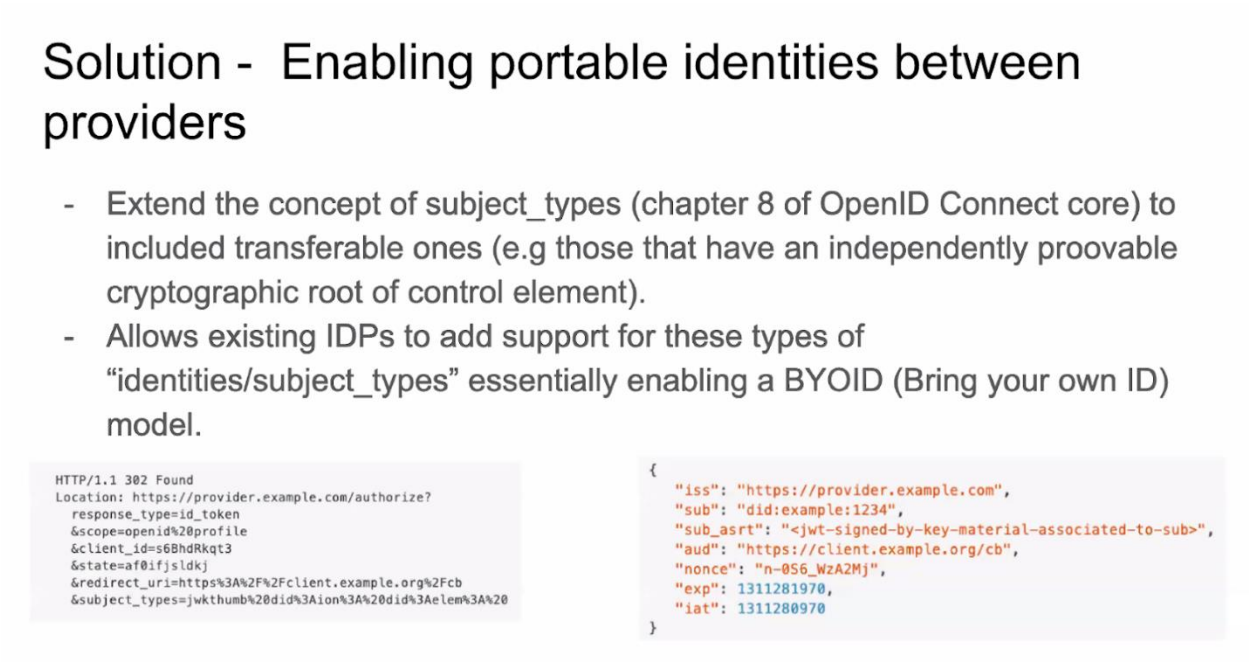
- How can we separate the coupling between the provider and the identity it is providing?
- How can I make these identities transferable between providers without having to start again.



Problems / Questions to answer?

- Is self issued an extension of the core OpenID Connect Protocol or an alternative flow?
  - At the moment a SIOP request is not a *valid* OpenID Connect request
  - The *id_token* returned from a SIOP response requires different signature validation rules and the role of the provider is unclear (e.g distinction between the end-user and provider is blurred).
  - Should an existing (conventional) OpenID provider be able to self issued responses?
- Unclear what happens where there is no protocol registration for scheme “openid://”
- Subject identifier prevents key rotation encouraging long standing usage of a single key pair.
- Static OpenID metadata
- We have a list :) https://bit.ly/3jmPmjs





4. **PWA and SIOP :** https://drive.google.com/file/d/1LZHgcyaEm1CgtKucN0Gib4BvQ4m-_Cho/view?usp=sharing

- From IdP to IdSP(Identity service provider)
- Currently, large providers give us identifiers; in a new model, user uses wallets to self-issue identifiers and manage their keys; to which claims providers issue claims
- ID key Service Provider?

Next Steps:
Join OIDF WG calls!: https://openid.net/wg/connect/
File issues in BitBucket: https://bitbucket.org/openid/connect/issues?status=new&status=open

Resources

- Orie: demo, using PWA, SIOP and CHAPI… https://chapi-siop.did.ai/
- a demo PWA wallet: https://wallet.interop.transmute.world/

Questions, Comments highlight

- Ben: can we use DID uri as redirect_uri?
  - Have not thought of it..
- Adrian: does SIOP solves user-tracking problem?
  -> in theory, yes. Would depend on the implementation
- Debbie: Are identifiers portable in 2 directions?
- Adrian: overlap with FIDO 2
- Dmitri: proposal to alternative for a custom URL scheme?
  -> nothing concrete
- Orie: CHAPI and different options of using it?
- Tom: there is no redirect in the mobile device - goes directly
- Dick: Native app vs Browser app = different experience
- Dick: what if there is more than one wallet? Disambiguation
- Oliver: would it make a difference if IANA registered schema? iOS 14, you can opt in - became an option (David)
- Dmitri: need browser support; while exploring - a lot we can do with polyfills?
  - David: Have you tried CHAPI polyfill on safari? - prompts you 2-3 times per interaction - hard to have good experience; all credentials may go ahead with CHAPI
  - Tobias: Web Origin may not be storing credentials - ability of using the credentials goes away
- Bengo: why we need browser support
  - Dmitri: OS support is needed; OPs have no way to know if your user/agent supports SIOP?
- David: Universal links - would that still work?
- Kristina: idea of proving integrity of the authenticator
- Mobile device that manages DID related

Zoom Chat

From Dmitri Z : +1 to record
From David Waite : +1
From Dmitri Z : yeah it's been really intense, session wise!
From David Waite : There can be only so many participants named Boaty McBoatface
From Orie Steele : I made this tacky demo, using PWA, SIOP and CHAPI… https://chapi-siop.did.ai/
From Wayne Chang : ^ think you forgot "5g" in that link
From Orie Steele : https://self-issued.me/.well-known/openid-configuration
From Dmitri Z : @Orie - whoa, nice!
From Orie Steele : Its terrible ; Everyone is using that
From timcappalli : Lol @5G
From Orie Steele : https://github.com/decentralized-identity/presentation-exchange
From Kristina Yasuda : https://identity.foundation/did-siop/
From Dmitri Z : also on desktop...
From Orie Steele : Nahhh guys, we can keep using only RSA forever :)
From David Waite : FWIW Apple no longer recommends using custom url schemes, so its unlikely they will fix their current behavior.
From Vittorio Bertocci : @David I would have bet money that you would have commented on that :D
From Dick Hardt : Custom URL schemes are a security issue
From Orie Steele : Meaning opened:// ?
From David Waite : yes
From Orie Steele : Or openid:// ?

From Dick Hardt : That one too
From Orie Steele : :(
From David Waite : You can have universal links/app links, such as having an app or list of apps that will open (if installed) on links to https://self-issued.me or the like
From Dick Hardt : Universal links allow an app to own a URL
From Orie Steele : Confused… pretty sure mike jones owns self-issued.me
From David Waite : Think instead of progressive web apps, progressive native apps. Twitter.com links open a browser or a native app depending on if the native app is installed
From timcappalli : Yes, Apple already said they have plans to change this behavior, even for SIOP ; The user getting prompted isn't a great solution either
From David Waite : Yes, the owner of self-issued.me would have to say they authorize your app to act on behalf of their domain. But thats different than custom urls, which don't have any root to base trust on
From timcappalli : A user is not going to know which wallet app they should use
From Orie Steele : So the proposal is use https://pwa.example.com instead of openid:// ?
From timcappalli : This is a much bigger problem than we're collectively making it out to be
From Oliver Terbu : openid:// is not mandatory
From Vittorio Bertocci : You can't support multiple wallet apps if they all need to sue the same domain
From Tobias Looker : @Orie I'll cover with mine hopefully
From timcappalli : Which is exactly the problem ; How do you interoperate wallets then?
From Tobias Looker : @Vittorio agree
From Neil Thomson : https://bitbucket.org/openid/connect/src/master/SIOP/siop-requirements.md
From Dick Hardt : Wallets will need mobile OS support to work well
From timcappalli : Right, but they don't
From David Waite : Its also worth noting that App Store rules prevent an app from requiring another app to be installed, so there are extra limitations from how you could use _any_ installed wallet app.
From Tobias Looker : In short the browser has some role to play
From timcappalli : And an Apple or Google's response will be to say to use the OS's wallet
From Orie Steele : Progressive Web Applications are the future of identity.
From Tobias Looker : Either expanded protocol handling or something more advanced like CHAPI or WebIDs proposal
From timcappalli : And Apple hates PWAs too.. soo
From David Waite : (But universal links would give you an easy fallback of a web-based wallet)
From Orie Steele : Apple hates fortnite too
From David Waite : This sounds like I should create a session tomorrow :D
From Dick Hardt : All RPs would need to use the same universal link — what would that be?
From Dmitri Z : @David - top 10 things Apple hates? the session?
From timcappalli : That doesn't solve the issue though Dick ; Because if the user has multiple wallets, and most will, how do they know which one to choose if presented with a picker
From Dick Hardt : @Tim I think you are agreeing with me.
From David Waite : "Supporting wallets on mobile"
From timcappalli : This exists on Android today, but confuses users ; :)
From Orie Steele : Chapter 7 bankruptcy?
From Debbie Bucci : would supporting multiple wallets equate a union of all? Its not select the correct wallet but correct claim/did etc?
From Dmitri Z : @Debbie good question. So far, the design is - select the wallet first
From Tom Jones : Interesting question - each wallet would have its own access end point ; The RP would not understand that
From Dmitri Z : uuuugh, the "can't remember which identity you used" is the WORST part of Nascar problem ; like, I'd put up with 50+ screens of logos, if the thing just remembered...

From Tom Jones : Yet - sux
From Orie Steele : yep
From Tom Jones : The browser could be the mediator, potentially, or any such password manager ; Something needs to track web sites for users
From David Waite : Credential Management API in W3C has a federation credential, but no browsers support it AFAIK
From Dmitri Z : @Tom @David - have you seen the Credential Handler API proposals? ; (there's a polypill too, which deals with lack of browser support)
From David Waite : That 'sort' of thing, or the 'WebID' proposal, would be ways to have the platform help with persisting state for discovery
From Orie Steele : https://whatwebcando.today/credentials.html
From Ajay_Jadhav : @Tobias - do you think a KERI identifier be used with SIOP ?
From David Waite : If you have a single wallet, you could have it also be the place for state/discovery - but there's no way to be the only provider of something for a platform :D ; (Except being part of the platform)
From Tom Jones : Should not care if keri or any self-issued id
From Ajay_Jadhav : Oh I see
From Oliver Terbu : @Ajay_Jadhav: no assumptions are made about specific DID methods
From Ajay_Jadhav : That's cool
From Kristina Yasuda : but RP should be able to advertise which did method it supports
From Orie Steele : The security failure of preventing key rotation is the worst.
From drummondreed : It's a non-starter
From Tom Jones : We would need the browser to support that
From Orie Steele : gg
From Dmitri Z : @orie it was proposed during a more innocent times.. before DIDs. :)
From Kristina Yasuda : "innocent"
From Dmitri Z : :)
From drummondreed : Yes, agreed. But we have to fix it now.
From Wayne Chang : Open questions around interactions between DID and WebID too
From Ajay_Jadhav : Haha - "innocent" :)
From Tom Jones : No interaction with web id ; Web id doesn't care
From David Waite : @Dmitri CHAPI is very interesting. It does seem to promote issuer = holder, and I'd rather see a first-class credential type rather than wrapping things in "web" ; A set of first-class credential types, rather
From Dmitri Z : @David - can you say more? why issuer = holder?
From Tom Jones : Well - we can push some of this to the http header
From Dmitri Z : (oh agreed, I'd looove a first-class credential type)
From Oliver Terbu : CHAPI is just a message pipe, not more ; According to Manu @last IIW
From Dmitri Z : @Oliver - is true
From Orie Steele : I love seeing provider.example.com instead of self-issued
From Tom Jones : So this problem cannot be solved by openid ; That's what nascar does
From David Waite : I could see CHAPI being used to register a bank credential at the bank, and then a request for that bank credential is processed by that bank including presentation of login/consent/disclosure.
From Orie Steele : Did uri could deference to http server...
From Tom Jones : So there is a solution to payments in process now
From Dmitri Z : @orie - that sounds dodgy :)
From Orie Steele : Why the did controller controls service….
From bengo : Kinda thinking about how everyone will be competing to register openid:// protocol handler
From Dmitri Z : @bengo - yeah, that is definitely one of the problems

From timcappalli : Biggest issue IMO
From Tom Jones : It has been registered already
From David Waite : My flappy bird clone already registered it, so back off everyone
From Dmitri Z : niiiice
From bengo : i mean by client apps, not in any 'registry' ; It's fine if we just have to do it 'because OIDC', but why not also start specifying 'did://' or others?
From Dmitri Z : @bengo - right, so, a 'non-custom-url' scheme solution for SIOP would definitely be the way to go
From Tom Jones : That is also a non-started
From timcappalli : Well, the actual string doesn't really matter ; Its the fact that everyone needs to use the same one ; It could be octopus://
From bengo : We could collaborate on open source code that accepts did://{method} uris, and *that open sourc eapp* can leverage things like uniresolver to provide a jump point ; (redirect_uris)
From Orie Steele : See also: https://github.com/whatwg/html/pull/5482/files
From timcappalli : Even then though, you could have multiple wallets for the same DID method
From bengo : Thank you orie
From Dmitri Z : @orie - oh INTERESTING (re that whatwg PR)
From bengo : Well, resolve the DID, and interrogate what 'further authentication' it prefers
From Debbie Bucci : Are the identities portable in both directions?
From drummondreed : Is that any different than having multiple devices you can accept a Signal message on? Or a iMessage?
From timcappalli : Right but the resolver has no idea which wallets the user has installed
From Dick Hardt : Or if the user has a wallet installed
From bengo : did document could say 'preferredAuthenticatorCapabilities' or something, and have a way of picking the best authentication with those caps (e.g. other wallet apps register with it?)
From Oliver Terbu : We have a lot of discussion in the chat. Please raise hand, so we can discuss it.
From Tom Jones : There is no did until the user releases one
From timcappalli : The only way I see this working is a DID wallet can register with an entitlement at the OS level and the browser can interrogate the wallets. Which obviously has its own issues
From Tom Jones : So first the web site needs to ask ; That doesn't help the RP select one
From Vittorio Bertocci : "on the internet, no one knows you're a dog"
From timcappalli : Well, if the RP can detect you have Microsoft Authenticator, it could craft a custom URI scheme that would launch authenticator
From Tom Jones : The RP cannot detect any authenticator,
From timcappalli : Right, scroll up to my earlier comment about entitlements ; (New functionality by OS vendors) ; Similar to how payment apps on Android can have an entitlement to be an NFC payment provider ; Aka Samsung Pay
From Tom Jones : That was my comment about the password manager - it could do this
From bengo : +1 eventual OS integration, but we can prototype it as a 'blessed app'.
From Dmitri Z : @bengo - have you seen how CHAPI prototypes it, through polyfill?
From timcappalli : There are no other options today ; Since we need interoperability ; @orie ^^
From bengo : @dmitri I have seen it, but I don't always remember it ; refreshing ; i recall liking it
From timcappalli : If you want to invoke a specific wallet, that can happen like any other deep link today ; If you want to invoke "a wallet", that's where the problem is
From Dmitri Z : @timcappalli - agreed. there's some ideas on how to improve that part. (at least on chapi) ; smoother onboarding
From bengo : Couldn't the IDP show a page that's like "Open with openid://" vs "continue redirecting to https://* redirect_uri". Ideally able to detect if openid:// is registered or not (but not by what)?
From bengo : kinda a bummer to redirect to openid:// directly if it's gonna break for my mom

From timcappalli : I don't believe the browser can detect this today
From David Waite : Safari does not support registerProtocolHandler, obviously :-)
From Orie Steele : : /
From timcappalli : @Tom right
From David Waite : Others require it to start with web+xxxx
From bengo : “the platform” or “digital public infrastructure”
From Dmitri Z : yeah agreed (re platform). Like Web Authn does it
From timcappalli : The Android mobile payment implementation is a great example
From David Waite : e.g. it can’t be a standard protocol handler
From bengo : Is there already a ‘blessed app’ for handling openid:// from OpenID Foundation? YOLO or something?
From timcappalli : Default is not the issue though
From Orie Steele : Hearing in chat that it both MUST be and CANNOT be openid://
From timcappalli : 1 wallet is super easy
From Orie Steele : Still confused.
From Dmitri Z : @bengo - lol +1 to a YOLO app.
From bengo : YOU ONLY LEDGER ONCE
From timcappalli : This is like saying I want to open Outlook for one email domain and Mail.app for another email domain.
From timcappalli : ^^ that's what we need to solve
From bengo : I think that’s a feature
From timcappalli : Of course it has to work on desktop OS
From Carly Huitema : I have a flip phone!
From Orie Steele : Obligatory “ don’t you all have phones” out of touch blizzard employee comment
From bengo : Safari also didn’t allow serviceWorker until it did
From timcappalli : Safari ruins everything
From Christopher Hempel - esatus AG : Safari is the ne IE
From timcappalli : ^^ this
From bengo : Apple why don’t you just throw it away and build on Blink!
From Orie Steele : Fore real
From Dick Hardt : Mobile Safari == iOS
From bengo : help us out already! ; (joking)
From Dick Hardt : Safari really is the OS — not a browser
From Tom Jones : So apple uses, runs webkit which does sync with blink
From bengo : +1 to identifying non-nascar problems and opportunities, and organizing around what we’re interested in
From David Waite : +1
From Orie Steele : Can you fingerprint based on registered protocol handlers? ; I guess so
From David Waite : Agreed, don’t want to jump the queue but there’s a lot of value to split out the features that differentiate SIOP from regular OpenID Connect, and to extend OIDC to support other credentials
From Dmitri Z : @Orie - I don’t think you can. (fingerprint) ; I don’t think RPs have the ability to tell
From bengo : Oh look Apple’s not so bad. https://developer.apple.com/ios/universal-links/
From Dmitri Z : @bengo - heheheh you say that now :) it’s a little rough to use (for like React Native)
From bengo : Is that just a ‘bug’ or ‘todo’ for react-native, or technical limitation @dmitri?
From Dmitri Z : @bengo - apple policy / iOS limitation
From bengo : smh
From Dmitri Z : like, the native links are nicer than what came before, but still have their friction/limitations

From David Waite : Universal links are fun, I don't know what happens when you have multiple apps though. Twitter for instance has like a dozen registered for twitter.com
From David Waite : (But most are internal staged builds)
From bengo : I believe you register them by path, not just domain (which is great)
From Dick Hardt : The app claims a universal link — so only that app can use it.
From David Waite : Yep! But they have many registered for each path :-)
From Tom Jones : The only way to get universal links to work is to have a single web site that everyone trusted to redirect the request -
From Dmitri Z : sad but true.
From bengo : It would let me 'delegate' from bengo.co redirect_uri to an iOS-registered app of my choice. OS would see that keys all add up, and just open the bengo app instead of the browser
From Oliver Terbu : I think it is not possible to have multiple apps for the same universal link. On iOS the link will be done based on a file that is hosted on https. The file contains info about the actual app that gets called. Right?
From Dmitri Z : @Oliver - right
From bengo : My knowledge about this is very old, so I am probably wrong about app-per-path
From Dick Hardt : Android has Android Apps that work *almost* the same as Universal Links
From David Waite : It doesn't require a signed file anymore, just JSON at a .well-known location under HTTPS, and app metadata at deployment time saying you want to act on behalf of said domain.
From Dick Hardt : We are looking at using the links for client registration in GNAP
From Richard Astley : I think in iOS it's the last installed app that claims the universal link that can handle it.
From Tom Jones : Same w/ android
From bengo : refreshed on CHAPI. Yes I want this, and I'm happy to just use a PWA of my choice as a redirect_uri for a long time.
From Richard Astley : Android gives the user the choice of which app can handle the deeplink or the user can set their default choice.
From Dick Hardt : Android Apps allow user to override in settings — Android Apps is a newer mechanism for deep link management.
From Dmitri Z : in muggle terms - situation's a mess. :) can't have nice things. (currently.)
From Dick Hardt : https://developer.android.com/training/app-links ; Android App Links is the official name
From Orie Steele : So I am hearing that native apps are dead, and PWAs are the future :)
From Dmitri Z : @orie - yes. IN OUR HEARTS.
From Tobias Looker : https://bit.ly/3jmPmjs
From Adrian Gropper : IIW Savings Time
From Dmitri Z : ^ so true.
From Dick Hardt : LOL
From Kristina Yasuda : The calls info: https://openid.net/wg/connect/
From Dmitri Z : @Kristina - thanks!!
From Kristina Yasuda : BitBucket to file issues: https://bitbucket.org/openid/connect/issues?status=new&status=open
From Kristina Yasuda : requirements: https://bitbucket.org/openid/connect/src/master/SIOP/siop-requirements.md
From Tobias Looker : Link to slides https://docs.google.com/presentation/d/1mNkseYBxOs90whrgDonYyVZj3SqA2QGsn_pp-JpLapY/edit?usp=sharing
From Kristina Yasuda : Oliver's slides: https://docs.google.com/presentation/d/1K9jlC17uDC-JYiomcJI8cbZX8pXJwJZcr5Y8M_9c1T0/edit?usp=sharing
From Kristina Yasuda : we did have a proposal to talk to WebID WG as well

From Dmitri Z : oh excellent. (re webid wg)
From Tom Jones : So - I guess what the next step is - we create a proposal to the w3c WICG and see that they say ; I guess I could start one if no one else is used to that process?
From Adrian Gropper : Kim just answered my first question!!
From Tom Jones : Paw just makes the nascar problem worse ; pwa
From Orie Steele : Here is a demo PWA wallet: ; https://wallet.interop.transmute.world/
From Tom Jones : Yeah - Kim developed one too
From Orie Steele : Lets get the link in the notes :)
From Kristina Yasuda : PWAs could actually surpass NASCAR problem.. - it's already a url that does not need custom schema indirection?
From Tom Jones : No - because each pwa has its own URL ; So it only works if everyone uses Kims wallet
From bengo : CHAPI allows ANY PWA to register, not just Kim's
From Orie Steele : Yep, I have similar code here: https://chapi-siop.did.ai/ ; Tries to blend the OIDC redirect with CHAPI ; But its pretty hacky…
From Tom Jones : Any one can register at any time - the user wold probably not understand the conflict
From bengo : I am the user.
From Dmitri Z : @orie - I was just looking at that demo. what's the OIDC part?
From Orie Steele : @Dmitri it converts chapi responses to redirect URIs
From Tom Jones : Sorry - the user is my father
From Dmitri Z : @orie - oh fascinating
From Tobias Looker : Yeap uses CHAPI for the NASCAR problem but still interacts with the provider via redirect ; An OpenID redirect ; E.g a SIOP request
From David Waite : Well keep in mind, CHAPI only solves the problem if there is a single CHAPI polypill :D ; The CHAPI polyfill works by tunneling all the requests through a single web domain
From Kristina Yasuda : @Orie, your links are in the notes
From Orie Steele : Cool, I'm a big fan of PWAs… you can even do webNFC with them :) ; And web bluetooth
From Oliver Terbu : This work is not only about solving the NASCAR problem as pointed out earlier.
From Tobias Looker : Not on MacOS though :)
From Kristina Yasuda : good point, Oliver
From Tobias Looker : @Orie
From Tom Jones : If there is only one redirector it can work, just let me control that redirector
From Orie Steele : It works on macOS, just not safari
From Adrian Gropper : Can PWA work with hosted Intel SGX?
From Tobias Looker : Yeah sorry meant Safari
From Orie Steele : Yes, you can connect it
From Tom Jones : Paw works in browsers ONLY ; Its just a bunch of javascript
From Kristina Yasuda : paw works on mobile and web browsers
From Orie Steele : Sadly web authn does not provide general purpose hardware signing interface.
From Kristina Yasuda : link to this doc: https://drive.google.com/file/d/1LZHgcyaEm1CgtKucN0Gib4BvQ4m-_Cho/view?usp=sharing
From Tom Jones : Web author level two is in process - let me check that out
From Orie Steele : window.crypto.subtle can support non extractable keys ; And they can be used by PWAs ; From Orie Steele : But they are limited to old NIST crypto sadly
From Tom Jones : The spec on hardware protection is unclear - need to verify what android & apple actually do with that

Guardianship, SSI and the Sovrin Working Group

Wednesday 14C
Convener: John Phillips

Tags for the session - technology discussed/ideas considered:
Guardianship, Trust over IP, SSI, the importance of Jurisdiction

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

John presented slides to provide a background to the discussion. [will be posted in this document too]

Slides accessible here:
https://docs.google.com/presentation/d/1v4rb9dWuzVhAWhyXx2DfQknzb4U4RNJigbyPZoInR2E/edit?usp=sharing

Discussion centred around topics of the importance of the verifier in giving meaning / agency to the Guardianship role

The potential risks of creating backdoor takeover capability if guardianship is done wrong
The need to consider the human/legal/social context of Guardianship across different societies, not just one model.

Slides Presented: [all under a Creative Commons share alike and attribution licence]


Guardianship is an essential capability for any functional, humanity centred, digital ecosystem


Guardianship is particularly interesting in an SSI digital ecosystem
There is a natural tension between independence (self-sovereignty) and dependence (guardianship)


How the Sovrin Guardianship Working Group got started
2016
Sovrin Foundation Formed
2017
Sovrin Provision Trust Framework v1 proposes guardianship principles (§2.2)
2018
2019
Sovrin Guardianship Task Force established
Sovrin Guardianship Whitepaper Published Nov '19
2020
Sovrin Guardianship Working Group established, 4 co-chairs, two regions
2021

Principles of the Working Group

All Sovrin Governing Bodies operate under the Core Principles in section 2 of the Sovrin Governance Framework V2

This governing body operates under the following additional principles:

1. **Holistic view of Guardianship.** Guardianship shall be developed within the context of the overall Trust over IP stack and will consider the technology and governance stack and also offline business operating models and processes.
2. **Global geographical coverage.** The Sovrin Guardianship Working Group shall organise itself to include the widest possible coverage.
3. **Promote a variety of application domains and implementations.** The Sovrin Guardianship Working Group shall be agnostic with regard to implementers and may treat Guardianship in any domain compatible with Sovrin's governance principles.

The 2020 journey so far…

Defining the Technical Requirements for Guardianship in an SSI / ToIP context

Learning how to think about Guardianship

Spreadsheets and false starts

Grand Designs and Tables of Contents

Extracting Requirements

Mental Models and Building blocks

Decoding Use Case Transcripts

Discovering Patterns - only 7 plots

Realising Definition(s)

At first we thought this should be simple

We believed that there could be a simple set of generic SSI Guardianship building blocks that could support unique instances of Guardianship.

We didn't want to "solve" the challenge of real-world Guardianship on a global scale, but provide "lego bricks" that naturally combine in ways that encourage and support good design.

we realised we needed to revisit our thinking

We needed a conceptual bridge, a way of understanding Guardianship broadly so we could write appropriate technical requirements.

We needed a mental model.

We started work on identifying and discussing building blocks and mental models based on earlier work from Sovrin and TNO [see IIW #30].

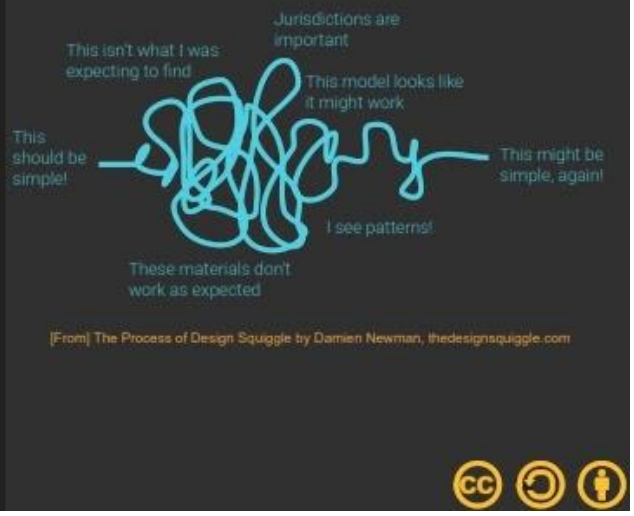
But the gap between Use Cases and requirements was too broad

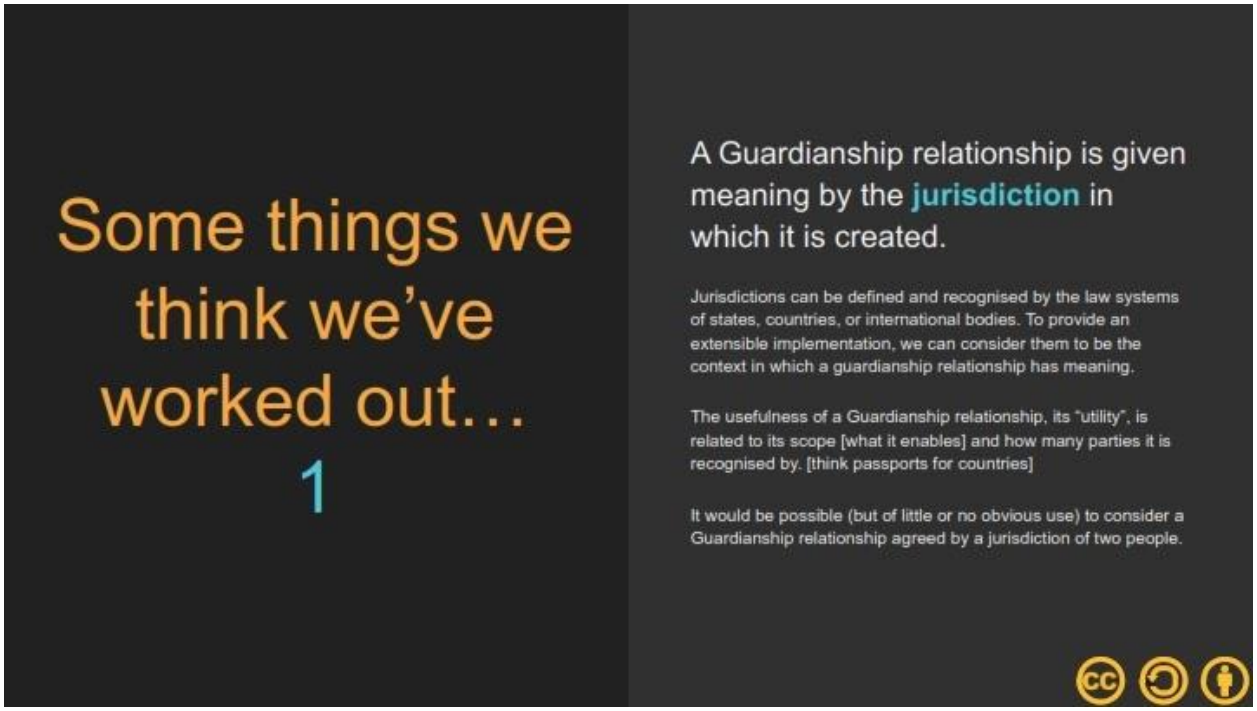
Use Cases are necessarily written in a situation specific way, often with solution elements embedded in the narrative.

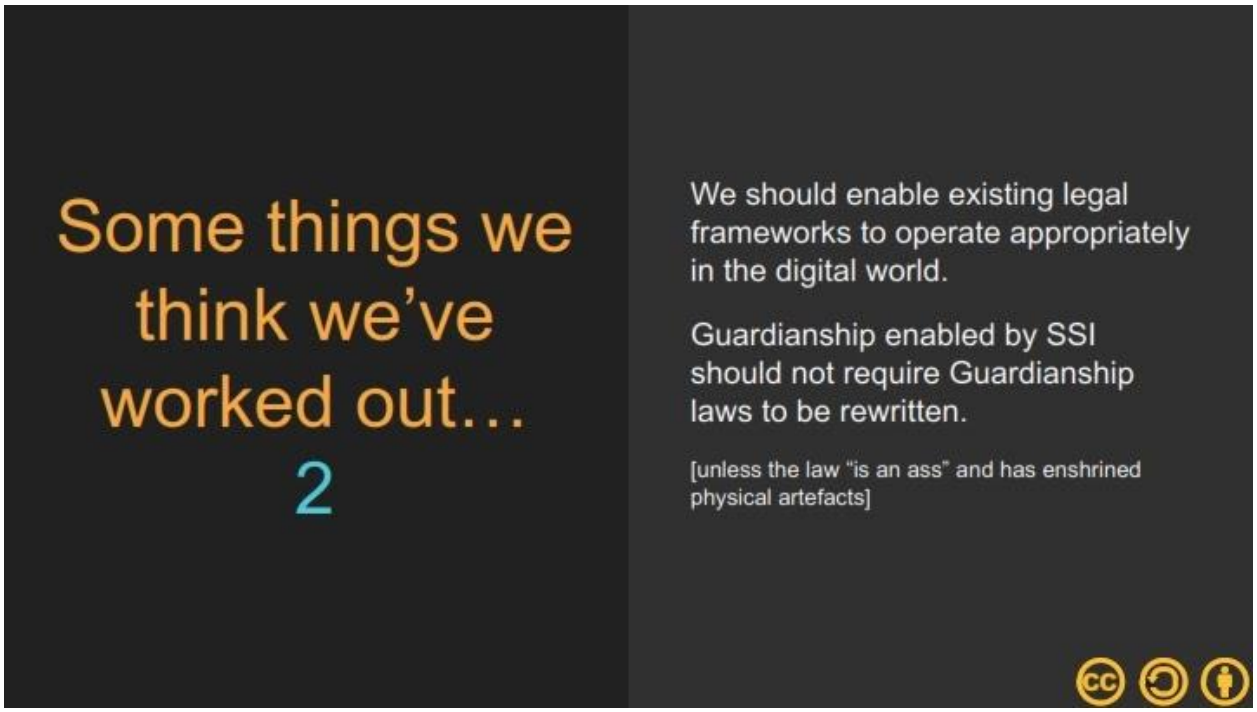
Extracting requirements directly from Use Cases meant filling in gaps, making assumptions, and removing details.

the journey hasn't been a straight line path

In fact, we rediscovered a familiar squiggle




Some things we think we've worked out…
1
A Guardianship relationship is given meaning by the jurisdiction in which it is created.
Jurisdictions can be defined and recognised by the law systems of states, countries, or international bodies. To provide an extensible implementation, we can consider them to be the context in which a guardianship relationship has meaning.
The usefulness of a Guardianship relationship, its "utility", is related to its scope [what it enables] and how many parties it is recognised by. [think passports for countries]
It would be possible (but of little or no obvious use) to consider a Guardianship relationship agreed by a jurisdiction of two people.


Some things we think we've worked out…
2
We should enable existing legal frameworks to operate appropriately in the digital world.
Guardianship enabled by SSI should not require Guardianship laws to be rewritten.
[unless the law "is an ass" and has enshrined physical artefacts]

Some things we think we've worked out… 3

We need a Guardianship Verifiable Credential that appropriately defines the relationship:

- Identifies the Issuer
- Identifies [and is issued to] the Guardian
- Identifies the Dependent
- References the issuing process
- References the Jurisdiction
- Defines the type of the relationship
- Defines the scope of the relationship
- Defines the start date
- [May] define the end date or condition

Think power of medical attorney, power of financial attorney, executor of estate...

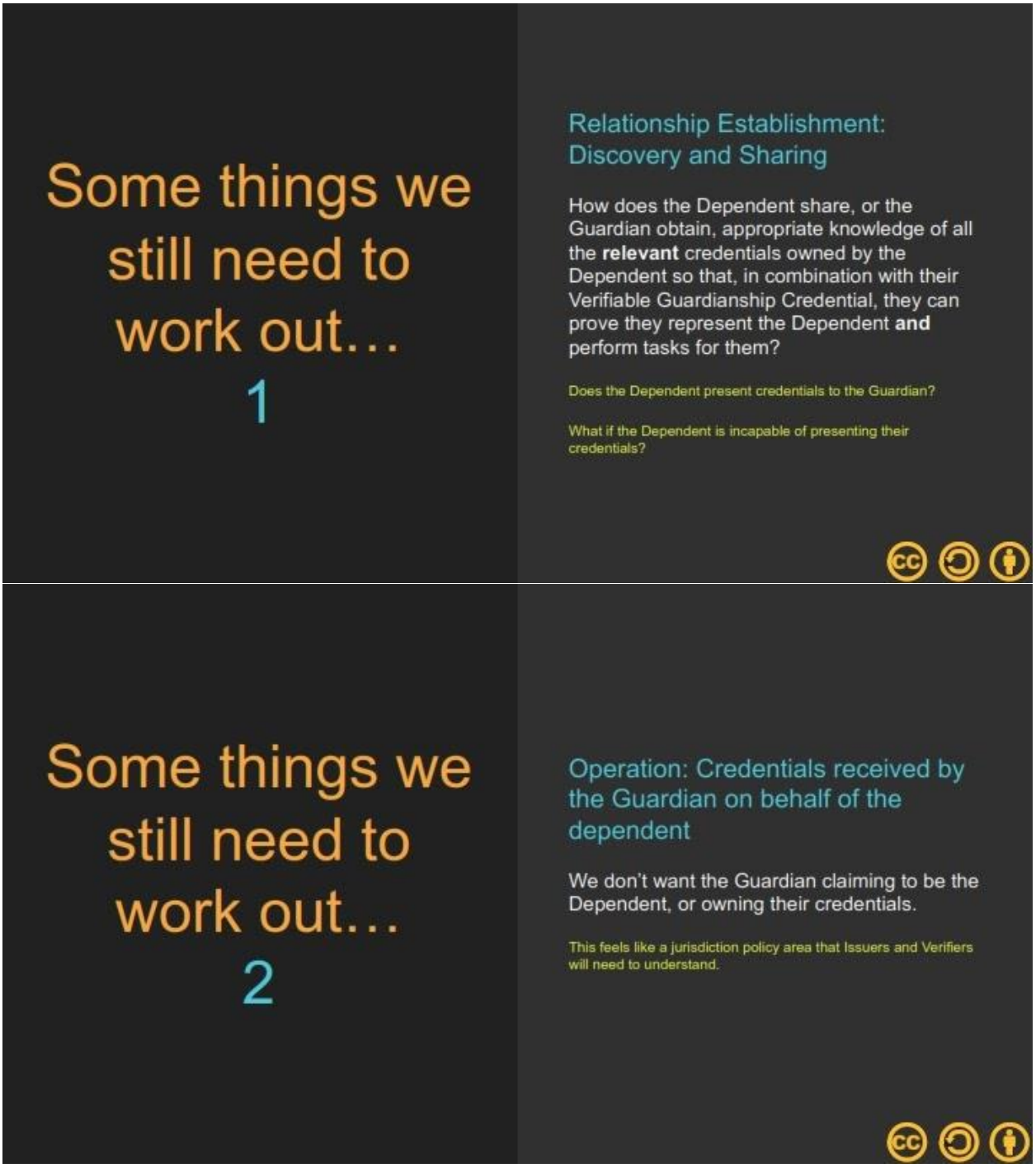
Some things we think we've worked out… 4

We don't want to prescribe solutions where the Guardian "takes control" of the Dependent's wallet and/or needs to use the Dependent's private keys.

Why?

Risk and Privacy issues:

- Weakens wallet security
- Heightens impersonation risks
- Erodes privacy


Some things we still need to work out…
1
Relationship Establishment: Discovery and Sharing
How does the Dependent share, or the Guardian obtain, appropriate knowledge of all the relevant credentials owned by the Dependent so that, in combination with their Verifiable Guardianship Credential, they can prove they represent the Dependent and perform tasks for them?
Does the Dependent present credentials to the Guardian?
What if the Dependent is incapable of presenting their credentials?
Some things we still need to work out…
2
Operation: Credentials received by the Guardian on behalf of the dependent
We don't want the Guardian claiming to be the Dependent, or owning their credentials.
This feels like a jurisdiction policy area that Issuers and Verifiers will need to understand.

Some things we still need to work out… 3

Operation: Guardian's role needs to be recognised by Receiving Parties

To provide effective Guardianship, the role for the Guardian must be recognised by the Receiving Parties that they need to interact with to perform their duties for the Dependent.

This is as much a socio-political and legal system as it is a technical system.

Some things we still need to work out… 4

Operation: How do we maximise agency and dignity, and yet provide appropriate care to the Dependent?

In the mature SSI world, where Independent people manage their own wallet, to the extent possible, we would prefer them to keep their wallet and its contents if they become dependent on another person or organisation.

BUT how do we appropriately (ethically) stop Dependents from using credentials in their own wallet if they shouldn't them? Do we revoke their credentials? Which ones? Do we need ways to revoke wallets? That sounds draconian, what if the keys get in the wrong hands…

Perhaps we just look at life as it is - make sure our digital approach is as good if not better than the real world. Don't cause damage by seeking perfection.

Some things we still need to work out…

5

Closure: Establishing and Recovering Independence

How does the Dependent, who recovers or gains independence, recover their credentials?

Two examples (there are many)

1. A child becomes an adult: how do they get their academic, health and birth certificates?
2. An adult recovers their independence: how do they get the history of transactions made by their Guardian while they were dependent?

Should we issue new credentials to newly independent person? How do know we what to issue? How do they know what they should have?

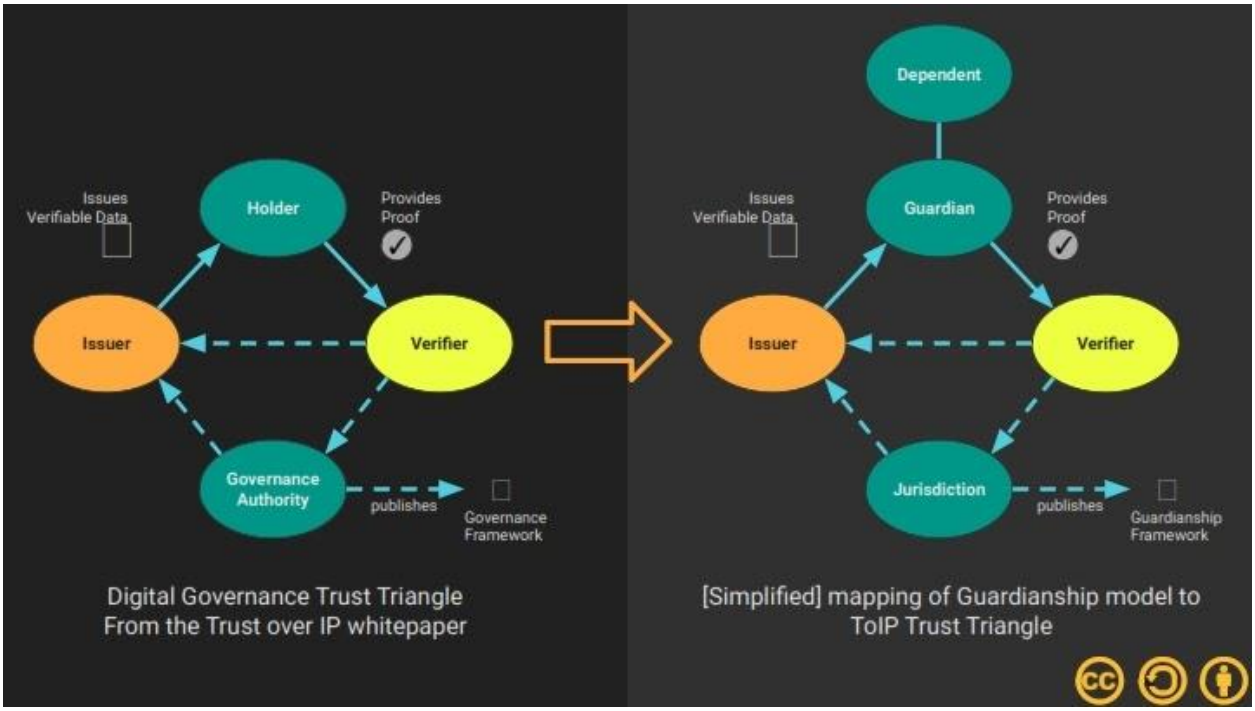
Do we always revoke the Guardianship credential, or can it expire?

[now] our work has an obvious relationship with Trust over IP

The working group was chartered to align its work with the Trust over IP framework.

By “re”discovering the importance of a jurisdiction and its place in Guardianship, we have a system that aligns with Trust over IP.

In this sense and context Jurisdiction defines our Governance Stack



Fusion: Leveraging Federated Identity to Scale Verified Credentials

Wednesday 14D
Convener: Ken Klingenstein
Notes-taker(s): Judith Bush

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

We want to leverage not just federated credentials but federated trust to take advantage to verified credentials. If i am issuing an academic badge or certification: institution is issuing an assertion - you are a faculty member - and a domain of expertise. Can a student deposit a DID in an enterprise directory. When i as an institution want to mint a credential for a student, i as a human am authorized by the institution to issue that credential. As institutions we have built levels of assurance in what we do.

Global ID -- will verify an existing physical credential, could be issued by another organization and user.

GlobaliD is receiving attestations / credentials from external party and then issuing the, GlobaliD verifies they are a company … GlobaliD tries to bring in companies that meet the needs of different levels of assurance. The SSI element is a value to reduce PII. GlobaliD creates a bridge between verifiers and institutions that need the credentials checked. The consuming institution integrates with GlobalId, Globalid tries to work with the consuming institution to minimize the data from credentials that are not needed.

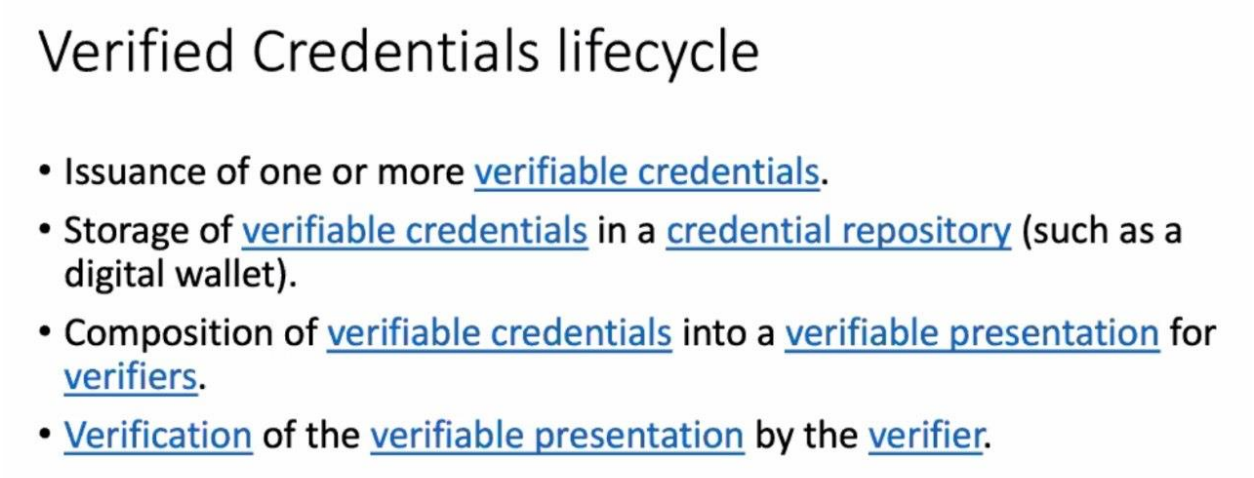
The credentials are issued by specific agencies, some credentials can be obtained from different agencies, create a schema, all agencies express the values in the schema, GlobaId can mediate….

Globalid has defined schema for things like Drivers License with some values optional -- because some DL don't have expiration dates, for example. Then the agency will not report an expiry on Singapore - -trust the agency to have validated the DL even though there's an absent expiry. Also encourage the consuming institution to simply accept that they could get access through the agency if needed but not require the access to all the data -- simply confirmation that the agency has the data .

European SSI laboratory eIDAS -- eIDAS was launched as the trans European cross border goverment ID -- verifiable credentials confirm the credential comes from assured place . "Seal of approval"

USE CASES

IMS Global -- syntax of badge



Verifying the issuing authority -- some challenges here. The organizational structure needs to decide if a particular individual can issue the credential.

Is the software for minting the credential assured?

A group of hospitals is trusted, an individual from the organization , issued the role, …

Do you trust the issuer and is the schema something you expect if you are automating this.

Global Legal Identifier Foundation -- that organization provides an id to act as a root of trust. Can give them a list of users who can issue. GLEIF … https://www.gleif.org/en/
https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei

REVOCATION
Is revocation an issue? It has come up with GlobaliD. However the relevance has gone away. “I no longer want to carry this credential.” “This has expired, no longer valid”

Is the credential still valid? (Individual not on watch list, eg) checked every day. Need to revoke the credential if the user shows up on the list. However, the organizations want to know if it’s checked -- instead Ongoing Verification.

Negative verified credentials? User will always provide access to the fact that a credential had been given to them. Is the absence of a specific credential a negative fact. Need the absence to not be a negative….

At Human Colossus : Whenever data is ported it’s linked to a credential with the consent and a life time, after which point at the data is invalidated.

Licenses need to support revocation?

80% credentials don't need revocation.

Credential over 21 based on a license that has been revoked.

Duration of the credential - boarding pass, ticket to event -- no need to revoke because the lifetime is so short.

Termination of an employee.

WALLET INTEGRITY

Need to go to the trusted digital assistant. Wallets not interoperable beyond Indy Hyperledger. Something other than the wallet. The question of credentials tied to different wallets, then the need to prove something with credentials from different wallets -- how?

Does KERI (or HOLOCHAIN) that don't need global consensus solve the problem? Suspicion no that there can't be one local universal resolver . 60+ (70+?) DID methods. Different wallet for different purposes. Wallet hidden in the hospital's app, the bank's app. Very correllated, not trust over IP.

Multilateral federation SSO is dead -- but R&E federations really about moving attributes with trust

How does an orthodox community that needs a shared consensus solution approach a collection of lone wolves who are innovating their own special sauce to distinguish themselves as a vendor?

Verified credentials need to be interoperable -- how to we span the diversity? Demand will impact the many different silos to make interoperable worth pursing.

Hoping KERI will align and solve the issue of the variety of DIDs. DIDs not required for verified credentials, verified credentials depend on URIs. Structure of DIDs particularly useful in linked data to pull issuer and make a pointer…. Just using a URI to point to a certificate may be easier for an institution.

Big pharma has a huge volume, make their own standard. Yet another identifier framework.

Interop between SSI stacks - A proposed handshake protocol

Wednesday 14E
Convener: Christoph Eckl (Condatis), Richard Astley (Condatis)

Tags for the session - technology discussed/ideas considered:
Interop, aries, siop, qr-code

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

Slides presented:
https://www.slideshare.net/secret/xom5XYxnMLVpJW

Jace Hensley
Uday Garud
Dave Crocker
Ian Costanzo
Daniel Hardman
By_Caballero
Kalyan Kulkarni
Ken Ebert
Lynn Bendixsen
Rory Martin
Salvatore D'Agostino
Sam Curren
Taner Dursun

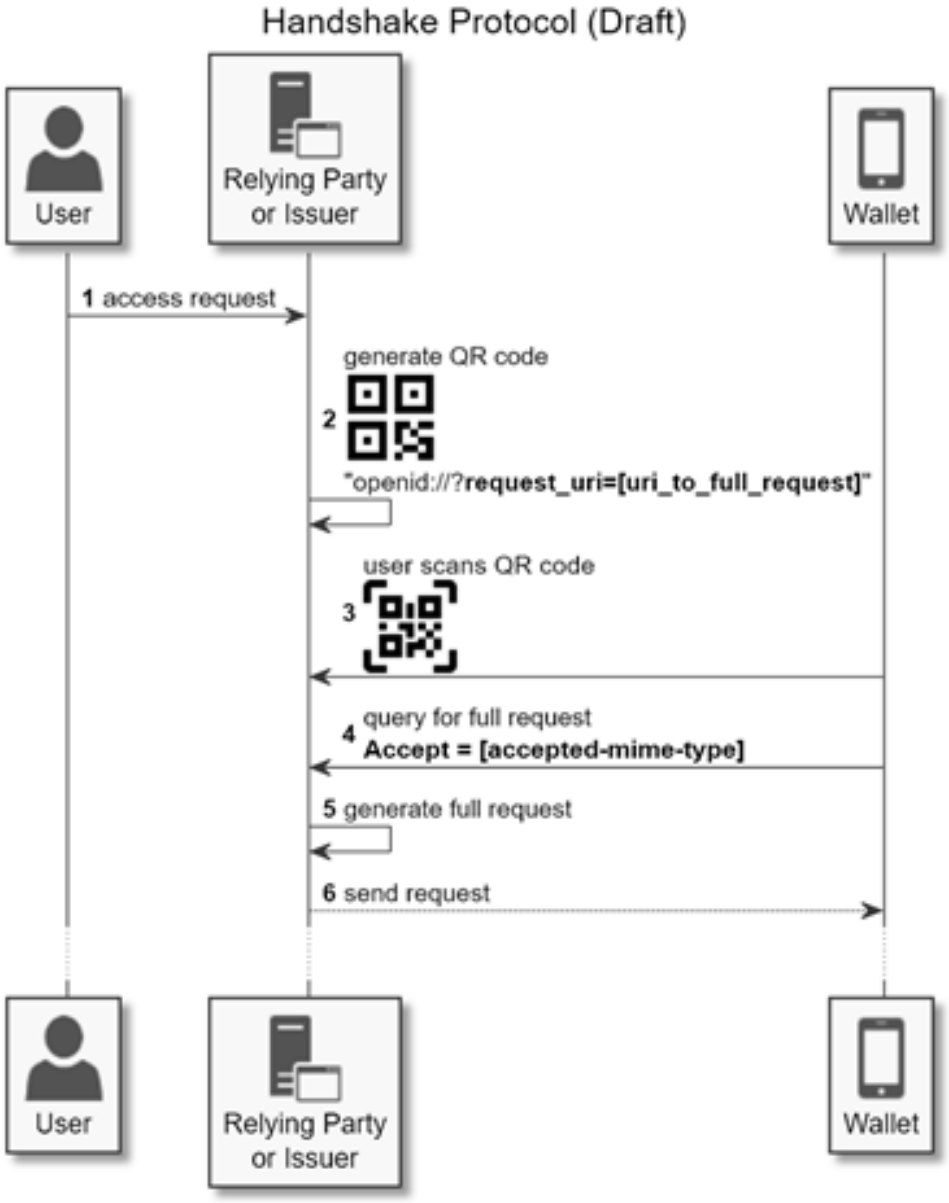
Chris outlined a UK project that given the public procurement nature is insisting on efforts in interoperability. In particular the project is currently built on Hyperledger Aries using Evernyms Verity and Connect.me but is also looking at MS Authenticator and SIOP.

A proposed solution to a QR code that can at least inform the RP or the Issuer of the wallet stack of the user was proposed that does not put the full initial communication request into the QR code payload but relies on a callback URI within the payload.

It was shown that MS already do this as part of their openid:// uri.
Evernym also support a callback URI in their connect.me app.

The proposal was for any wallet provider to add an accept header based on https://tools.ietf.org/html/rfc7231#section-5.3.2 to the callback to the RP/issuer.

This enables the issuer to distinguish between wallets and therefore SSI stacks:



Condatis as part of their UK project already negotiated with Microsoft and Evernym the following content types:

Provider	Wallet	Protocol	Accept Content-type
Evernym	Connect.me App	Aries	application/json
Microsoft	Authenticator	SIOP	application/jwt

Discussion:
RFC document proposal
Discuss in the community
Propose for Aries Interop Profile

Sample implementation helps get adoption
Better to implement in AriesGo or similar to gain more traction

Join community call to circulate proposal

Where should it be socialised outside of Aries

Other discussions include adding full VC in QR
Animated QR code to fit more data in

UX user expected to know the QR code should be scanned with any QR code scanner.

Accept Content-type not enough to identify intended stack, options to add subtypes: e.g. application/json+... (see current mime types: http://www.iana.org/assignments/media-types/media-types.xhtml)

Next steps:

- Chris and Richard will propose an Aries RFC and will ask Daniel Hardman for review and advise in engaging the wider community.

Amateur Radio and Identity

Wednesday 14G
Convener: Aaron Parecki

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

Constraints/properties:

- Anything you send on the radio can be heard by anyone nearby
- Messages can't be obfuscated or encrypted
- Constrained payload sizes of messages
- No confirmation of messages received, nobody knows if you're listening

Barriers to entry in the community:

- You need a special radio to send and receive messages

Identity is based on call sign, globally registered identifiers managed by local governments.

Communication on amateur radio is always identified by call sign, but there is no authentication of that message, it's entirely the honor system. It is also mostly not a problem because of the barriers to entry and lack of incentive to cause trouble.

Encryption isn't allowed, but signatures aren't obfuscating a message so it would be okay to use cryptographic signatures when sending a message.

Pack your message into a string, sign it with some private key, then transmit the message and the signature. If the recipient knows your public key, they could verify the message.

https://w7apk.com/radio-authentication

Digital vs Analog? Could be done with voice but will need to be manually verified. Digital modes provide the opportunity for computers to verify signatures.

Why is this important? Use cases:

- Remote control of devices already allows encryption
- Wanting to know you are really talking to the person with this call sign
- Confirming someone's identity before a trade

LoRa - license-free radio on a few narrow bands for long range wireless signals

- https://revspace.nl/DecodingLora
- https://theholo.space/

The Sovrin Technical Ecosystem

Wednesday 14H
Convener: Stephen Curran, Sovrin Foundation

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

Presentation Link
Review the components of the technology underlying Sovrin -- past, present and future.

Is Identity Only for Transactions?

Wednesday 14I
Convener: Lisa LaVasseur & Chris Buchanan
Notes-taker(s): Chris Buchanan

Tags for the session - technology discussed/ideas considered:
Identity - Definition / Governance - Meaning

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

Heyo everyone left their twitters and keybases at the last minute, mine are @ by_caballero

#START_CHAT
all of the data points that allow you to id a unique human in space.
Identity for Ownership?
would my relationship diagram with transactions be helpful?
From my worldview identity is fundamentally based on a relationship - and a transaction is simply a form of a relationship
If you can only ever experience a pseudonym or a persona is it effectively “your identity” in that context or interaction?
Late binding is cool
"Let's not confuse identity with truth.."
"...and that's how life works."
...ya...
Wip, I’m interested in what caused this particular diagram
@Jeff Doctor: Is there a form of relationship that doesn’t involve a transaction?
This is my diagram for interaction I put together a while ago for a paper but its not digital really
I like the ambient environment’s influence arrows
@Kaliya : The identity you need in the Jane Doe example is the one the claim is being made against.
The Echo Maker: https://www.amazon.com/Echo-Maker-Novel-Richard-Powers-ebook/dp/B000QCTMQ0/ref=sr_1_2?dchild=1&keywords=capgras+syndrome+crane&qid=1603320719&sr=8-2
Can define identity as a series of channel integrity measurements. BOLTS channels and their sub channel
Question of duties. Those are described in contracts. Guarantees, etc.
Duties can be delegated (or not). Rights can be assigned (or not). HIPAA requires that statutory responsible parties make sure, by contract that their service providers are reseponsible for data breaches, etc.
yes, there's "gossiping" and "taking"
That's exactly the Me2BA proposition: our current me2B relationships are dysfunctional and abusive.
it’s interesting because abusers typically cannot remember the details of the abuse.. in fact they often forget it entirely.. but the abused remembers.. it’s an asymmetric emotional reaction to what has happened
i never thought about this before but in digital, abuse is remembered in the data and servers but the abused typically hasn’t been able to get at the data and metadata
from dooty to duty (sorry)
completely agree with Asimov rules...
for products there is a kind of anthropomorphism. and I think that's kind of what we do in general. It's also theory of mind.

https://bookshop.org/books/the-immune-self-theory-or-metaphor/9780521461887
^^ @Scott David, is this the book you mentioned?
Yeah, it's a privilege to not think about identity
Yep that the book.
Web of relationships.
Identity is a word that has several pages of definitions in the OED
The concept of identity can be fruitfully disambiguated
Interactions produce information which has value. Transactions suggests value in the form of transferrable monetization.
Group identity based on responsibilities. Are those normative based on prior interactions?
there's something coming up here regarding: parts of our identity that are necessarily public whether or not we want them to be.
Or at least necessarily “shared”
yes for me "transaction" is sharing
it is meaningful under Western frameworks of law
The isolation of the individual and neoliberal economics (colonialism, imperialism, European philosophies, etc.) are very strongly correlated. In fact, it is causative. We produce individuals for the commercial machine. Opinions differ on whether that is a good idea!
^+1
mileage may vary
I think interaction may be better than transaction
incommensurable
Wholly non-interoperable
Rhetoric is the epoxy that glues together incommensurables. Shamans used rhetoric in stories/folkways. They are meaning engines. Our rhetoric is offered by large commercial and political power structures without qualia. They are intrinsically unsatisfying as a reals for humans.
We need new “patterns” to create new rights/duties zones in those new interaction spaces
+1 to Kaliya.
Interaction makes more sense than transaction to me
They are imperialist, colonialist frameworks.
Patterns of laws are merely narrative within a meaning domain.
(I think Scott made the suggestion yesterday--i.e. interaction)
Market-speak (in Girardidadas)
win-wins, private/public partnership, that kind of thing :D
Sovereigns are belief systems. Period.
It is considered to be impossible to have multiple sovereigns, but in fact we have that all the time for different groups of interactions.
Worship your gods, know your icons.
Inherent duties emerging from my asserted identity
if you have a second passport, keep it quiet
also inherent duties emerging from my perceived identity???
identity actually is a risk for transactions, identifiers are for transactions, maybe..
Sky woman would disagree :)
it is missing from much of self-sovereign identity, it is borne of self-sovereign governance (/responsibility...)
words are only fingers pointing at the moon.
not the moon.
relational and interpersonal?
interdependence
^the name of a great podcast!

about overcoming individualism in the creative economy, fun fact
https://interdependence.fm/
(seeing a lot of podcasting mics in this room :D)
Settler colonialism/capitalism requires alienated peoples - alienated from themselves, from each other, from the land, and from all life in general
interdependence also relates to the buddhist notion of no-self
"digital representations of ourselves"
Atomized is a really good way to put it
^a traditional materialist/Marxist way :D
“How do I apply this” - https://www.gida-global.org/care - these principles are a start, for Indigenous data at least
Identify engineering requirements for technical systems that entrain human behaviors that perform duties that give rise to the desired rights.
For me, I start with modeling (describing) the human behavior
@Jeff thanks for that link.
That is the guild idea
If there were a code of ethics it could apply across specific engagements and assignments
we talk a lot about governance, and I'd really like to get that unpacked at some point. because I think it mainly is focusing on governance of technology vendors/makers.
sounds like a trade union to me :D
usually more specific with an adjective in front of it to narrow it down
Governance means rulemaking, enforcement and operation under the rules.
data governance, codebase governance, organizational governance
my fault for using it unqualified :D
Rules are made 5 stages: Agenda setting, Problem identification, Decision, implementation and review.
When we talk about governance we are talking about USING technology to allow the “users” to Govern themselves:)
it's kind of like ethics-- a very broad field, particularly for people who do it for a living :D
Governance: ethical rules of behavior
They are enforcing rules so it is an aspect of governance.
Lots of resources on Indigenous data governance here - https://indigenousdatalab.org/webinars/
rules + enforcement
Governance: setting rules for rewards and punishment
rules + consequences
The individual must be at the table in the creation of the rules. RUlemaking is the most existential
Inclusive stakeholding
aligned incentives
not easy!
bad governance is worse than none at all :D
+1 Juan
Governance can be broad or narrow.
Juan.. yes.. but.. if abusers are doing bad things.. it can be bad.
Governance can be formal or informal
Sound like “government”
government tends to be very formal
(fwiw, the me2ba has Rules of Engagement that form the ethical base of how we believe technology should behave: https://me2ba.org/principles/ they're based on attributes of healthy human relationships)
living in an anarchist squat, on the other hand, is all governance, no government :D

https://www.haudenosauneeconfederacy.com/government/ - a lot to be learned from Haudenosaunee governance
Informal governance? Examples?
(I'm obviously biased :))
Governance == rules + enforcement/consequences + how to refine the rules
A lot I imagine
@JeffD thanks so much for sharing that--I wasn't even close in my spelling of haudenosaunee
Governance = Government - Justice?
classic examples of informal governance is word of mouth/gossip as enforcement, anarchist self-organization, cash-only economics, etc
Stories are persistent, and may be good or bad or both.
anarchists like to insist they have their own justice :D
but it's begging the question: formal/informal justice :D
Story telling is a "dual use" technology. They are persuasive speech
Canada is a story, a legal fiction in my view :)
Governance = the plan for the success of a group
^ love it
+1 to Jeff. Nation states are stories, violently enforced
definitely a good definition of good governance, if the group defines success :D
According to whom?
@Chris not sure which comment you're asking about. one of mine?
yes, America is a story. my identity is also a story
my identity is many stories
+1 to Mary. Dynamic stories for human "neighborhood watch"
The plan for success of the group — who defines success?
consent and coercion-- getting into Gramsci territory
who gets to set the narrative and how they convince people
People in the group? @Chris
Yes the group decides
(kind of begs the question a little-- cuz how you group speaks at one is... governance :D)
So democratic process is the only valid process?
as* one
just a few?
This is the time for humans to regroup with other living forms and de-hubrify our stories
I think it's good to remember that we don't actually have a democratic system in the united states
quaker tradition as well :D
also big on concensus
although the cynic might say that can also border on gramsci territory. (not me, I love the quakers and the daoists and the Buddhists)
deliberative processes = informal process that can really powerfully correct/complement formal ones
This conversation makes my heart so happy.
but who is doing the "informing" in these cases?
as Shoshanna Zuboff says: "who decides, who decides, who decides"
#1492LandBackLane (look it up on social media) is good example of Haudenosaunee participatory democracy in action, and it's criminalized
cjb@mitre.org
Diversity processes also signals gaps. The bigger the gaps the bigger the benefits of closing them. It is like a heat engine - maximum efficiency from maximum differentials (of temperature). In society they are "entropy" gradients that can be harnessed for social/ciultural engines

full consensus is really interesting.. i like the idea of 36 people.. like a jury.. or something. i'm sure there are many other models we should consider and think about the pros and cons
Beautiful discussion. Thanks to everyone
really great.. thanks Lisa and Chris
Thanks Chris for bringing us together
And Lisa!
Chris and Lisa . Good stuff.
Thanks.
Jeff - where can we learn more?
the good news is that western hegemony has fairly brittle governance
Pluggin my own work :) https://niiwin.ca/
:F
Data decolonization — google it.
Articles at the bottom
The chat will go in the notes so put your URLs in.
build a new table
https://hpec.io/
@Chris , are you going to save out the chat log?
Yes.
It will be in the meeting notes.
Thank you!
IP
world epicenter of IP so valuable it needs no permanent employees
Read lots of Black feminism :)
Futarchy https://en.wikipedia.org/wiki/Futarchy
Holarchy https://en.wikipedia.org/wiki/Holarchy
options
Lots of foundational Indigenous data sovereignty resources here: https://www.gida-global.org/resources
https://1.qiqochat.com/breakout/30/iiw31
^is this where we stick notes and urls?
our Rules of Engagement are universal
session 14?
one cool trick is to cut and paste all the chat into an editor and remove everything that's not a URL
I use my twitter account as an amplifier and reading list of sorts too: https://twitter.com/jeffadoctor
particularly good for sessions where people might be speaking about things their employers and/or sovereigns might not like
Thanks all, nya:weh!

#END_CHAT

Data Seder: A Dinner Ritual For Our Generations

Wednesday 14J
Convener: Phil Wolff (@evanwolf)

Tags for the session - technology discussed/ideas considered:
Storytelling, seder, privacy, culture, rites, rituals,

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

- What elements belong in a Data Seder? | by Phil Wolff | Digital Justice

- 2020 Data Seder - working document and haggadah parts
    - https://docs.google.com/document/d/1aPND6pzrMPkQCdEET7MQdNxI04mHHG3CWE7e0I2hMC0/edit?usp=sharing

Closing Sessions 10 - 14 / Open Gifting / Opening

Notes Day 3 Thursday April 30 / Sessions 16 - 24

Overlays Capture Architecture (OCA): Global Semantic Harmonization (Repeat Session for EU/APAC Attendees)

Thursday 16A
Convener: Paul Knowles @pknowles

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

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.

A database model shows the logical structure of a database, including the relationships and constraints that determine how data can be stored and accessed. Common kinds of data models include Hierarchical database model, Relational model, Network model, Object-oriented database model, Entity-relationship model, Document object model, Entity-attribute-value model, Star schema and Object-relational database model. The data semantics across these common database models can be harmonized using OCA.

Everything is documented in the slide deck which is available here.

Related blog post: https://humancolossus.foundation/blog/cjzegoi58xgpfzwxyrqlroy48dihwz

Brief Intro to ACA-Pico (starting at 6:00am PST)

Thursday 18L
Convener: Bruce Conrad
Notes-taker(s): the convener

Tags for the session - technology discussed/ideas considered:
Picos, Aries agents, Manifold, ACA-Pico

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

Those in attendance are invited to follow these steps to make their own Aries Cloud Agent using ACA-Pico.

1. Sign in to manifold.picolabs.io
2. Click on "+ Add Thing" (near upper-right corner)
3. Provide a name for your new thing, then click "Create Thing"
4. Notice a card representing your new thing (can be moved around)
5. Click on the gear (near upper-right corner of the card)

6. In the popup menu, click on “Install an App”
7. Select the ruleset named “io.picolabs.manifold_cloud_agent” then click “Install it”
8. Notice the app is represented by the Aries logo at the bottom of the card
9. Click on the Aries logo/button
10. Click on “Enable Connections”
11. Notice that an “Action” button appears
12. But first, click on “Open Card” (a doorway icon near the gear) to have more room
13. Connect with other people in the session by sharing invitations out of band

The above was the plan, and Will and I ended up working together in this session, which extended well into Session 19 territory time-wise. We did a deep dive into the ACA-Pico code.

A follow up session will occur with him and one of his students Monday at the same time.

7 Essential Life Credentials for Identity for All

Thursday 19A
Convener: Nicky Hickman - Sovrin
Notes-taker(s): Sankarshan

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

- Introductions from the participants
  - [please see recording for the detail]
- “Delivering Identity for All”
  - Having a more focused approach to address some of the missing bits
  - The conversation is aimed to start understanding what the next step is on the delivery
- Why does Identity for All matter?
  - **Inclusion** + **trust** = **resilience** and **prosperity** for all
  - Significant progress made in the Sovrin foundation - driven by the use of inclusive design techniques. The Governance Framework includes Inclusive By Design as one of the 5 design practices. The whitepaper on IoT includes personas which are edge cases which are deliberately chosen to underscore this approach
  - DLT Identification Systems in the humanitarian sector and Guardianship whitepaper
  - The core components of delivery are present
    - Reference frame of the ToIP stack and work underway for the Sovrin Governance Authority = Sovrin Ecosystem (SSI as a universal service for all) + Sovrin Utility (enable SSI as universal service for all)
    - Missing : standard credentials are still reliant on a state/organisation
    - Missing : guardianship, offline connectors and low-tech SSI
    - Missing: delivery on the ground for missing 1.1bn
    - Missing: Ability to self assert most basic identity
    - Missing: ability to have SSI for > 50% of global population or for all of our lives
  - Next Steps Life Credentials

        - We are human beings and therefore there are certain things which are common to us (7 ages of man) - what are those common life credentials?
            - Using the construct of "I am …" to understand and arrive at are essential credentials
            - [Neil] individuals at a vulnerable state need assistance and special services to be part of the economy and social structure - different access, different credentials or perhaps different management.
            - [Alan or was it Jeff?] are there specific reasons for omitting gender from the construct - assertions of gender
                - [Nicky] it is a political point and when in context of this conversation it would not specifically matter
            - [Rachel] what would be an assertion of "I am a worker"
                - [Nicky] these assertions "I am…" are the core life arc credentials but there are also core roles
                - [Carly] Is that also similar to Parent? Would that be too limited? Transition child → adult - there is a blurring of the line based on rights
                - [Neil] as we go through life we tend to take on different roles (perhaps noted as attribute)
                - [Eric]
            - [Karen] can we capture Work Life, it has become a very big identifier in our society
    - Arc of Guardianship
        - Guardianship supports Self-Sovereignty
            - [Carly] Just a thought - you move from being passive (being governed) to active (governing) and back finally to passive. As you move along the path you gradually move from one to the other with many abilities being added and subtracted.
            - [Neil] A problem with SSI is it may not be credible (or trusted). The current model is that personal identity is asserted by central/large organizations (Government, Bank, Licensing organization)
                - [Chris] important to consider that, SSI is not limited to self-issued credentials. SSI supports an entire universe of possible credentials, including government issued credentials.
        - Life Credentials as the backbone for asserting of our human rights

Closing / Opening Day 3 / Agenda Creation Sessions 20 - 24

DID Document Representations (JSON-LD, JSON, CBOR, ...)

Thursday 20A
Convener: Markus Sabadello
Notes-taker(s): Drummond Reed

Tags for the session - technology discussed/ideas considered:
DID (Decentralized Identifiers), JSON, JSON-LD, CBOR, abstract data model, common data model, data representation

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

Markus, one of the editors of the W3C DID Core Specification, presented a slide deck explaining how DID documents are represented, and the challenges of using an abstract data model.

LINK TO MARKUS' PRESENTATION:
https://drive.google.com/file/d/1RBjubnmJXXlooIn3_ptiHzqCc7O4fIR6/

Chat from the session:
From Paul Bastian : Are we already in the middle of the session? Open Circle just ended
From Swapna Radha : Did it already start?
From David Huseby : hiya
From Ryan Faulkner : it is recording, hopefully you should be able to catch up with the first few minutes later if need be :)
From Orie Steele : Currently 100% of did spec registry extensions require JSON-LD… which leads to some interesting problems wrt the ADM translation complexity
From Orie Steele : "You could write code" famous last words :)
From Orie Steele : @Dave Huesby: https://github.com/w3c/did-core/issues/439
From Tom Jones : @orie that was the scariest answer I have ever heard - you have to write some code
From Paul DIetrich : Do DID docs still have optional signatures? Is that now based on the abstract model?
From Orie Steele : JSON-Only is going to be marked at risk and may be removed… its really not doing much but deleting an `@context` and allowing RDF nonconformance
From Nathan_George : I agree with Dave here, I cannot know about the foreign representations, I want a good enough handle on the ADM that I can live in my own fantasy land
From Tom Jones : if json only is at risk, I would suggest that DID is at risk
From Orie Steele : @Paul proofs have been removed from did core, but they can be applied with extensions ; @Tom I agree, its been very hard to get any real contribution to JSON-only ; Its essentially a representation that defines itself by not being JSON-LD :/
From Dave_McKay : @Dave https://www.w3.org/TR/vc-data-model/#extensibility
From Tom Jones : @orie - every single semantic representation that has ever been proposed for the web has failed - is that the future you want?
From Orie Steele : @Tom I think search engines work :) ; And I work with companies that use linked data every day :)
From Tom Jones : @orie - there is no special semantic for search - they accept local languages
From Orie Steele : @Tom, I invite you to learn more about schema.org and https://developers.google.com/knowledge-graph
From Tom Jones : @orie - I know lots of sematic federations - I know of no broad acceptance of semantics other than local languages

From Orie Steele : And also to join the W3C and help solve this through standards participation :)
From Tom Jones : @orie - I was an early member of the discussion group and was driven out by manu ; over semantics
From David Huseby : and he just ran into why JSON-LD is a problem
From Orie Steele : You can't be "driven out"… there is a formal process… you are welcome to join the discussion and help fix this :)
From Andrew Whitehead : abstract partial data model
From PhilWolff : backward interop?
From Tom Jones : I was accused by manu of being a a troll because I would not drink the kool-aid
From Orie Steele : Here is a cool example of how you can support multiple representation from the same did method… ; Https://did.key.transmute.industries
From drummondreed : It's an abstract data model that's only interoperable to the extent that extensions are registered in the DID Spec Registries
From Orie Steele : ^ which requires JSON-LD for registration :) ; Which is why its not really "RDF-free"
From Gabe Cohen : Continues to be interoperable as long as you support LD…which is not interoperable
From David Huseby : ^LOL
From Orie Steele : JSON is interoperable but JSON-LD is not? Makes no sense
From drummondreed : Just to be clear, the requirement for JSON-LD is just to describe any extension so it can be rendered in JSON-LD. It doesn't mean you have to produce a JSON-LD representation.
From Gabe Cohen : It's like comparing java and spring boot, the difference is clear
From Orie Steele : X-Headers are also deprecated ; lol ; We call this the "preserve by default" ; And it has almost universal adoption
From David Huseby : +1 @Orie
From Gabe Cohen : +1.2
From Paul DIetrich : Is the list of supported representations stewarded by a standards process, or is this a free for all like DID methods?
From Orie Steele : Jonathan holt is probably the only person who has contributed to a representation other than JSON-LD ; I've seen no other contribution to did spec registries, so if I seem frustrated by this….
From Gabe Cohen : Workday uses plain json…
From Orie Steele : Its because a lot of folks like to talk about PRs instead of write them :)
From Paul DIetrich : but does that have to go through a standards process?
From Paul Bastian : do you have a link for that proposal?
From Orie Steele : https://github.com/w3c/did-spec-registries/pulls ; https://github.com/w3c/did-core/pulls
From PhilWolff : has anyone been using ML or NLP toward understanding semantics of unknown endpoints?
From Orie Steele : Dude, I want waffles
From Andrew Whitehead : Yeah I hope he made enough for everybody
From Paul Bastian : Can someone summarize the core motivation for other formats other than json-ld?
From Orie Steele : The hope was that they would be safer or smaller
From Paul Bastian : except from this is my favorite format/saving some bytes
From Orie Steele : Neither is true today
From Gabe Cohen : The motivation is the desire to not touch JSON LD
From Orie Steele : JSON-only actually currently normatively supports prototype pollution ; Which grants ACE ; lol ; A lot of talk about security, but then a "preserve unknown properties by default" approach :)
From Paul Bastian : @Orie in which way is json-ld or the parsers unsafe?
From Markus Sabadello : Yes, there was a long discussion some months ago in the DID WG about not requiring JSON-LD, which is one of the reasons why this design was adopted

From Orie Steele : And no real contribution to shaking it out ; @Paul I don't think it is ; Thats my point :) ; Not safer, and not smaller
From Brent Shambaugh : I jumped in late. What is an "abstract data model" ?
From drummondreed : That's helpful, Dave, thanks
From Orie Steele : Dave just quit an help us fix this!
From jonathan holt : The Abstract Data Model is a bit too abstract for my taste, hence way I'm leveraging CDDL to make it more concrete.
From Orie Steele : Yep, json sucks compared to CBOR….
From Orie Steele : Except its readable
From Brent Shambaugh : @Orie I pinged you about the world of Category Theory in twitter land. I wonder if Abstract Data Model could be represented by Dr. David Spivak's and Ryan Wisenesly's work on CQL (catagorical databases) and FQL.
From drummondreed : The "tags" in JSON are—wait for it—JSON-LD context entries :-)
From Orie Steele : Lol lets use ASN1 ; Said no one ever
From Paul Bastian : ASN1 is cool :D
From Orie Steele : And we should listen to the guy who wants to use ASN1 ? ; lol
From Colin Jaccino : +1 to abstract data model. the model is the source of truth. Other formats are merely representations. The pattern is good architecture, but a bit more work. What format to use for the canonical model is what I'm less clear about
From Shigeya Suzuki : (I don't want to use ASN.1 ... :D)
From Paul Bastian : You had OIDs
From David Huseby : HDF5 i superior to everything else but it solves the data archiving problem above all else
From Paul Bastian : OIDs make internal structures totally clear in ASN1
From David Huseby : and isn't ideal for high speed and scalable systems
From Orie Steele : IMO CBOR could be massively better than JSON ; But requires a lot more help, can have Jonathan solo it :) ; Can't *
From Colin Jaccino : OWL or RDFa?
From Orie Steele : +1 to what mike is saying, as a did method, you are responsible for your representation…. The problem is that somehow we got stuck trying to get other people to care about "your representation" ; Yep, data sanitization and input validation are required regardless of representation ; And you have a combinatorics sanitization problem if you have unbounded representations ;)
From Dave_McKay : Yup, always need code that understands the context. We need that for innovation.
From Orie Steele : Ahhhh drummond ; please ; stop ; :)
From David Huseby : :) ; tags are not just for types but also field ordering so that digital signatures are easy to construct and validate
From drummondreed : Good point about ordering. The representation specs are responsible for that.
From David Huseby : json and stepchildren don't possess any notion of ordering. so they rely on canonicalization algorithms
From Orie Steele : Its not guaranteed unless you write code that comprehends the registry ; Which I doubt you will be doing :) ; Because its complicated
From David Huseby : canonicalization algorithms are an endless source of interop bugs
From Orie Steele : I like stable content identifiers… I use IPFS a lot :)
From David Huseby : +1 @Orie
From jonathan holt : One security concern for not allowing preservation of "unknown" properties is that it may present processing of nefarious code, such as a buffer overflow. The way we handled this in HL7 was create a property called "extension" and in that field you define your extension.
From Orie Steele : It adds work, that nobody does :)

From Swapna Radha : Looking to use IPFS in one of the projects.. is there any downside of using IPFS as content identifiers
From Orie Steele : Just be careful that you objects are canonicalized before uploading ; Or you will get different identifiers for the same object :)
From Paul Bastian : Comparison: is anybody in favor of adding 5 more proof formats?
From Orie Steele : -1
From Swapna Radha : Is there any example of IPFS usage other than w3c? I mean in an example use case..
From Orie Steele : TL;DR I prefer to ask for a representation from a did method, as opposed to asking for some to translate a representation for me… telephone game applies. ; From Orie Steele : Better to always ask the did method directly, when you can ; {accept: application/did+json}
From Gabe Cohen : If you get a did you care about translating you will translate
From Orie Steele : I'm unlikely to want to translate a did, form a method provider that couldn't figure out how to support my requested representation, but of course, asking the client to translate is always an option.
From jonathan holt : I was still hoping to get feedback regarding using CDDL from y'all. Any thoughts?
From Orie Steele : The client might also drop properties / sanitize injection attacks, or insert additional keys :) ; You would now need to trust not only the method, but every translator as well ; There is no "general purpose" integrity protection
From jonathan holt : Yep, +1 to Orie.
From Orie Steele : If you want to prevent translation, you might always sign it ; But a translator can always drop your signature :) ; Its not true, what is being said
From Nathan_George : The signature type specifies it not the serialization ; The signature type may require a particular representation as input for signing
From Orie Steele : There is no DID Core document signing ; Normatively defined ; Its 100% a did method specific thing
From Nathan_George : (I'm drawing on the VC approach, apologies)
From Orie Steele : Many did methods have no support for this.
From JC Ebersbach : ^^
From Nathan_George : Some methods sign some don't and rely on the consensus component of the storage repo
From Orie Steele : There is not "integrity" across translation ; Its a trusted process… you have to trust the software or operator doing the translation ; And it will almost 100% break any integrity protection the controller may have applied
From JC Ebersbach : the resolving process is already requiring lots of trust, even without translation
From Orie Steele : Exactly, but now you will be trusting resolvers to both resolve and translate.
From PhilWolff : FIVE MINUTE WARNING. NEXT SESSION STARTING.
From JC Ebersbach : well, if I use a resolver than I can also trust it for translation, don't you think?
From Orie Steele : Depends on who wrote the code :)
From Nathan_George : Terry —> very much this ; (I agree)
From Gabe Cohen : +1 provide in the format it's stored in. Translate at ends where necessary
From Orie Steele : But yes, resolvers are generally a trusted service
From Michael Jones : The next session starts in two minutes
From jonathan holt : I think it is to re-use your favorite processing library, i.e. JSON-LD
From JC Ebersbach : a solution could be to ask multiple resolvers/translaters to establish more trust
From Orie Steele : ^yep thats one solution ; If you don't trust the resolver, compare resolutions ; Finally YAML!
From Paul Bastian : who needs all these different formats, after parsing nobody cares anymore
From Paul DIetrich : Thanks Markus. Heading a quick break before the next session.
From JC Ebersbach : thanks a lot

Dependent Wallet vice Guardianship and Custodial - Alternative Approach?

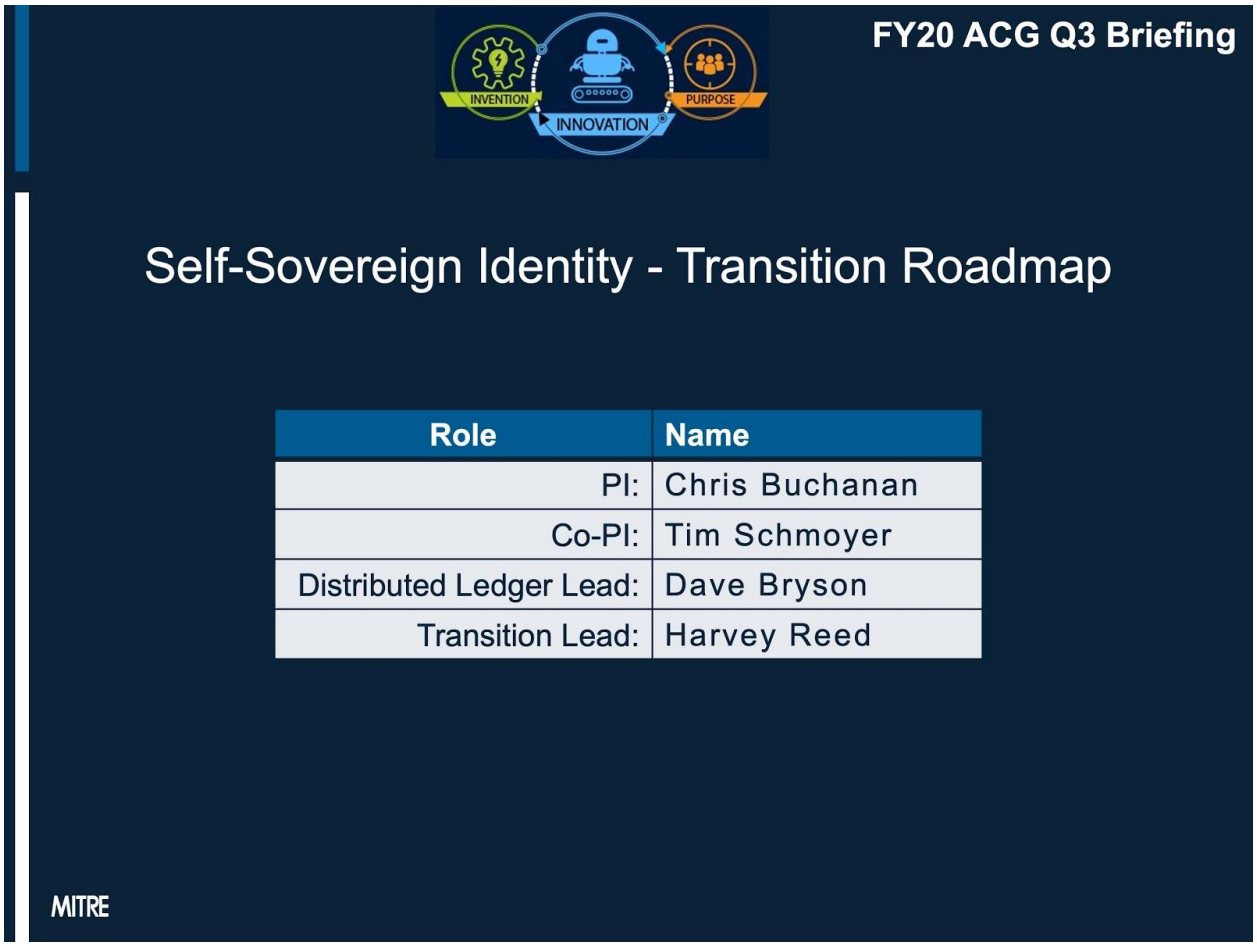
Thursday 20B
Convener: Chris Buchanan @ MITRE; cjb@mitre.org
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:
Guardianship, SSI, Custodial Wallet, Dependent Wallet

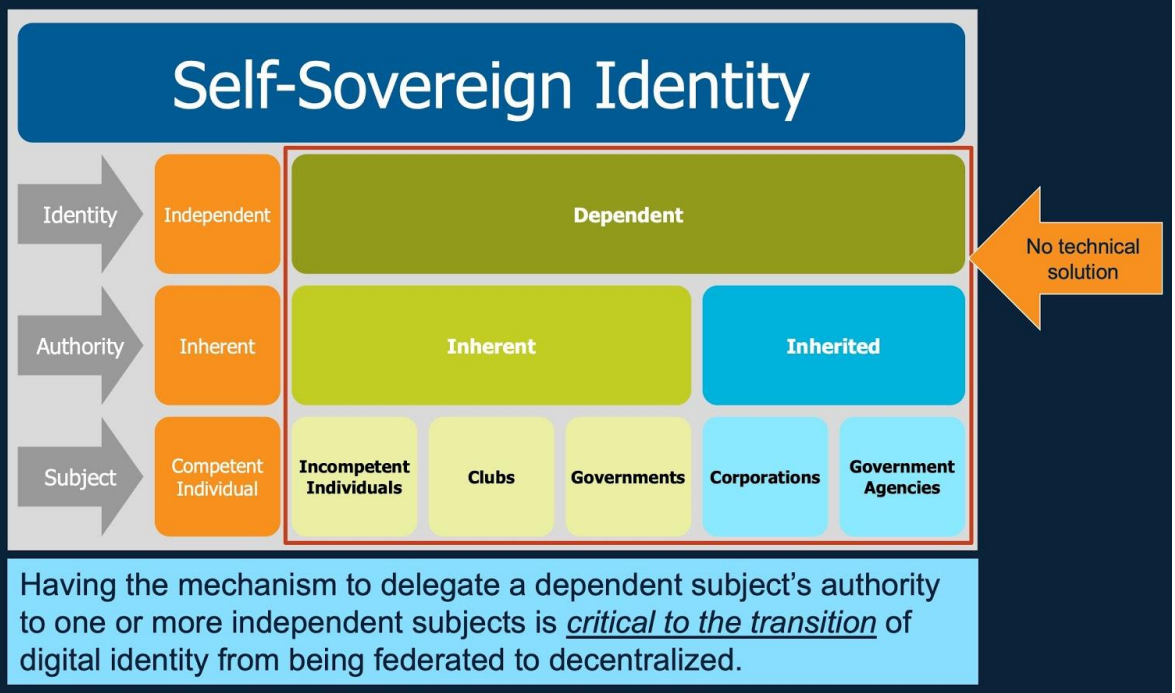
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The intent of this session was to proffer a potential solution to both guardianship and (maybe) custodial wallets by creating a technology that could allow control over a "dependent" identity. In this context a dependent identity lacks an independent will and cannot initiate transactions on its own. Instead, the dependent identity is utilized by one or more independent identities (people or agents).

Slides:



Problem 1 - A hole in the SSI ecosystem



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.

MITRE

Problem 2&3 – Establish and Use Dependent ID

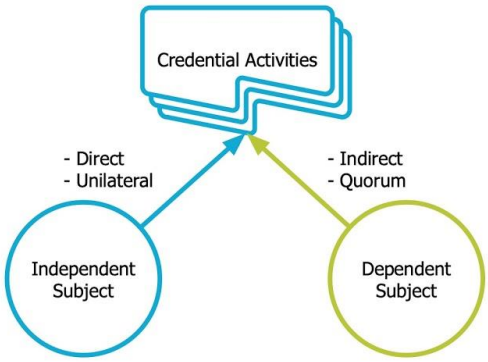
- **Establishing and utilizing a dependent identity presents two problems.**
- **Genesis**: How is the initial authority to delegate created?
- **Actuation**: Is the mechanism for the governance of *delegation*, usage, and revocation of authorities embodied in a system or a metasystem?

In other words, is it software or protocols?

Progress to Date – Systems Analysis (2/6)

Differential Analysis - Independent vs. Dependent

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



Progress to Date – Systems Analysis (3/6)

Assumptions

- A dependent identity is formed from the intent of one or more preexisting subjects.
- A dependent subject's authority must be intentionally delegated to authorized subjects.
- All activities by a dependent subject must be auditable with traceability back to the authorizing subject(s).

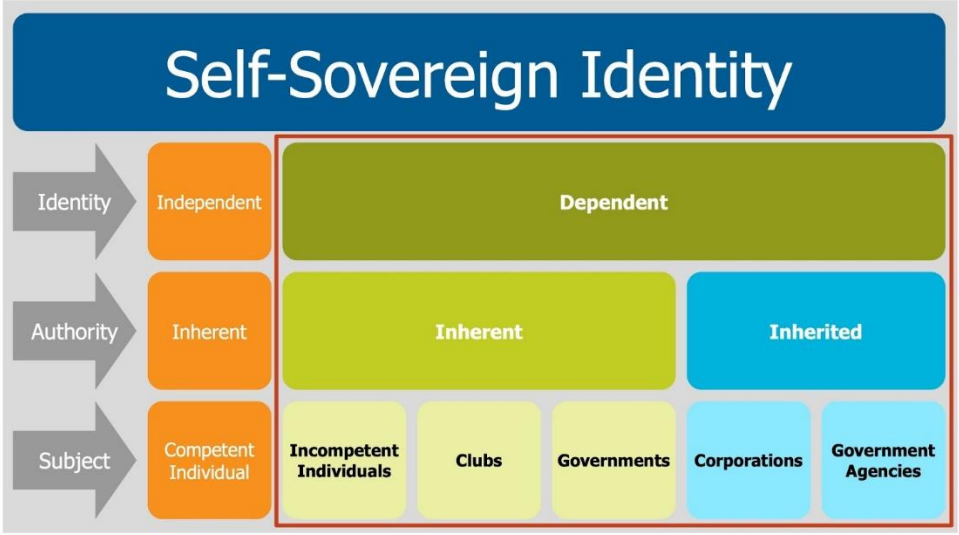
This assumption leaves open the door for one dependent subject to create others, but also creates a recursive loop that necessitates origination with one or more independent subjects.

This assumption, when combined with the preceding assumption, ensures that an authorized independent subject must be present in all activities (albeit not directly).

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.

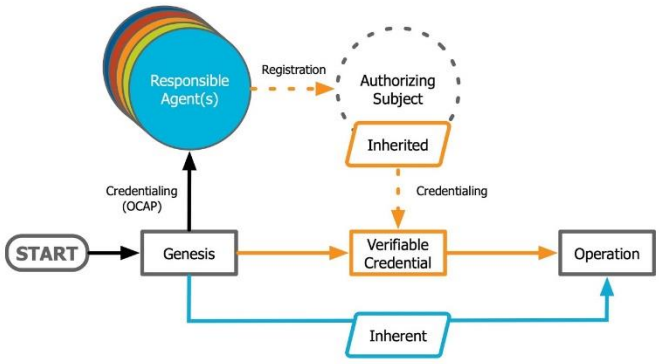
MITRE

Progress to Date – Systems Analysis (4/6)



Progress to Date – Systems Analysis (5/6)

Model of Genesis for Authority Types



Progress to Date – Systems Analysis (6/6)

Remaining Issues	Required Roles
Onboarding	**Trust Agent** - Individual - Quorum - Rule Based
Role Definition	**Role Manager** - Individual - Quorum - Plugins

MITRE

Browsers, Privacy & Federation (Cookies, WebID, CHAPI, etc)

Thursday 20C
Convener: Sam Goto
Notes-taker(s):

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

CHAPI (Dimitri Z):

- Worked on solid
- Ran into the the nascar flag problem
- We ran into many cases where we could use the help from the browser
- Introduction to CHAPI
- CHAPI standards for Credential Handler API
- (shows polyfill demo)
- https://chapi-demo-wallet.digitalbazaar.com/
- The cost of mediation is ossification that you pay for increased privacy/security
- https://github.com/digitalbazaar/credential-handler-polyfill
- https://w3c-ccg.github.io/credential-handler-api/
- game theory analysis?
- Judith: does this work in EDU/Enterprise use cases?
- Charles: mobile wallets?
- QUESTION(goto): What problem is CHAPI solving? The nascar flag? Evidence of demand?
    - David Waite: NASCAR FLAG is more prominent on EDU where you can sign-in with multiple universities (say, thousands) on a specific relying party.
    - David: currently, there are some third parties (seamingless?) that try to help with that will manage your relationship. identity verification, etc.
    - David: even infrastructure as wifi is something that you can use your university credentials to get access to wifi (eduROAM).
    - Currently works as "pick your universities out of these many logos"
        - https://its.uiowa.edu/support/article/655

QUESTION(goto): Can it be polyfilled? If so, why? openconnect.org? Payments Handler API?
ZCAP-LD or GNAP?
George: this solves the IDP tracking problem in a very interesting way.
https://w3c-ccg.github.io/ldp-bbs2020/

Conversation With The Future Users Of Your Products Or Services (Combined with Don't let 1st level support be the wrecking ball for your customer relationship - How to do it right in an SSI world)

Thursday 20E
Convener: Mawaki Chango & Andre Kudra
Notes-taker(s): Sankarshan, Andre Kudra

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

- Welcome and introductory notes
    - Building of products and development of services - discussion around the value proposition to the end user
    - How are the products/services going to make the life of the end-user better?
    - How far/close are we/you from/to widespread adoption of your products or service by the end user?
    - Bonus question - what are your predictions around the demise of password-based logins and access
- [Andre] interested in build optimal first level support in the SSI world
- [Bruce] will be presenting about Aries cloud agent in a few sessions (ACA-Pico make your own Aries Cloud Agent (point & click. no coding!)
    - Customers are called “owners” and not “users”
    - If you are a owner of something have also owned a Pico then the Pico can store all the relevant information about it
    - [Joyce Searls] If I am mowing my lawn with my brand new lawn mower and it goes bad. Then the QR code can be scanned to dial directly a call center which already knows the details about the machinery (which I am allowing to know)
- [Eric] responded to a government services RfP for a project at West Africa - looking for a way to go to existing or soon to be rolled out government services- using that to bootstrap digital identity component
    - Was not a SSI first play but a digital transformation and then asking what toolkits can be added to existing portals to link it back to SSI perhaps in the form of wallet so that the holders can accumulate the attestations originating from these transformation initiatives
    - Interested in lower mobile use cases and scenarios - combination of cloud+device based wallets. Similar to the Kiva Protocol talk - where the credentials could be accessed via simple terminal
    - citizens/peoples will have access to the services by overcoming paper hurdles
    - The adoption of the services would be through the governments extending their processes to online via digital transformation models
        - [Tom Jones] have generally noticed that it is regulated processes that are most likely to adopt self-issued ids
- [Michelle] At Kiva there has been a lot of conversations and discussions around the topic of support. Possible consumer protection legislation necessary prior to wide roll out.
    - Biometric fingerprinting with cloud wallets - the fingerprint is the form of consent for the national civil registry to open up an account (National ID and Kiva Protocol - see notes from Rachel C’s session on Day1)

    - Now Aries compliant credentials can be put into any blockchain - aimed at making it possible for businesses to be able to quickly add all the components needed to get a credential issued and verified
- [Karl] At iDRamp interactions with customers blockchain, SSI, cryptographic keys - topics which are not brought up unless the audience is very well versed.
    - Value proposition being bespoke for specific persona of customers and attempt to contextualize the value VCs bring to the customer's use case
- [Vic] HearRo is presented to enterprise customers (call centers and Customer Service Orgs) - it is a revolutionary way to connect and communicate with customers. Traditional forms are notorious for creating friction - all conversations have an immediate response to the delays and friction. Putting together identity, connections and communications it is a transformational process. "How many barriers do you want between you and your customers?"
- [Judith Fleenor] I'm hearing a lot of diversity concerns here… we are presuming a level of economic ability to have technology, to get help.
- [Scott David] Is Confidentiality in the cloud is purely contractual? Are there technical means to assure privacy in cloud, i.e., encryption.
- [Melody Musoni] Cloud based security and privacy issues when using that to managing digital identity
    - [Eric Welton] Africa needs more data centers - and there is a huge issue of national data outside of the country. We've run into problems using Singapore data centers from Bangkok - storing national data in some other country

Questions for 1st level support in an SSI world:

- Call center plan?
- Know-how about key management
- Technology available to end users
- Integration with existing support technology / portals
- Legislation for consumer protection?
- Who do you want / need between you and your customer?

Take-aways for 1st level support for vendors/product makers/service providers:

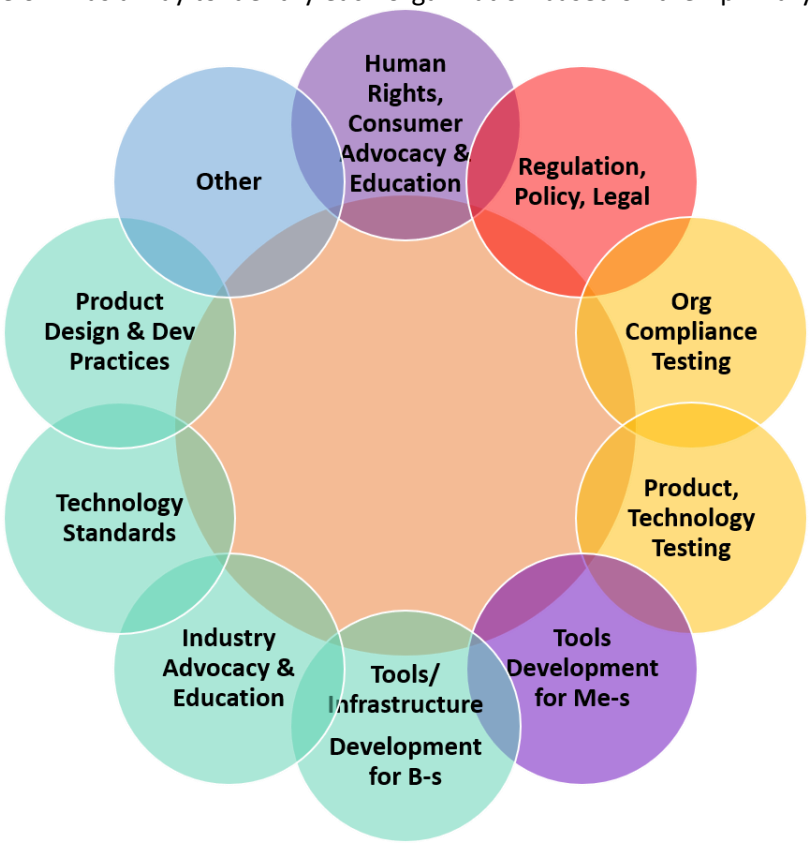
- We need to elevate customers in status. Instead of "user" maybe "owner" or "associate" or "groupie" or "fan" even
-
- Carefully designing support scripts intended to provide better understanding of the user persona - advice/escalate/help as appropriate

Me2B + Customer Commons + MyData + .. other .orgs =How we cooperate to effect change

Thursday 20G
Convener: Doc Searls, Lisa LeVasseur, Paul Knowles
Notes-taker(s): Lisa LeVasseur

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

- The Leadership Caucus: spawned from April 2020 VRM/Me2B day; Kaliya is chairing/organizing. It's not a new "group" it's just a convening, a place for org leaders to cross pollinate and also to address cross-org issues where solutions can be "greater than the sum of the parts".
    - It's early still, but developing.
    - Also thinking there will be maybe two regular gatherings: TLC and also one for the "super connectors". TBD.
- Diagram below was a way to identify each organization based on their primary function.



- During the session, participants identified the functions for the orgs they represented: https://docs.google.com/spreadsheets/d/1hBs5U5HXIS8jBkDGwlhF4Q50hwccu4WvUwwk

[partial] Chat window:

Notes from yesterday's Unified Messaging Front (for decentralized identity specifically), in case it's relevant: https://docs.google.com/document/d/1conHV3y-Fs2xWddeEQVv7UpKyuU4I_pVBlh-aW1qb2E/edit

From Lisa LeVasseur to Everyone: can you pls change that to a public link?

From By_Caballero to Everyone: https://drive.google.com/file/d/107GohjIc_ZFOZzqIQglE8jJ8krOlong4/view?usp=sharing

From Lisa LeVasseur to Everyone: thanks!

From John W (JLINC & MyData) to Everyone: Communities of practice and interest. Some of which are open source.

From Me to Everyone: farm analogy is a good one, if everyone is producing the same produce you flood market and its devalued

From By_Caballero to Everyone: Kaliya was working on cleaning up that doc a few weeks ago but I don't know if she finished

From Doc Searls to Everyone: I think it's important to hear from people who are in multiple .orgs: Lisa, Mary, Iain, adrian, John W... And also, for those who don't know, the elevator summary of what each of the orgs here are doing.

From By_Caballero to Everyone: ^^ GOOD PROCEDURAL RECOMMENDATION who's timekeepin'/directing traffic?

From Lisa LeVasseur to Everyone: hey kaliya! perfect timing

From Kaliya Identity Woman to Everyone: HI :)

From Lisa LeVasseur to Everyone: I just mentioned the Leadership Caucus

From Doc Searls to Everyone: I think it's important to hear from people who are in multiple .orgs: Lisa, Mary, Iain, adrian, John W... And also, for those who don't know, the elevator summary of what each of the orgs here are doing.

From Wip to Everyone: +1

From By_Caballero to Everyone: 11:58 AM https://github.com/decentralized-identity/decentralized-identity.github.io/blob/master/assets/map-of-adjacent-orgs-and-specs--sept-2020--one-sided.pdf

^ PARTIAL map of JUST the decentralized identity orgs by kaliya and myself

ooips better link: https://github.com/decentralized-identity/decentralized-identity.github.io/blob/master/assets/ssi-architectural-stack--and--community-efforts-overview.pdf politics is when the other guy does it :D

From Me to Everyone: not sure it should be organized around SSI in this case

From By_Caballero to Everyone: thus the PARTIAL in all caps!

From Doc Searls to Everyone: "where three or more are gathered, at least two are doing politics."

From mary hodder to Everyone: Instead of happiness, work toward satisfaction in the progress

From Me to Everyone: ah,, title threw me...

From By_Caballero to Everyone: :D Also happy to help if anyone is making a similar diagram/list of resources for the groups represented here!

From Lisa LeVasseur to Everyone: yes we are Juan

From Kaliya Identity Woman to Everyone: there is a cue

From By_Caballero to Everyone: oooh sorry hand-queue

From Me to Everyone: so some of the places around the circle depends on where you are in the lifecycle, e.g. standards precede certification

From Doc Searls to Everyone: We have a meeting of the 23 Families...

From By_Caballero to Everyone: this is awesome

From Lisa LeVasseur to Everyone: Me2B is a proto standards group
From sheldrake to Everyone: The Digital Life Collective has always been keen to maintain a map (in Kumu, as Kaliya here) of initiatives working towards decentralisation, agency, P2P etc. But as soon as you make the map, it's out of date. We've been trying to figure out how to keep things current, and so we're now working with https://murmurations.network/ <<< could be useful here. Happy to connect.
From Me to Everyone: I like the colors for category and then relationships from there..
From Doc Searls to Everyone: https://identosphere.net/
From Kaliya Identity Woman to Everyone: If you want to add your blog - https://identosphere.net/blogcatcher/ go to the end of the list and there is a mini-form. The projects on that map are mostly committees and discussion groups.
From Me to Everyone: on the tech for good front, we are doing work in Canada in collaboration here https://www.facebook.com/TechForGoodCanada/
From Doc Searls to Everyone: +1 to Murmurations. Looks very cool.
From Lisa LeVasseur to Everyone: ugh FB
From Me to Everyone: yes, I know.. its reaching out to kids though and uses social media
From Doc Searls to Everyone: The problem with Facebook is that it is the easiest possible way to create a group and get people involved. Unfortunate, but true.
From Jeffrey Aresty to Everyone: human rights groups like the World Justice Project,
From Me to Everyone: knew that would happen, look at the work and the salons and focus on addiction by design message as opposed to the platforms
From Jeffrey Aresty to Everyone: ABA Rule of Law Initiative Many others - just like them where I work in the human rights area, and, they do NOT understand the empowerment/inclusion potential of technology they just equate technology with surveillance
From Me to Everyone: +1 on the identity comment
From Jeffrey Aresty to Everyone: these are the front line SDGs groups
From By_Caballero to Everyone: ^ I find Jeffrey's point interesting from a messaging POV
how do we change the narrative of humanity versus tech :D
From Jeffrey Aresty to Everyone: with projects and funders - and generally are going as far as humanitarian aid and not much more
From sheldrake to Everyone: The problem we've found with wikis is that because it's not front of mind, because it's not in the projects' own domains, it gets forgotten / neglected. Search engines encourage webmasters to keep info bang up to date, so Murmurations protocol attempts to do it similarly. The info is maintained by projects in their own domain, front and centre, but in a form that can be pulled into a map.
From By_Caballero to Everyone: is it red?
From Kaliya Identity Woman to Everyone: We need to listen to and include the folks working on Indigenous Data Sovereignty (there are now three indigenous folks i know in the community)
From [TIOF] Jean F. Queralt to Everyone: The usual HR crowd has some really worrying angles/demands. Needs techies to be feeding a different narrative.
From Nader Helmy to Everyone: +1 Kailua **kaliya
From By_Caballero to Everyone: neoliberalism - nothing exists until it has been valued
get kaliya a Kailua! or... a Kahlua
From Nader Helmy to Everyone: amen!
From Debbie Bucci to Everyone: monetization may be consumer benefit - not necessarily a bad word
From By_Caballero to Everyone: More data decolonization, less HR automation (that uses confidentiality and AI to skirt anti-discrimination law)
From Debbie Bucci to Everyone: why should I benefit from the use of my data
From Kaliya Identity Woman to Everyone: Also this may be hard to hear but it building on what lisa is saying about "The white faces" - there needs to be more training and learning about howto learn new

cultural habits and patterns so our community goes from being passively problematic (like all of the culture mostly is) to actually inclusive
From Debbie Bucci to Everyone: shouldn't
From By_Caballero to Everyone: god cop bad cop
From Me to Everyone: hehe, neoliberal redux
From Kaliya Identity Woman to Everyone: (the good thing is our community isn't actively hostile like many tech communities are - so yeah - but it isn't good enough for women and people of color to show up).
From By_Caballero to Everyone: we're the less evil monetizers
From Me to Everyone: frankly the identity community is the source of the most advanced surveillance technology on the planet..
From Nader Helmy to Everyone: @juan what even is data decolonization in somewhat concrete terms?
From By_Caballero to Everyone: oh sorry it was a term from yesterday's session
From John W (JLINC & MyData) to Everyone: +1 Kaliya. The particularly hard part of that is that people of privilege (white and/or male and/or tech) have to learn to step back, shut up and listen.
From By_Caballero to Everyone: host can lower hands
when you call on people :D
From Me to Everyone: different than identity management though..
From pknowles to Everyone: Cool diagram. I call those two bubbles the "Inputs domain" and the "Semantic domain".
From Juan (By_) Caballero to Everyone: the borg some of you don't want to be "identity people" but everything is identity… :D
From sheldrake to Everyone:
From Margaret Wheatley's work in the 90s:
https://generative-identity.org/content/images/2020/10/wheatley-identity-relationship-information.png
From Doc Searls to Everyone: In Kaliya's Venn, agency is on the left, I think. Also, there is choice about how one identifies themselves, including nameless ways (e.g. with a verifiable credential saying one is over 18)
From Kaliya Identity Woman to Everyone: Yes Meg's work is super key.. and I have leveraged it to help advise how we actually network our community together and do work together
From Doc Searls to Everyone: +1 on Margaret Wheatley.
From Juan (By_) Caballero to Everyone: notes: https://docs.google.com/spreadsheets/d/1hBs5U5HXIS8jBkDGwlhF4Q50hwccu4WvUwwkEMlgc8/edit#gid=0 filling out a matrix cuz I like spreadsheets
From Kaliya Identity Woman to Everyone: the systems leadership articulation - https://identitywoman.net/systems-leadership/
From pknowles to Everyone: Human Colossus Foundation - building core utility tech components for a safe and secure data sharing economy. We definitely sit in "Infrastructure".
https://humancolossus.foundation/about
From John W (JLINC & MyData) to Everyone: Apologies. Have to step away.
From Juan (By_) Caballero to Everyone: all GPL, right? I saw the TDA is GPL (exc dependencies :D)
From Jeffrey Aresty to Everyone: I was lucky to spend 3 days with Margaret Wheatley in 2000 - she changed the way I look at everything - New Terms of Engagement for the Global Society
From Doc Searls to Everyone: This is stale (for reasons Philip gives above: everything changes), but may be useful: https://cyber.harvard.edu/projectvrm/VRM_Development_Work
From Trev Harmon to Everyone: ID2020 Alliance Manifesto https://id2020.org/manifesto
From Nader Helmy to Everyone: OpenMined are awesome!!
From Kaliya Identity Woman to Everyone: ITs so great to have folks from ID2020 actively participating in this IIW
From Juan (By_) Caballero to Everyone: all B or Mes too? the Me/B distinction might be significant here

From sheldrake to Everyone: commonsstack.org/
From Michael X Shea to Everyone: A metric clock..
From pknowles to Everyone: https://www.openmined.org
From Wip to Everyone: I hope to have much more OpenMined participation here in the future
From Jeffrey Aresty to Everyone: https://www.techforjustice.org/ibo-summit/ We are bringing the tech (IIW) and SDG human rights which I work with (World Justice Project, Institute for Global Leaders at Tufts, Rule of Law Initiative) together to work on Identity for All - ALL TOGETHER NOW!!! NOVEMBER 17-19
From Nicky Hickman to Everyone: I think AI is the next frontier that needs exploring with respect to SSI. Feels like something we need a TF for
From Doc Searls to Everyone: These are all "Me" tools that wish to exist:
http://customercommons.org/home/solutions/
From Juan (By_) Caballero to Everyone: boom
From [TIOF] Jean F. Queralt to Everyone: Gosh, I dislike Zoom.
From Lisa LeVasseur to Everyone: Can you please add M2BA in the list, Juan thx
From Juan (By_) Caballero to Everyone:
https://docs.google.com/spreadsheets/d/1hBs5U5HXIS8jBkDGwlhF4Q50hwccu4WvUwwkIEMlgc8/edit#gid=0 crowdsource! everybody feel free!
From pknowles to Everyone: Good spreadsheet, Juan!
From sheldrake to Everyone: I can put the AKASHA Foundation in the mix. Heavily focused on Ethereum and Ethereum-type technologies, with the purpose of empowering individuals with the nod to creating the conditions for collective intelligences to emerge. In terms of the spreadsheet columns: C, G, J, K
https://akasha.org/
From Juan (By_) Caballero to Everyone: ^ feel free? or are you on a browser you don't want to sully with google cooties? :D someone else capturing this? i'm having audio problems
From pknowles to Everyone: This is super beneficial. Thanks Lisa, Kaliya, etc. . my mate, Juan, too!
From [TIOF] Jean F. Queralt to Everyone: Mine was residual.
From Doc Searls to Everyone: anyone know how to unlink text in this kind of spreadsheet
From Juan (By_) Caballero to Everyone: ctrl-K the block there is an unlink icon in the upper right
google is dangerously convenient :D
From Iain Henderson to Everyone: agree with Nicky's point above; ML and AI are very much the up and coming frontier in both good ways and bad ways. Needs to show up on the map somewhere ideally.
From Jeffrey Aresty to Everyone: Funders are asking me about AI implications of SSI
From Lisa LeVasseur to Everyone: Nicki what's a TF?
From Juan (By_) Caballero to Everyone: task force?
From pknowles to Everyone: WG Work Group TF Task Force FG Focus Group
From mary hodder to Everyone: The Identity Gang - 2005 at PC Forum
From Jeffrey Aresty to Everyone: Funders are asking me about AI implications of SSI. Will is the one to talk to about that :D
From Nader Helmy to Everyone: TF = trust framework I'm assuming
From Lisa LeVasseur to Everyone: thanks
From Juan (By_) Caballero to Everyone: OpenMind is very interested in SSI as a tool to combine with blinding and/or differential privacy
From Jeffrey Aresty to Everyone: AI is where the ethics will be built in
From [TIOF] Jean F. Queralt to Everyone: Some links:
Let's talk Digital Rights
https://docs.google.com/document/d/1YIKgxID7nEtGQrU6X2EOMi75I1WjJ8_EAPv_X1KXe-E/edit?usp=sharing
UDDR White Paper Draft

https://docs.google.com/document/d/1Id4gIcoDzsZs04EdWZM-5vs5M_nSlheAMb68ZmJwrhs/edit?usp=sharing
UDDR Draft
https://docs.google.com/document/d/1y9C-5TPYmRruRQqJq39-HePk3ypWLDpSAEVzuonOH2Q/edit?usp=sharing
UDDR Concept Brochure
https://docs.google.com/document/d/1y9C-5TPYmRruRQqJq39-HePk3ypWLDpSAEVzuonOH2Q/edit?usp=sharing
From Iain Henderson to Everyone: yes it's been a long journey Doc...; in many ways that the cohesiveness in the community is very impressive. Yes, it's all getting bigger and more difficult to cross-pollinate but at the core there is a good alignment.
From Doc Searls to Everyone: control-K or command-K don't do anything other than bring up the menu that doesn't include unlinking. don't see unlink elsewhere, including the upper right. Agree, Iain. I think we're making a not-elephant together. What is it? we'll find out...
From Juan (By_) Caballero to Everyone: mine's a woolly mammoth and I worry it's stepped in something and I never figured out how to unlink column M, only how to unlink column A
From Mark Lizar to Everyone: Next Gen - Community Education Framework +1 - this was great
From mary hodder to Everyone: raised hand
From John W (JLINC & MyData) to Everyone: back
From Lisa LeVasseur to Everyone: W3C Privacy CG W3C PING
From Kaliya Identity Woman to Everyone: Rights
From Lisa LeVasseur to Everyone: IEEE 7012, IEEE 7000-series and ethics series of standards (SSIT standards)
From George Fletcher to Everyone: @Lisa could you make me the host when you leave... my session starts in this room at 10am PT :)
From Lisa LeVasseur to Everyone: sure
From Doc Searls to Everyone: We're now up to 28 people.
From Mark Lizar to Everyone: W3C Data Privacy Vocabulary Controls (is a good one)
From Doc Searls to Everyone: 29
From pknowles to Everyone: Terrific idea, Mary. That would be a useful exercise for sure.
From Lisa LeVasseur to Everyone: @ George--how do I do that
From Kaliya Identity Woman to Everyone: That doesn't really feel possible. They are super intense - it took the W3C and DIF 3 months of lawyers talking to get alignment to have a joint group
From Bill Wendel1 to Everyone: If Me2B's goal is to position themselves as consumer advocates encourage leadership team to connect with Consumer Federation of America, see Privacy header and other sections on their landing page http://ConsumerFed.org
From Kaliya Identity Woman to Everyone: No lawyer wants to give any advice that isn't specific about specific documents.
From Juan (By_) Caballero to Everyone: where do I submit my application :D
From Doc Searls to Everyone: Latecomers might want to look at the spreadsheet we're building: https://docs.google.com/spreadsheets/d/1hBs5U5HXIS8jBkDGwlhF4Q50hwccu4WvUwwkIEMlgc8/edit#gid=0
From Juan (By_) Caballero to Everyone: ^and add their orgs!
From George Fletcher to Everyone: @Lisa I'm not sure :) Maybe it will default when others leave
From pknowles to Everyone: paul.knowles@humancolossus.org
From Mark Lizar to Everyone: We have worked on a Master Privacy Controls (normalising rights regimes) with Receipt types
https://openconsent.atlassian.net/wiki/spaces/IHD/pages/768245803/Receipt+Types+to+Master+Privacy+Controls+for+Privacy+Agreement+Clauses

From James Manger to Everyone: Next session
From George Fletcher to Everyone: For others who are joining this room... the Mobile App Impersonation session will start shortly
From [TIOF] Jean F. Queralt to Everyone: Thx everyone.
From Doc Searls to Everyone: We peaked at 30. Nice.

Which Came First, The Issuer or The Verifier? Overcoming the Chicken & Egg Problem for the 3-Sided Verifiable Credentials Market.

Thursday 20M
Convener: Riley Hughes
Notes-taker(s): Stewart Whitman

Tags for the session - technology discussed/ideas considered:
Adoption of SSI - VC Cred adoption

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

Interviews of business persons selling VCs into the market

Chicken and Egg problem is no value until there is a network. Need the network effect to create volume.

50/50 Split
Ecosystem first.
Single Sided market approach.

Ecosystem - All partners come in at the same time. Cold start.

Single Sided - just went to one partner, (just issue or verifier) and sell them on the benefit. Then bootstrap the other side of the transaction.

Experience in selling single sided, getting a few issues who believe in the vision, then building the verifiers.

Other models as a proxy to start up and the issuer (ID verifier) and then use that on the verifier side.

Pays vs Plays in the ecosystem, single sided one payer morphs to all pay and engage in the market.

Verifier is the payer and is creating the standards for the issuers data.

Margo's 5 levels of approaches (very early idea -let's iterate!)
Inside vs across companies
"Pay" vs. "Play"

Issuance Experience	Verification Experience	Notes
Company A issues (pays)	Company A* get verification value (plays)	"Self-contained", primary value within issuing dept /team *Could replace "Company A" with "Consortium A"
Company A issues (pays)	Company B gets verification value (plays)	
Company A issues (pays)	Company B verifies, sets requirements (pays)	Discussion of revenue share opportunities here
Company A participates in issuance (plays)	Company B verifies, sets requirements (pays)	
Company B participates in issuance (plays)	Company B verifies, sets requirements (pays)	"Self-contained", primary value within verifying dept/team

Types of ecosystems:
Self-contained
Proxy-issuer
Curated
Open

"Player" vs "Payer"

Relating the American Express Credit Card market, ecosystem born from all participants entering the market together (Corporations who want expense control (issuer), Sales people who want to spend on client dinners (holder) , restaurants who want to accept payments, (verifier)

Which are the use cases that are harder or easier to achieve

Ecosystem is the "sexy" exciting use case that we all want, academics, kyc, etc. pitcher and the catcher are on different teams.

But Single Sided is an easier route. Pitcher and the catcher are on the same team.

Tech constraints IAM industry in crossing domains, (eg Boeing to McDonalds)

Low hanging fruit, passwordless login.

Physical Access, where it can be done offline.

Social recovery scheme is difficult to cold start.

NHS Dr. credentials example of single sided build, multi entities but under "one roof".

Need to not sell the technology, selling the solution.

Vitamins vs vicodin vs viagra

How do you sell SSI as an IAM service when institutions have already invested heavily in enterprise IAM, which are increasingly offering passwordless options

- Phil -> it doesn't necessarily save the university money, it's a foundation for future opportunity and new use cases, plus it solves the existing problems
- Maybe UX is the better argument rather than cost savings
- Password resets are another big painpoint

Duo was a bad experience trying to recover, eg. for Riley out of the country. But this is a common problem even for VCs, where people don't understand how the wallet works and lost their backup, etc. Must make sure the support/corner cases work.

Is the university registrar a profit center or cost center.
Universities are big processors of application which include transcripts, and it is a big cost center. This is about consuming the transcript.

There isn't really a reason to issue an outgoing transcript via VCs.

Reverse articulation, transferring classes back into the university to complete the degree, it can be a painful process.

Keith Kowel(?) mentioned the CLR standards for transcripts that is gaining traction.

Zoom Chat Transcript
(Sorry, copy/paste was wonky so I couldn't get names or timestamps)

Are we going to record this session?
Thank you.
resonates!
I think the holder should be paid:0
and the verifier should as well
verifier should pay for the verification proecss
My thoughts are the holder should pay, but someone could pay on behalf the of the holder. For the covid example it would be paid by insurance
holder already pays in most circumstances…
I just paid $800+ for my DEA renewal
Then wouldn't this VC just be a part of that fee?
The network-bootstrapping problem is not novel to SSI. (e.g. Facebook, Visa, Paypal, and email, have all solved this kind of problem). Any interest in talking through historical examples, to see if there's any pattern(s) to how networks have been successfully bootstrapped in the past?
They should pay for this service so they capture more of that and don't lose so much on admin cost, but when the verifier pays the holder should get a cut because they paid the original cost… it needs to go in any direction that fits that specific business model. each of the 3 entities holds a certain amount of control and value when these VC's move.

Thanks for calling this session Riley. See you all out there. -David
Yes Jace that fee should go towards paying for this tech to retain more revenue $ for the issuer
Re Pay Pal- they had to pay (give people $10 free to spend) in order to get a fire under their business model… same as Uber $5 free ride etc...
I think the business model for every ecosystem is unique. However I say motivating parties to issue is always the hard part - because issuance carries implict risk in the US context.
+1 Keith
I think one challenge we tackled was background check companies who are ideal organizations to bootstrap a users trusted identity to overcome the chicken and egg. However in this context we are breaking the existing background check companies business model so finding the model is hard.
Convener = Please put your name into the Agenda Wall so we know who you are. Thank You!
If anyone has copy for what you send to the issuers re the value of this, please share with Leah@hpec.io
we are working with multiple SSI companies to approach some of these legacy issuers in healthcare… we imagine that if they receive the same information in different ways from different entities they may open their eyes and start paying attention,
+1
this is why we NEED complete interoperability FULL STOP
Fully agree with Timothy
we sale as "digital certificates" then back up with benefits like password-less, MFA etc
Anyone hear of Axuall?
www.axuall.com
Yep, Axuall is legit
they are tackling this
making agreements with health systems and medical schools
yep Truu.id
"People don't buy a drill, they buy a hole in the wall"
+1 Keith, you gotta dollarize it.
Can someone take over the notes, I am going to drop into Room E
Just make sure you catch Phil's and Riley's comments about Viagra ;)
I'm wishing that the three pills in the analogy were alliterative: "Vitamins, Vicodin, or Viagra" 
:)
BUT… and think about this… You NEED a Doctor to get Viagra AND Chemotherapy… think about that and come to Demo Table 12 to see how we are gong to make this easier for EVERONE
+1 Leah! Time for sales skills like that to take over this industry... :)
LOL
As Phil said Universities use Duo because its cheap to use :)
I've heard many complain about the UX with Duo. Maybe that's the better argument than cost savings. :)
And "cheap" is relative. It's still six-figures plus, so not chump change.
Gotta run... great convo!!
Take a look at National Clearing House for issuing transcripts. I believe that are participating in Velocity.
Great conversation thanks for running!
But also be aware the new standard gaining steam to issuing transcripts is the CLR standard.

The Real-World Benefits of KERI (muggle-friendly, really!)

Thursday 21A
Convener: Timothy Ruff, Sam Smith, Drummond Reed

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/10f0H9y4WAc28BE17CMRfTzbX_SWO8M7rj-FXqH0tCMk/edit?usp=sharing

We discussed this ^^ slide deck, which reviewed all the high-level benefits of KERI.
The session was recorded to the cloud, but I'm not sure where to retrieve it? (Timothy)

Policy-Based Authorization: The Abacus

Thursday 21B
Convener: Jacob Siebach
Notes-taker(s): Judith Bush

Tags for the session - technology discussed/ideas considered:
Policy-based authorization

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

See previous PBAC sessions.

Abacus Authorization jacob@abacusauthz.com https://abacusauthz.com

ASSUME:

Domain driven design: Domain is business driven, self controlled

Policies protect access
Consider : identities (persons, device), authN (confirm the identity), access management (manual ways to designate certain controls, not derived by alternative attributes), authZ (can the identity do the thing)

Requirements
- Protect domain's data
  - ONLY allow access through API and not thru direct DB access
- Rely on authZ-important attributes
  - authZ "over 21" not birthdate
- BE SUPER FAST - part of infrastructure

How does Abacus keep fast: cache attributes.

- Attributes super available
- No load on other DBs
- Reduce network traffic
- Authz when domains are online

Domains own the attributes and push the attributes to the engine. Updates get pushed.
AuthZ engine has no DB connection, just the cache of data WHICH IS NOT PII
Thus attributes used in policies without seeing the data

LOG EVERYTHING

- Maintain policy history
- Allows auditing and metrics
    - Have different points calling the engines with different endpoints
    - SIEM can then integrate by watching
    - Verify that domains are changing their attributes no other

- Support system
    - Logging analysis can show why X had access to Y then and not now . The attributes the decision was made on, the domain that owns the attribute, and can refer X to the the domain that changed the attribute or the system that changed the policy
- How long to keep logs? Depends on business purpose

Consider Registration and the mad dash for signing up for classes and the churn, but then quiet. How to make registration provisioning quickly -- and engine specifically for that domain during the surge period populated with ONLY the attributes needed for that use case. -- but since many consuming domains use the attributes from the same domains, it is more efficient for the consuming domains to all share the same engine.

XAML allows circular references so they use a simple policy sets for an action on a resource. "Self service policy" written ones and included in the sets. Has their own grammar for speed in parsing. Efficient memory management.

Business owners implement their own policies through abacus UI.
Use with access management: user has access management role PLUS active employee attribute.

So core attributes can be used across many domains. Once ONE system gets the attributes provisioned and pushed, then many policy domains can benefit. Infrastructure builds up and benefits many policy domains. Role is about what you are allowed to do, a capability, a feature you can utilize. Separate from permissions: what objects you can work with. - Neil Thomson.

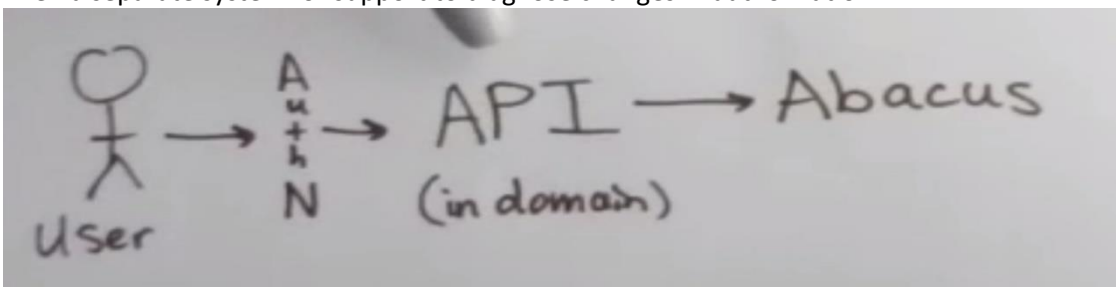
When you are sending data to the authZ engine, you want to send data that is also specify the specific resource and action. File + author can be sent, so the policy can be "author of file can do thing". Role can be "Report author" and policy can be that authors of report can edit, others can just view.

Polices are part of a policy set, where the set is an action on the resource. Don't couple the action to a specific endpoint, but to the abstract, so the policies can apply across different interfaces.

Policies are centralized and can be easily audited. The specific folks with manual role grants can be easily audited.

Can drive role assignment for cloud services from the policy engine. Consider providing an LDAP connector that generates the "groups" from the policy engine.

Request: Subject, target, client ID of system, other bits of data (IP address, file owner, took training)
Response: Allow/Deny
Then a separate system for support to diagnose changes in authorization.



DIDComm Mediator Agents (v1 &v2) - Intro & Where Open Source Projects Are

Thursday 21D
Convener: Sam Curren
Notes-taker(s): Bruce Conrad *et al*

Tags for the session - technology discussed/ideas considered:
Did, didcomm, mediator

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

Overview diagram, DIDComm Mediators

Link to DIF spec for relays see also this guide

Link to Hyperledger aries RFC 0046 mediators and relays (see images therein)

Alice and Bob may *need* a mediator/relay because their devices cannot be endpoints directly

Each edge agent (Alice and Bob in the diagram) has a relationship with their mediator, so that the latter knows which messages to forward to their edge agent.
Communication between edge agent and mediator agent are *not* part of the spec, at least currently. This is vendor specific, and does not break interoperability.

Another reason for using mediators is to gain crowd-produced privacy. And each agent can use a chain of mediators (of arbitrary length (depending, as Sam says, on the thickness of their tinfoil hat)).

We don't expect "normal" (no disrespect intended) human beings to configure these chains, but rather this is done by the user's agent.

Much discussion of privacy/security concerns. Someone needs to elaborate here!

Dave Crocker points out that these kinds of concerns have been addressed for decades, and refers us to RFC5598 (thanks to JC for the link (and Wip for this history (from 1981!)))

Micha raises concerns about mediators as a single point of failure. Question to be answered.

Outputs of the DIF working group: the spec and the guide (see links above). Watch for useful updates coming soon.

When Bob makes a new DID for communicating with Alice, Bob must inform his mediator, so that it will know what to do when messages arrive for that DID. Note that in DIDComm version 1, there are no DIDs in the outer envelope, only keys.

Requests for mediator service, and Grant/Deny responses, etc are defined in Aries RFC 0211.

Adrian comments about how this is like negotiating service agreements and their contracts.

Sam pointed out the "Key List" operations in Aries RFC 0211. The ACA-Py codebase is being modified to embrace the newer specifications.

Also shoutout to the aries-framework-go group who have extensive documentation.

Adrian points out that this exact same conversation is happening in the UMA group.

Daniel points out that you can totally use DIDComm without mediators.

Why would we want mediators to be packaged together? We have several cloud agent implementations and several mobile agent implementations. That's where the mediator conventions come in handy, so that you can mix and match vendors. Advantage of using a package is that the mobile agent can come pre-packaged with its meditor, and the end-user doesn't have to get involved at all.

[notetaker taking a bio break (is that TMI?) so some discussion may not be captured here]

Bengo asks, "MLS is new to me. Is DIDComm-Messaging an implementation of MLS Architecture? https://www.ietf.org/archive/id/draft-ietf-mls-architecture-05.html " Kyle replies "+1" see also the chat for more from bengo.

Biometrics & Identity: A Preview of The Future

Thursday 21G
Convener: Jeff Kennedy, John Callahan, Asem Othman
Notes-taker(s): John Callahan

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

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

Slides for the session can be found at https://docs.google.com/presentation/d/1D1GsI6bev64Mkqr5hzNhO48699kF6vuVnQwItj_gytE/edit#slide=id.p

A video at: https://www.youtube.com/watch?v=hZPhri9rpAk&feature=youtu.be

Mobile App Impersonation

Thursday 21G
Convener: George Fletcher
Notes-taker(s): George Fletcher

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

We discussed the issue of OpenID Connect and OAuth public clients being easy to impersonate and the implications thereof. While most mobile apps using these protocols use custom schemes to give control back to the app after the user authenticates via the "system browser" the better choice is iOS Universal Links or Android App Links. However, there is still an issue with Android App Links in that they don't completely resolve the "impersonation" problem.

We talked about other solutions like app attestation + device attestation + dynamic client registration and how that could completely block impersonation attempts and provide companies with high confidence that they can identify their 1st party apps.

It was also raised that there is very little data as to whether this is an ongoing problem for mobile apps and solving it is worth the cost to developers or companies. No one attending had any data nor do I believe anyone has even looked for app impersonation in their logs:)

The session was recorded but that should not live forever.

Session cut off abruptly. I suspect because 1 of the 2 hosts left. That was unexpected. Sorry for cutting off TJ.

Ideas to Action: Putting Decentralized Identity to Work (Alternate Title: Get Over It: What are your barriers to adoption?)

Thursday 21J
Convener: Scott Harris (Indicio) & Karl Kneis (IDRamp)
Notes-taker(s):

Tags for the session - technology discussed/ideas considered: Adoption strategies, facilitating understanding of verifiable credentials, use-case specific solution building

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

In this session the key takeaway was that the technology is no longer a limiting factor. There have been enough use cases and development to enable useful building and implementation.

The blockers continue to be:

1. Education of both business and technology decision-makers
    1. There is rarely a "simple" story to tell surrounding implementation and understanding of the value propositions. Therefore it is important to focus on problem-solving at the micro level.
2. Competing vision of top-down vs. grass-roots adoption cycles
3. Real world wallet use and interoperability
    1. Making credential holding and use simple for end users in the B2C world
    2. Finding ways to solve for multiple wallets on the same device and credential movement between wallets is important

EISPP/VRM, Interop., RDF, Category Theory, Data Migration

Thursday 21M
Convener: Brent Shambaugh
Notes-taker(s): Brent Shambaugh

Tags for the session - technology discussed/ideas considered: Category Theory and EISPP

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

Brent discussed Category Theory and FQL[1] and made a brief mention of EISPP when Kim Duffy mentioned it after it appeared in the chat. [1]
Kim wondered if too much manual mapping of each field was occurring, and whether category theory could ease the transition between different data models. There are serializations in XML and different ones for RDF.

Brent wonders if FQL, functorial data migration language, could be applied to data migration and enhance interoperability. Dr. Spivak talked about categorical databases (added for context), David Spivak: Categorical Databases [2] . Categorical databases preserve nodes and connections. Is this enough for what Kim was talking about?

Kim mentioned being impressed by Eric Myer's work , and found it interesting viewing things from an orthonormal basis . be more expressive and (unable to read my own handwriting!).

Kim thought that it would be appropriate to have Henry Story present in the credentials community group . Brent mentioned that Henry Story has his own community group for category theory (ref: added after: https://web-cats.gitlab.io/). Kim said she knew him. Kim thought that category theory was a bit abstract and may be too far along (maybe too abstract) for the work doing right now (too low level maybe).

Kim mentioned expressing things algebraically, and Brent remembered Dr. Ryan Wisnesky's comment (outside communication) about Category Theory being useful if things can be expressed alegbraically. (add outside note: except Brent is confused because category theory can be applied? to so many mathematical fields and other areas outside of mathematics?)

Brent wondered if category theory would inform decisions, but wondered if his ego was getting in the way, but wanted it to be useful sooner than later.

Kim asked about a comment in the chat about EISPP. Brent explained that it was a model for stigmergic collaboration. It was his explorations as he was learning from technical papers without a computer science background. He explained that if anything it informed him about the semantic web and linked data.

Brent said a lot more, but if was basically an overview of the Category Theory and CQL document and comment about what was going on in the space.

[1] https://drive.google.com/file/d/1riKKtxwD-HcKNhv1W7fBjaMCKhI8bXV3/view Category Theory and FQL

[2] https://www.youtube.com/watch?v=bk36__qkhrk David Spivak: Categorical Databases

The Verifiable Credential Stack

Thursday 22A
Convener: Timothy Ruff
Notes-taker(s): Neil Thomson

Tags for the session - technology discussed/ideas considered:
VCs/Verifiable Credentials, SSI, ToIP, Business of SSI

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

Story

1956 Malcom McLean – inventor of the shipping container – contributed more to world trade than any other changes in 50 previous years.

Cost of $5/ton -> 16 cents. Took 10 years due to resistance to change

Verifiable Credentials is the shipping container of Authentication.

There is disagreement about a lot of the ways forward (block chain vs. KERI)

What is being getting a huge support for is verifiable credentials

LER – learning and employment record – for Universities – as a standard on course accreditation via verifiable credentials

What are the contents of a credential to verify, but the concept is a done deal

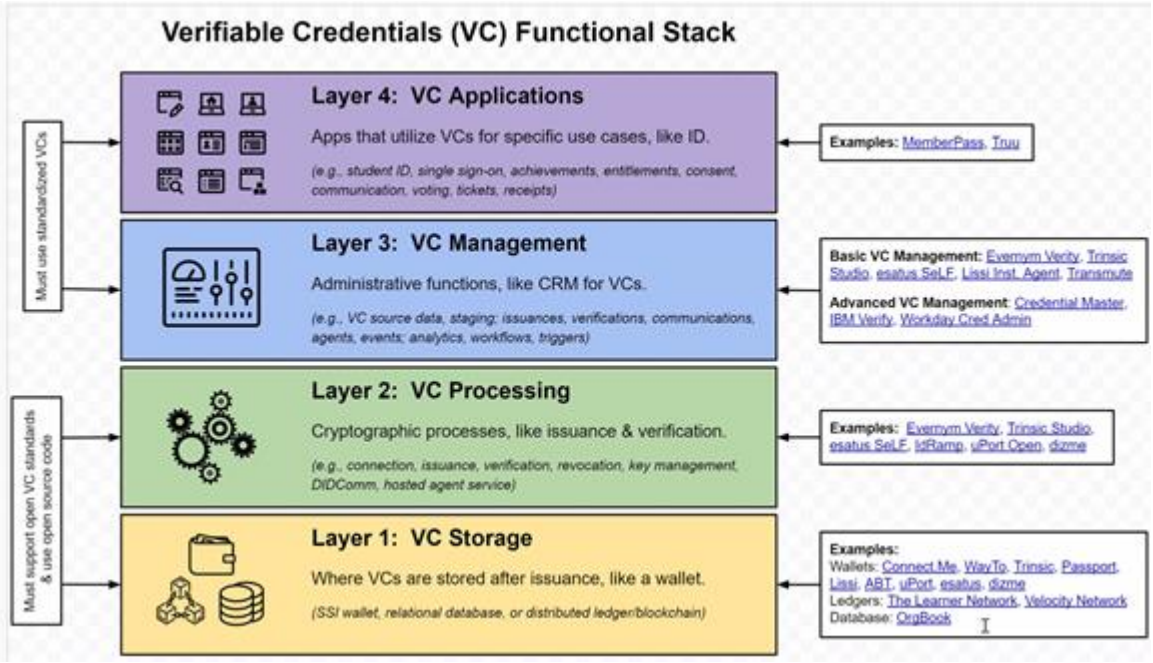
How data moves today is similar to pre-container shipping. Add verifiable credentials to the data and it becomes containerized

Prove to a lender I still have a job. The only way to do is via equavac or call previous employers. With verifiable credentials, that problem goes away.

Looking at SSI, possible places for verifiable credential storage – (all currently in play)
- Blockchain vs. KERI vs. Wallet vs. database

Individual is courier about own stuff. They can make a claim, which an employer can validate and hand that back to the user (to store in “wallet”).

The following (unlike the TOIP stack) is a VC container centric stack



There is a blog on this

Where does VC from layer 2 go – BC, DB or Wallet

Layer 3 – we are going to be awash in VCs. With performance improvements in VC processing, this will explode with thousands per person (which can be very short time frame) and millions per organization. This provides traceability of verified transactions.

What if a university id generates many VCs for all access on campus.

Verifiers can now track when a user has accessed their services

Layer 4 is where it touches users – new payment systems, voting systems, etc. all VC driven. Example – enable student to take selfy for ID purposes that becomes a VC

Managmeent of VCs MAY be simple (currently are not) and can be distributed (as well partitioned) and specialized.

What are the points for “bespoke” code vs. off-the shelf – V4 is likelyto be the most customized, lower layers more standardized (as you go down).Interoperability from 3 down is required.

Force big tech to hand stuff back to people so they can port their VCs and “stuf” to other vendors (VCs as portable model)

To be competitive at layer 4, those VCs must be portable (vs. lock in)

Connections – in layer 2, but connection management will be critical

Killer use of SSI is point to point connections to support CRM communication.

Can’t verify a credential without the connection.

Connections are created as required, but connection management (about what connections can be contructed and are validated) are critical

Idea: Credential Connection – e.g. service account at electrical supplier – supplier provides credential validated connection to the connection, which allows user to delegate use of that account to someone else.

Example of performance improvements
- KERI – issuance, verifiation
- BBS+ builds on zero knowledge proofs, which are scaleable milliseconds vs. seconds
- <undisclosed developer> revocation (formerly difficult) now simple/fast

Any area is open to disruption is when there is a data imbalance (e.g. simplification and lower transaction time/cost is a killer)

Lacking discussion in SSI space – how are you going to make mone?

Actually Tinsic sessions on SSI stat of the business are AT IIW31 (Riley Hughes chicken and egg)

Where am I going to build vs. buy.

Anticipated – wallets built into phones (alternative – cloud wallets provided with services, etc.)

Verifiable COVID-19 credentials – is a Layer 2 problem, user has to carry around the credential in a wallet and/or app?

Airlines have to verify and track all the user/s credentials – layer 3

Layer 4 – is where you have to hide all the complexity – they should NOT have to deal with the NASCAR problem.

QR interface is Layer 4

Trust Triangle for agrigulture – and how farmers fit. Farmers don’t control their data and are not at the table in discussing (so far). Farmers want it and are willing to invest. No one wants to be the first to put the baby in the car seat in the autonoumous car. So building the entire stack is a challenge as it does not exist (yet).

Can you transfer a VC. You can’t as a VC is only issued to a unique Identity (person).

While a vehicle has an independent ID, which can have VCs which are tranferable from one person to another.

A ticket is tyipcally issued only to a specific identity (say as VC), which the ticket issuer can make transferable or locked – would be an aspect of the ticket’s credential.

Identities vs. credential vs. connection – the distinction is fuzzy

Farmer use case discussion

Supply chain includes supliers distributers and processors

Farmer has to put data into the system (including personal information and economic records), with no control (vs. VC). Yet grocers have to provide traceability to the farmer for various reasons.

There are use cases.

The easy part of the problem is to envision the future state (end game and the benefits). The hard part is where to start and how to fund it. Farmer level is cooperative non-profit. Figuring out who plays what role.

Before you get to the stack – Running Lean – by Ash Maria – for taking an idea and turning into profits. Problem/Solution fit (before Problem/Market fit) and how are you going to (initiallyl) make money.

The money maker is ideally a tiny slice that pays big (saves costs or makes money for customer)

Value proposition that the client will pay for.

Has a processor that would pay for it (need to refine)

Use the “Lean Canvas”

Verifiable credentils with multiple presentations (e.g. VC contains multiple claims). Or would university issue multiple VCs per student.

No currently facility to update an existing VC once issued. Currently will have multiple credentials.

Potential for VC “set” which is a collection of related VCs.

Frustrating that the SSI adoption rate is slow.

T. Ruff has been talking about VCs for 4 years

Need to understand: VCs and Data Access/Transfer

What is new – the user owns their data and directly controls connections and use
Porting VC to IoT – in context of passive and active identifiers/crentials (was a session during this IIW

All the ingredients are there to day to secure IOT
In talking with a mortgage processor – the ability to have a persistent conection to the borrower and lender. Many potential VCs involved in a mortage broker scenario.
Could reduce mortgage processing from 1+ month to 2 weeks.
Another use case – VCs for criminal record checks for non-profits (primarily a cost at the police level in Canada).

GOOTB – get out of the building and talk to an actual customer. Threshold is a minimum of 20 customer conversations, then validate with another 20 more. THEN you can talk with the money.

Best way to fund is with revenue – pre-orders from customer is very credible

Back to MVP – minimal viable product

Credential Master – volume credential manager at layer 3, based on sales force

Chat:

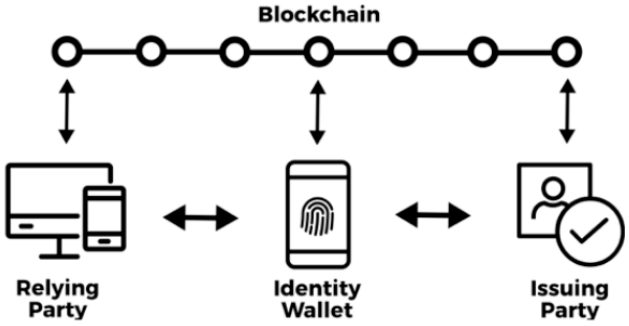
From RuffTimo : brb
From John Court : Most here in OZ just insist on seeing some recent payslips !
From Debbie Bucci : actually the ask customer to physically produce w2 for 4 weeks ... so the verifiable claim seems to align - if my employer would be able to release ...
From Debbie Bucci : yep
From Dan Robertson (he/him) : And with ZK proofs, that process can preserve privacy much better than the "here are my W2s" model we have now...
From Ashok Dhakar : When you relational database, will it allow to use NoSQL databases as well?
From John Court : Layer 1 - Physical, Layer 2 - Communications, Layer 3 - Session/Management, Layer 4 Application …..hmmm seems to follow a well known pattern
From Karen Hand : Does anyone have a ballpark idea on cost and time to implement a MVP for a simple trust triangle?
From Debbie Bucci : Revocation has alway been an issue ...
From Gabe Cohen : ZK revocations, yes
From Neil Thomson : https://medium.com/@rufftimo/verifiable-credentials-arent-credentials-they-re-containers-fab5b3ae5c0 Timo Ruff credential blog
From Neil Thomson : Riley Hughes (Trinsic) has done two sessions on SSI business Chicken and Egg @ this IIW - recorded
From John Court : I guess that makes it a Bearer VC
From Neil Thomson : Running Lean book https://www.oreilly.com/library/view/running-lean-2nd/9781449321529/
From Will Groah : Always enlightening to hear your perspective, Timothy. We are currently working a the business model aspect of converging VCs with background checks, particularly if cases where the user is paying for the background check. Interested on your quick perspective and/or perhaps offline discussion.
From Vic Cooper : https://www.albertosavoia.com/therightit.html
From Neil Thomson : Technololgy is complicated. You need to get to the point where "you can ignore the man behind the curtain"
From RuffTimo : Thanks Will!
From Karen Hand : For us, we have the relationships and reputation which is putting us in the boardrooms. Has been very important.
From Mawaki : Vic, your link doesn't seem to work.

Identity Architectures: Developing a Methodology to Evaluate Different Identity Architecture Characteristics

Thursday 22B
Convener: Todd Gehrke, Trev Harmon
Notes-taker(s): Todd Gehrke

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

Session Context
This was a working session and conversation around developing some key properties of a "good" identity architecture. The goal was to go slightly beyond the simple issuer -> holder -> verifier and represent some of the components of the system



The context of the discussion was for a Non-Enterprise setting because including integration into the backend system made the problem space too complex.

We also want to be considering system that might fit within the ID2020 Alliance Manifesto
https://id2020.org/manifesto

The focus was on Public and NGO sector use cases where there were transactional interactions.
Digital Identity Vital Signs
A set of 6 Identity System Characteristics in prioritized order. These items are derived from a much longer list, The goal is to use them as a starting point for a conversation.

Feedback:

- In the context of the underserved Population Accessibility should be higher on the list.
- It is best to not order the list. All are equally important
- Each item needs a clear definition, Security is too vague
- The meaning of all these words is key to understanding what you mean. Each one could be a 30 min or more conversation.
- Combining Transparency and Security might be enough to constitute Privacy Preserving
- James Manger : Usability
- 1. Fit for purpose. Good digital identities offer a reliable way for individuals to build trust in who they claim to be, to exercise their rights and freedoms, and/ordemonstrate their eligibility to access services.
- 2. Inclusive. Inclusive identity enable anyone who needs it to establish and use a digital identity, free from the risk of discrimination based on their identity-related data, and without facing authentication processes that exclude them.

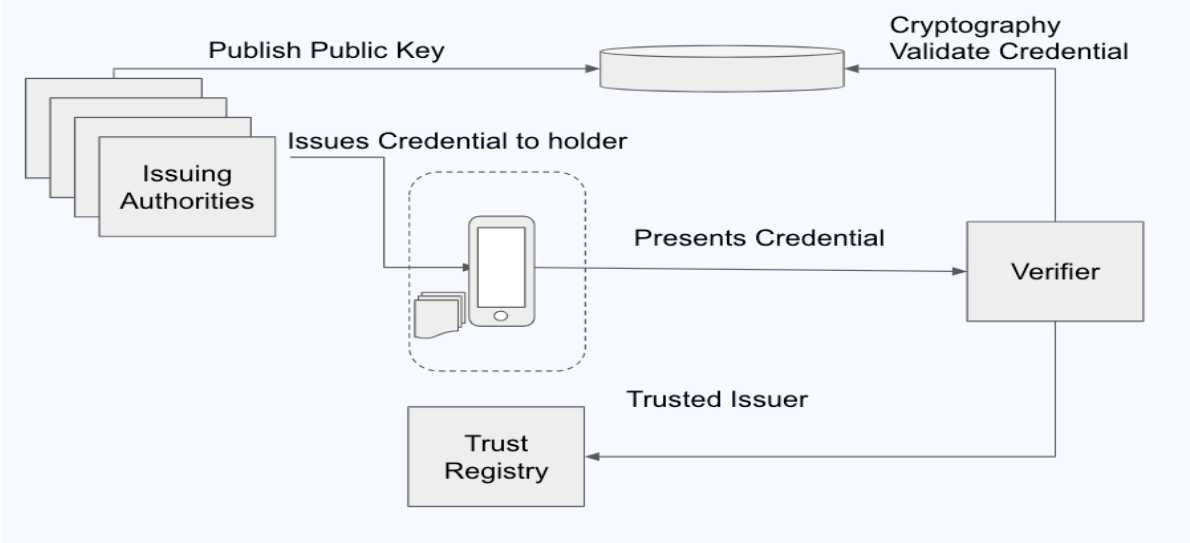
- 3. Useful. Useful digital identities offer access to a wide range of useful services and interactions and are easy to establish and use.
- 4. Offers choice. Individuals have choice when they can see how systems use their data and are able to choose what data they share for which interaction, with whom and for how long.
- 5. Secure. Security includes protecting individuals, organizations, devices and infrastructure from identity
- From John W : From one of my deck's. A slide on Privacy and Data Autonomy: A person maintains their privacy when they have the ability and power to choose what information about themselves to disclose, to whom, and for what reason. They are autonomous and have agency. When information about a person's behaviour or performance is recorded by an organization (like at work or at school), an individual's privacy is protected when they they know what information

Shared Link:
http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

Final unordered list created by the group:

- User Autonomy
- Privacy Preserving
- Interoperability & Portability
- Security (Anti-Honeypot)
- Population Accessibility
- Transparency
- Usability

Example architecture 1
The goal of this diagram is to represent multiple issues that issue credentials to a users handset. This is intended to be a starting point, or ideal architecture. We are disregarding fundamental elements such as guardianship and the details of backup and recovery. . .

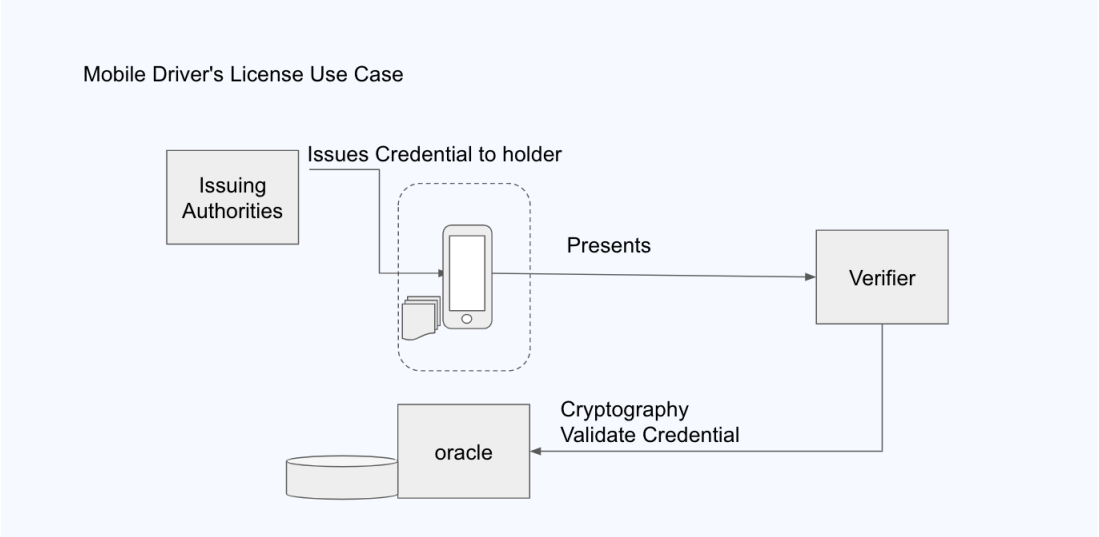


Feedback:

- The diagram doesn't show a user (it is implied by the handset)
- The architecture diagram itself doesn't tell us enough.
- We need to talk within the context of specific uses cases
- We need to talk about both the what and the how

- Public key and cryptography are part of the how and don't belong on the diagram.
- An example of a challenge, here, is that User Control is essential, but has to be balanced against User Burden. (For typical uses of the term Usability, it is actually an additional, separate concern)
- How is Trust Registry different from the 'Publish Public Key' repository? The trust registry is the list of issuing authorities the verifier will respect. Could be included as part of the verifier . . .

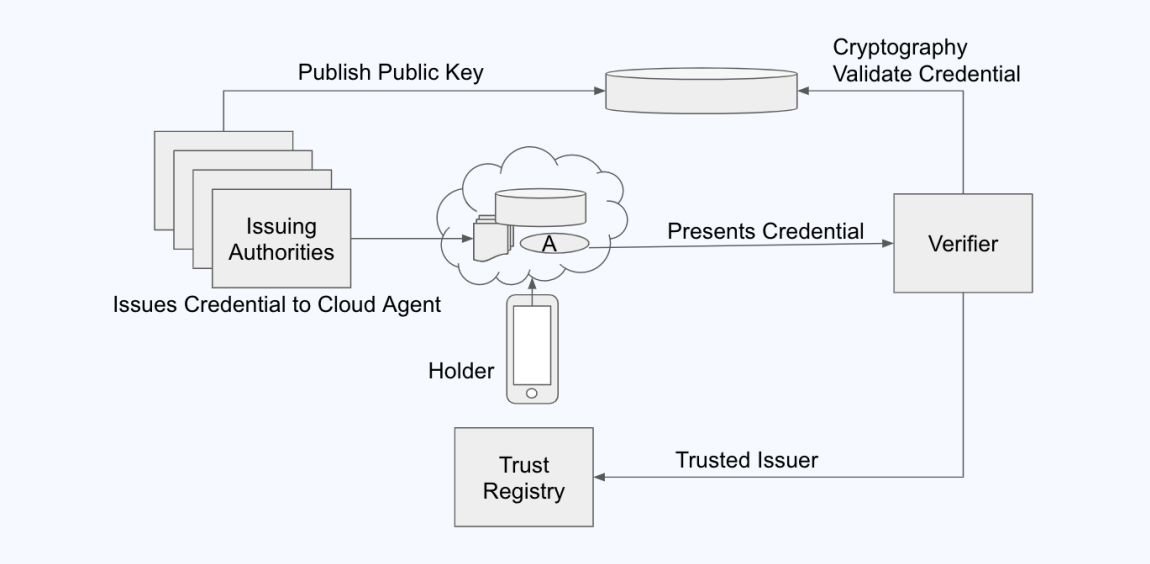
Example architecture 2
This is an example drawn from Mobile Drivers License Initiative and a presentation given by John Wunderlich (Kantara)
https://www.securetechalliance.org/mobile-drivers-license-initiative/



Feedback:
- Overall the group thought this was an inadequate architecture because of the "phone home" component.
- The use of an oracle to validate the cradentail doesn't remove the fact that there is tracing going on even though it's not the same as going back to the original issuing authority.
- Dan B pointed out that this is like the approach that is much like the pattern used in Estonia e-Residency program. Using a single government issuer but a decentralized network of verifiers.

Example architecture 3

Credentials held on a cloud agent owned by the holder. User owns and provisions infrastructure provisioned in thor cloud account.

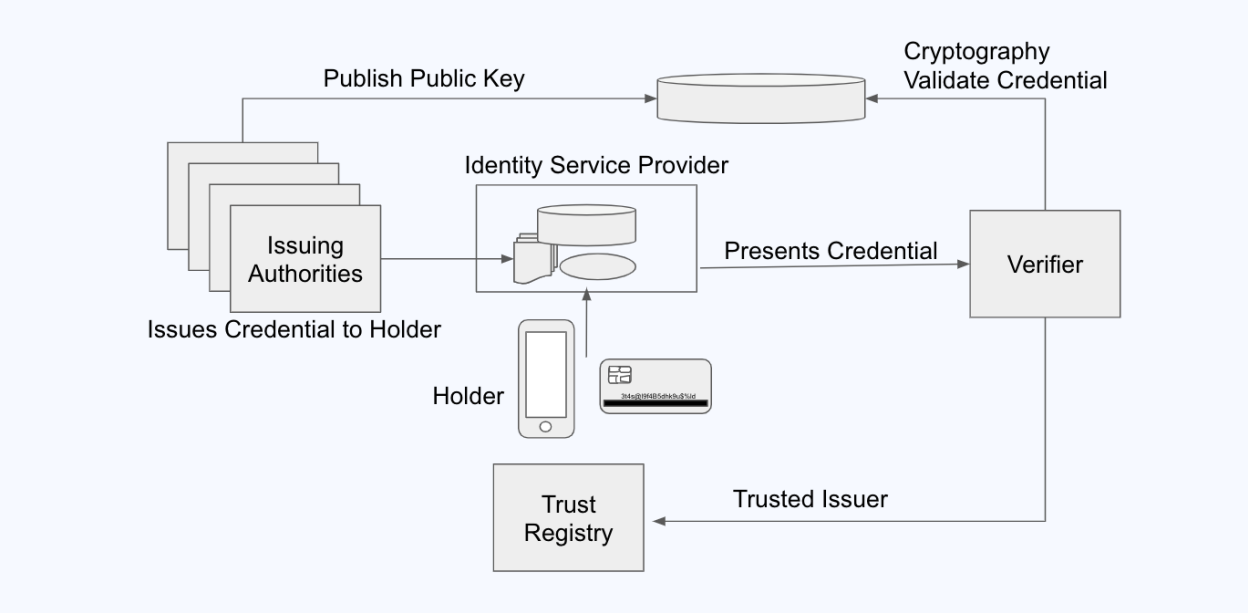


Feedback:

- Group was OK with this, didn't have a lot of feedback.

Example architecture 4

Identity provider, government or private company, provides Identity as a service. Holder has control of credentials but may not have control of the infrastructure hosting the agent and storage services.



Feedback:

- Although this is likely to be the most common model the group did not feel this was a good architecture.

SSI + Confidential Storage + Tapestry Credentials for Proof of Occupancy (Encore Wed)

Thursday 22C
Convener: Dmitri Zagidulin, Liam Broza
Notes-taker(s): Liam Broza

Tags for the session - technology discussed/ideas considered:
SSI, Confidential Storage, Tapestry Credentials, LifeScope

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

Presentation
https://docs.google.com/presentation/d/1bwOMI5mB-mL6sKkj86-iXFdePaPlsfJpdoLTdRzROFE/edit#slide=id.p

Yuliya Panfil
Senior Fellow and Director, Future of Property Rights, New America
panfil@newamerica.org

Liam Broza
Data Architect, LifeScope Labs
liam@lifescope.io

Dmitri Zagidulin
Data Architect, Privacy/Trust/Storage, LifeScope Labs
dmitri@lifescope.io

1 Page Summary
https://drive.google.com/file/d/1_IvefA7lYJpAe1PRpIjtUCWQH63GvIjs/view?usp=sharing

Abridged Paper
https://docs.google.com/document/d/15pUIUKTa81rAhtYNCK9EO_KisNgijGXiW1Sk1WAGtVo/edit?usp=sharing

Discussed:
- Some overlap with formally proving ownership in the majority (AKA developing) world.
- Even though those places are low-capacity WRT electronics, there are satellite images and service providers who are willing to give data; this will usually require humanitarian assistants, though, eg. when it comes to vetting truth.
- There are minority (AKA developed) world issues too: wildfires have been burning homes (eg. Paradise CA fire), older people lose their memories for recovery (eg. a story in someone's family), keys get lost
- Let's gamify the goal of data restoration/protection.

UX for SSI - Applying Design Principles to SSI

Thursday 22D
Convener: Josh Welty
Notes-taker(s): Josh Welty

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

High Level Brainstorm: Problems and Ideals with verifiable credential interactions

Problem:
Language of SSI - a barrier to understand
"presentation" - everyday user doesn't know what that means
"connection" - persistent?
Management/organization of credentials
making sense of how connections and credentials interact
Users don't care about connections
Why do I need to engage with the wallet at all? Why do I need to leave my workflow to use a separate wallet?
Selling the benefits of using a wallet -
Ethical mission of SSI - is it obvious enough to encourage users to use SSI (do we want to rely on the user to care?)
Ideal:
Interface would have the next step in the workflow obvious - only show things that make sense in that context.
We have to think of the user's workflow and build around that
Maybe not letting them know they're using a wallet?
Familiar questions, not jargon (when sending information)
Workflow opens the wallet - I don't know it's a wallet, my credentials work for me in the background
As much control/information as the user would like

Self Sovereign Progressive Web Apps

Thursday 22E
Convener: Adrian Gropper
Notes-taker(s):

Tags for the session - technology discussed/ideas considered: PWA, Intel SGX

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

The Save Chat failed. Let's hope the Zoom recording has the chat to save.

- Monopolistic Platforms
- PWA contribution to User eXperienc
- SIOP Recap by Oliver Terbu as CoChair of DIDComm
- Browser-Based Agents may be required by Info Sec managers
- PWAs might be easier to sell if each 3-letter agency could serve their own.
- Zero Trust Architecture can be explained as "Always Verify"
- SSI needs to blend with COTS - standards may not be enough
- Sell PWA as distributing risk - The App Store model is too centralized

KERI Roadmap (and how to contribute)

Thursday 22F
Convener: Sam Smith
Notes-taker(s): Ajay Jadhav

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

https://didme.me/did:meme:1zgs8suu9h3sjfx9cl2c0pf279wk76yy8z7zwuzxwvvcurtaxc5pyj4qt76hnq

https://keri.one
https://www.github.com/decentralized-identity/keri/

IIW! - Oct20-22 (Tu-Th)

- Intros
  - Dave Huseby - Security Maven still? - COME ON IN, THE WATER'S FINE!
    - Crate builder?
  - Joachim (Jolocom) - contributes to admin/positioning/comms roadmap items
  - Charles (Jolocom) - Github contributions welcome (primary editor of /keriox repo)
  - Joel Hartshorn - USAid dev eng - identity first, then blockchain, then identity
  - Micheal Shea - stalking KERI for a while - happy to try to help with writing and business -
    - Use cases! PARTIC IOT
    - There's already an issue open!
  - Michal (HCF) - /keriox contributor and also working on TDA
  - Robert (HCF)
  - Shivam (Spherity) - /kerijs primary contributor
  - Steve Todd (independent) - enthusiast! Jive co-founder, knows Sam from them
    - Been working on a Java implementation JKeriLOL

    - Ajay Jadhav (AyanWorks) - interested in ledgerless
        - WASM? or Node.JS?
            - Charles: React Native and Node.JS aren't the best API; we prefer/recommend WASM wrapper from our experience
        - Deno.land? Consumes rust library and TS directly
        - Charles: Git issues for advice on ergonomics, aesthetics etc of Rust APIs welcome!
    - John Walker (ToIP DSWG & CCI) - Semantic Web first, identity second; PHI focus; I'm just here to understand the roadmap and see where I can contribute down the road
    - Mark Lizar (ToIP DSWG; Kantara; etc) - Notice and Consent as EVENT/signature log -
        - Sam: Georgia Law review paper on consent chaining
        - Mark: ISO crossborder consent paperwork (but begs the question of crossborder metadata-trackable identity)
        - Sam: Forensic compliance/auditability versus interactive crypto; automatic/passive signatures require less laws and regs to change
        - Mark: International law transfer use cases; consent ←→ surveillance is a hard circle to square without portable/standardized consent receipt semantics; we are working on
        - Sam: Verifiable credential proves authenticity, not veracity (doesn't line up well to legal concepts)
        - Mark: Event key logs are what we need to fit to legal frameworks from CA era - don't want to skip that step!
        - Unified data control vocabulary (another ToIP project)
- Roadmap Report-out (on-cam)
    - Joachim: development and other functions in parallel (spec writing and implementation guidance as well as marketing/positioning)
        - Messaging / FAQs:
    - Robert: Align with other communities? How to be more open to other communities or prevent reduplicated efforts? Provide the library for AcaPy?
    - Implementations (Py & Ox first)
        - Last two event types
            - Delegating rotation and interaction events - different verification process, involved delegation seal
            - Delegated inception and rotation events- different verification process
        - Witness library
            - Witnessing logic for KAACE
            - Validator (depends on ^)
            - Watcher logic/calls
        - Networking (HTTP & UDP still pending)
            - Ajay: gRPC between two KERI agents? More bidirectional streaming options?
            - Sam: WebSockets (TCP tunnel); that can be added later for adoption purposes, *but* not necessary for core spec;
            - Sam: I'm more interested in standardizing APIs first
            - Steve: HTTP has lots of infrastructure
        - Recovery
        - Discoverability mechanism - for finding and getting the log anytime you have the [*current? Or also historical?*] key
            - Simpler version: Out-of-band / IP discoverability

        - Kademlia DHT - publication (equivalent of did resolution mechanism?) digest of service endpoint
        - Ledger-based discovery for DID world
            - Charles: as many as possible :D
        - Cname: KERL:: A : discoverability mechanism
        - Witness API → Service endpoints that can be queried multiple ways
            - Robert: How do you get the service endpoint from an ID if that's all you have? <20 minutes follow>
- Proposed Action Items (within the WG)
    - Charter of new WG
        - Scope should include independent discovery mechanism (will be separately donated)
            - But out of scope of core spec
        - Scope should include at least one popular ledger-based discovery mechanism (ideally today's Indy)
            - But out of scope of core spec
        - Credential master issuance middleware/containers ; "Processing layer" (//Trinsic and Evernym's DID issuance APIs); a KERI ID issuance API seems like the next step for scaling infrastructure and aaS models
            - But out of scope of core spec
        - Reference wallet
            - 1: Universal wallet spec + Keri libraries from Jolo wallet → https://github.com/jolocom/rust-multi-target
        - SemVer protocoling (major and minor have to align for trust)
    - Update Py demo (lessons learned from demo)
        - Console options
        - Verbose error methods (debugging mode)
    - Curves needed for 1st release
        - secP256k1 helps with NIST compliance
        - DAVID: SEND ME A DELTA OF THE CURVES YOU NEED IN URSA
    - Workshops on architecture mapping in WG (for documentation parallel efforts)
    - Integrate KeriPy to AcaPy (or maybe KeriOX, with appropriate wrapper, for AriesJS)
        - Issuing VCs against KERI IDs
        - Michal: Indy is Rust-friendly
    - Mark Lizar: Use case pull request on international law transfer use cases or ISO informed consent receipt standards?
    - AriesJS - separate item, if AyanWorks or other AriesJS volunteers help-- Spherity not the best for this :D
    - Adoption within DID Community
        - Drummond & Indy Inter-op-athon: new namespace hierarchy for next V of did:indy (and Drummond is onboard to incorporate DID:Un/KERI)
            - DID:Indy:FINDY/etc:*KERI* - sub namespace
            - "DID: <keriID>" might require some more substantial lifting in W3C
        - Deadline? As yet unknown; DID Core Spec reaches Recommendation when? (2yr charter ends Sept 2021)

Call for Asia Pacific Collaboration in Healthcare, Education and Public Sector Use Applications

Thursday 22G
Convener: Apichet Bhusry-Finema
Notes-taker(s): Catherine Nabbala

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

Most players are looking for use-cases, standards, what is the benefit?

Finema has built projects in Thailand.

Thailand is the second country to issue a VC standard.

Currrent interaction needs (volume and types)
Verified information chains

Decreases entropy of identity to receive multiple signals of identity from independent sources
Challenge is the coordination of sources attesting to identity attributes
Standards of technology and business, operation, law, technology and society/culture/ (BOLTS) will need to reduce interaction costs of delivery of infinite factor identification
Transition of reliance on signals

Dee Hock Birth of Chaordic Age
Original issue discount is a form of interest
Equity versus debt distinguished by level of “participation.
Common Bond of credit unions was based on protestantand catholic support organizations.
1850s Germany credit union birth

Shake - shake@finema.co

Deep dive in this SSI 1st level support issue: Follow-up from Session 20E (Conversation with the future users of your products or services/Don't let 1st level support be the wrecking ball for your customer relationship - How to do it right in an SSI world)

Thursday 22l
Convener: Andre Kudra
Notes-taker(s): Andre Kudra

Tags for the session - technology discussed/ideas considered:
Customer Support in SSI, Interwoven Product & Service Landscape

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

Jacob: Good customer support is possible! It is a cultural thing. Identify: Is it a technology issue or is it a cultural issue.
Johannes: Who is responsible in the first place? Wallet provider?
Andre: Users will call whomever they think of first.
Jacob: Solve problems in underlying platform and investigate in open source stack if necessary. Immediate follow-up with calling back people and owning a problem with possibility to pull right people in. Establish company policy to make investigations possible right away in urgent matters.
Andre: Make man-hours of skilled developers available for support.
Jacob: Needs to be made a priority if it is really meant seriously by the org. Requires making developer man-hours available for support.
Jacob: Give authorization to support agents to investigate on device.
Andre: Interwoven SSI product and service landscape may prohibit in-depth investigation by one of the customer supports.
Mawaki: Multiple components involved
Jacob: Reproducibility is key. Is it on my stack? Or some elses?
Jacob: Report issues across stacks to a common issue / problem report space, for the community. Would work in the interwoven SSI space. Could work in the SSI community!

From earlier session:
Take-aways for 1st level support for vendors/product makers/service providers:

- We need to elevate customers in status. Instead of “user” maybe “owner” or “associate” or “groupie” or “fan” even
- Carefully designing support scripts intended to provide better understanding of the user persona - advice/escalate/help as appropriate

Questions for 1st level support in an SSI world:

- Call center plan?
- Know-how about key management
- Technology available to end users
- Integration with existing support technology / portals
- Legislation for consumer protection?
- Who do you want / need between you and your customer?

Offline input from Sankarshan:

- the availability of internationalization/i18n for the customer facing software components enhances the ability of the customer and the support team (if well trained) to identify and explain issues; triage and resolve issues. As an example, in India where there are many official languages, the policy often mandates English+a set of languages
- to Karl's point about scripts for supporting customers, there is a need to also see if self-service can be enabled for a class of errors or flaws being reported
- build the product development cycle to manage product releases addressing the more invasive defects on priority - reduces the load on L1 from the "that same darned issue again"
- if it is possible, L1 representation during product readiness prior to release/GA

Work Session: did:indy DID Method Spec-athon

Thursday 22J
Convener: Stephen Curran
Notes-taker(s): Stephen Curran

Tags for the session - technology discussed/ideas considered:
Topics Covered: Moving forward the specification of the new "did:indy" DID Method.

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

- Presentation: http://bit.ly/DIDIndyIIWXXXI
- DID Method Draft: https://hackmd.io/@icZC4epNSnqBbYE0hJYseA/S1eUS2BQw

Notes collecting from the session as we went through the topics:

Documenting the DID Method -- ReSpec or SpecUp? No decision, we'll experiment with both and select one. For now, we'll work on the hackmd.io document.

Defining the <network> element of the DID Doc:

- Initial: like to use the first 5 characters of the hash of the genesis file
  - Problem: over time, the genesis file (which is inappropriately named) will change as it must contain IP and ports of nodes of the network. Over time, the original nodes will no doubt disappear.
  - Want to be able to fork a network and have a new network ID for the forked network.
- Other ideas:
  - (Somehow) Add hash of previous genesis file version to new version to create a chain.
  - Add hash of initial genesis file as a transaction to the config ledger to enable verifying the ledger.
  - Look into what the Trustbloc is doing, including the use of an alias name for the ledger.

Finding the ledger from a DID URI:

- No consensus was found, and not a lot of time was spent discussing.
- From the Indy Interop-athon, the idea was to just use configuration vs. some discovery mechanism embedded in the DID. That configuration could be stored by each agent, or a shared service could be developed to enable lookup from DID to ledger location (which is really genesis file location).

Supporting DIDs and DIDDocs using Indy NYMs and ATTRIBs

- Basic consensus reached on how to do this -- the details to be defined.
- Use Indy config and permissions to manage creation of NYM and ATTRIB
- NYM contains the local network identifier for the DID and a verkey to enable control over updating the NYM and adding/updating the ATTRIB.
- An ATTRIB of type DIDDoc contains the entire DIDDoc for the DID.
- If there is no ATTRIB of type DIDDoc, the NYM and verkey must be processed much like did:key handling to produce a DIDDoc by a resolver. Details of "much like" to be specified.
- If there is an ATTRIB of type DIDDoc, the latest version of that is to be returned as the DIDDoc by a resolver.
- The verkey of the NYM is NOT implicitly part of the DIDDoc. If the controller of the DID wants it in the DIDDoc, it must add it to the DIDDoc before writing the ATTRIB of type DIDDoc.

Specifying versions of DIDDocs

- The existing TxnID generated by Indy for the DIDDoc ATTRIB (or the NYM if there is no DIDDoc ATTRIB) will be used as the version-id as documented by the DIDDoc.
- TBD is whether a resolver (and what resolver -- internal or external to indy-node) will supplement the DIDDoc with the TxnID of the DIDDoc on resolution.

Supporting version-id and version-time

- Indexing of TxnID is already being done by Indy, so returning a DID by version-id using TxnID as the version is already supported.
- Indexing of Txns by time and related NYMs will need to be added to Indy to support version-time resolution support.

Supporting ledger objects as DIDs

- The DID Spec may or may not support "type" as an attribute of a DID
- Other Indy ledger objects should be able to be supported by adding an @context to the DID Document for the type, and adding the details about the object into the DID object.
- Indy-node processing may be needed if specially ledger-levelling handling of ledger objects is needed -- e.g. the ledger "knowing" that an object is a "schema" and hence handled in some special way. It's not clear that is needed.

Next Steps

- It was agreed that the next discussion of the Indy DID Method would occur at the next Hyperledger Indy Contributors meeting and at that time, a regular meeting to evolve the spec would be planned and contributors added.

Session Title: not-so-smart wallets

Thursday 22K
Convener: Kim Hamilton Duffy, Orie Steele, Darrell O'Donnell
Notes-taker(s): Kim Hamilton

Tags for the session - technology discussed/ideas considered:
wallets, agents, dids

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:
Context (Kim's presentation)

- Goal: Tease apart wallet-related concepts
- Based on CCG's survey of wallets
- Highlights (see slides)
    - DIF Glossary report
        - the relationships are interesting
    - Darrell O'Donnell's wallet report
        - tease apart wallets vs agents and also minimum viable wallet
        - his wallet definition matches DIF glossary definition
        - Stuff as a proper noun
- Question: is a wallet hot, dumb, secure storage? What are we missing?
- Reviewing Darrell O'Donnell's minimum viable wallet
- Why do we care? universal wallet interop spec -- what goes in there?
- Maybe there is some awareness of entities it's connected to when we talk about "wallet". Tease apart what these concepts are.

Discussion:

- Sam: What's missing from this presentation is that many wallet designs have crypto happening in the wallet.
    - Discourage devs from doing stupid things with keys
- Wallet and public-facing abilities
    - Keith: Portfolio/credential management is a wallet feature in workday wallet
    - Orie: Conceptual mismatch about wallet exposing publicly shareable info. Are we exposing an interface that shouldn't be exposed?
    - Keith: wallet helps manage
    - Kim: The way we talk about wallets in LER space is different. More like portfolios.
    - Matthew: There may be a central location for storing / curating data, then I can publish/curate data, and authorize access through some agent protocol. Publish in some way that they can either access immediately or access via an endpoint. Managing access to data via some policy (wallet controls or public)
- Discussion about trust model
    - Bart: things at edge need to be zero trust. What if you as an issuer have certain security requirements of a wallet? What if I spoof a capability I don't have?
    - Orie: Apple -- apis expose certificate chain to prove claim is signed from root. e.g. if I make a claim about a key being hardware protected
    - Darrell: accreditation and certification. Can I trust Bubba's wallet? Other concern is backup and recovery

    - Bart: Physical wallet -- different paradigm. Stuff inside wallet is secure, but not the wallet itself. Gap: digital wallet is supposed to "do" something -- sign presentation, do crypto. We should focus on that tiny gap, trust minimize the wallet. (rather than accreditation -- less scalable)
    - Tyler: placing trust on wallet misses the mark
    - Darrell: reality is putting things in/pulling things out. We have to figure out what I truly control. We need to tease apart what wallet actually does.
- Corollaries to physical wallet:
    - Sam: worth teasing out some aspects. Curious about corollaries to physical wallet. Contents of physical wallet can be swiped.
    - Darrell:
        - Suppose I held a credential, but I lost the wallet. Important that there was a record that I got it. Backup and recovery is critical.
        - Name of digital wallet -- I wish we had a better name. I can't draw a crisp line
        - Issues like authorizing access (automatically) for health provider.
            - If it's my doctor, part of health system, and normal query
                - don't want doctor to have to ping me every time.
            - law enforcement: DL - sure
        - bar: DL - no, and maybe notify authorities
        - Some stuff is irrecoverable. Bearer asset that only exists in my wallet (e.g. cash) -- that scares the most.
    - tmarkovski: wallet importing/exporting goes along with. Interested in practical problems that can only exist in one instance and cannot be duplicated
- Recovery as an attack vector
    - Darrell: recovery vector becomes the attack vector
    - Tyler:
        - Tying recovery to biometric provider. for providers that do biometrics right.
        - Wallet by itself is not enough
    - Sam:
        - I prefer social recovery, m of n recovery
        - I don't have a good handle on: if keys were in secure element and I lose that phone in the ocean, how do I get it on a new one. How do we mechanically do that?
- Key management feasibility
    - Keith: a lot of individuals aren't prepared to do key mgmt. When they lost control, they became upset that they lost access to their credentials and had to be re-issued. Moved to custodial.
    - Darrell: there are ppl that won't manage keys; e.g. if they are targets (known to carry a lot of crypto)
- Different recovery modes
    - Orie:
        - data model - structured json: keys, entropy, metadata, credentials, author caps, etc
        - 2 scenarios for recovery:
            - locking and printing it out (single wallet, lock, save it to dropbox, etc)
            - sync to external service, e.g. secure data storage
    - Rouven: separate recovery and backup
    - Sam:
        - Difference between data being stored and software libraries used to prevent bad behavior

        - Don't think it's important that there's standardization of the libraries. More useful to have standardization of core data. Ability to take core data and stick it somewhere else is valuable. Move to another wallet, import it in a future version of the same, More important than hiding behind API.
        - Separately, Promoting good architecture to avoid bad key use
        - One about interop, other about preventing bad developer behavior
    - Keith: mobile vs web -- accessibility
- Separation of concerns
    - Darrell: didn't need credentials for many actions when we already had dids. sending messages "do you approve transfer?" crypto sign using did. Crypto lives in wallet
    - Rouven: split wallets conceptually
        - secure thing in OS, holds some keys
        - many different applications that access or wallet OS level??
    - Orie:
        - browsers have software isolated key caps
        - progressive web app with dongle
        - metamask (trezor, etc)
        - sometimes intfc isnt' handled by wallet itself. wallet is way to ask for a signature, or to trezor to have a signature.
        - Ask for signature for wallet and have it only mean there's plaintext keys in wallet. Against security practice of teasing apart.
        - What's in a wallet vs capabilities
- Dumb wallets
    - Discussed Bart's claim that wallet is dumbest, lowest security thing that's useful
    - Orie: from security perspective, prefer non-extractable private keys. want hardware/software isolation. but for variety of reasons we can't get it. plaintext private keys. if you can afford to have hw/sw isolated and store capabilities in wallet, good. But there are cases where you can't do it or locked out of modern crypto (don't have hardware support)
- Central vs distributed management of keys/devices
    - Rouven: central dashboard to manage devices, keys, revocation, etc. Is that mobile wallet?
    - Sam: responsibility of devices. circle, quorum of devices. Can't be one thing. Dont' like centralized service
    - Orie: trust graph
    - Rouven: Centralize logic / rules, run smart contract
    - Darrell: 737 cockpit
    - Orie: contract locks away token
    - Brent: skynet no kill switch
- Context-aware
    - Orie:
        - Wallets have to be flexible to support security context relevant to ppl and businesses
        - different security properties, but speak about in same ontology
        - a way of relating security props of 1 system with another

ACA-Pico: make your own Aries Cloud Agent

Thursday 22L
Convener: Bruce Conrad
Notes-taker(s): convener and volunteers (name yourselves, please)

Tags for the session - technology discussed/ideas considered:
Picos, Aries agents, Manifold, ACA-Pico

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

Those in attendance are invited to follow these steps to make their own Aries Cloud Agent using ACA-Pico.

1. Sign in to manifold.picolabs.io
2. Click on "+ Add Thing" (near upper-right corner)
3. Provide a name for your new thing, then click "Create Thing"
4. Notice a card representing your new thing (can be moved around)
5. Click on the gear (near upper-right corner of the card)
6. In the popup menu, click on "Install an App"
7. Select the ruleset named "io.picolabs.manifold_cloud_agent" then click "Install it"
8. Notice the app is represented by the Aries logo at the bottom of the card
9. Click on the Aries logo/button
10. Click on "Enable Connections"
11. Notice that an "Action" button appears
12. But first, click on "Open Card" (a doorway icon near the gear) to have more room
13. Connect with other people in the session by sharing invitations out of band

Help, comments, and explanations will be offered while this is being done.

I'm open to a deep dive afterwards, and any who wish to leave with their Aries Cloud Agents may do so.

Five or six people attended, and most or almost all of them created an Aries Cloud Agent using Manifold (an "agency" as Dev pointed out) with it's point and click interaction.

Many questions were asked (and answered) as we dove deeper into the architecture of Manifold and picos. We at Pico Labs are always delighted to provide this kind of guided tour through our open source code. We also welcome pull requests as you see improvements.

Many thanks to all who participated in this session!

Readers who find these session notes in the conference proceedings are hereby invited to acquire their own Aries Cloud Agent by following the 12 steps above. When you have questions, please feel free to email bruce_conrad@byu.edu for answers and/or guidance.

An Open-Source SDK Approach To Build A Mobile Wallet

Thursday 22N
Convener: Horacio Nunez
Notes-taker(s): Horacio Nunez

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

This session had an objective to connect with the community to review the fundamental needs of people starting mobile wallets and share how some of the components we are open sourcing on Kiva Protocol may help.

We did this session 3 times and in every instance we polish the list of fundamental needs. The final list could be seen below in that endeavour.

An Open-Source SDK Approach To Build a Mobile Wallet

From the time you download this sdk wallet code, you have full feedback loop to experiment with SSI.

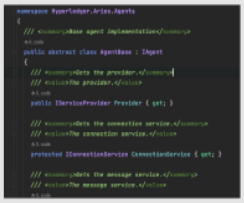
Provide a basic implementation for handling connections, credentials and proofs.

Suite of UI Components that use WPF template to user all community members don't need to create basic components all the time like: credential, attribute.

Small suite of UI Components that can expose credential/connection metadata to use in debug time.

Support more than one framework for Dependency Injection.

```
Horacio Nunez *
public class DefaultAgent : AgentBase
{
    Horacio Nunez *
    public DefaultAgent(IServiceProvider provider) : base(provider)
    {
        Console.WriteLine("Mikoba in da House");
    }

    /// <summary>
    /// Configures the handlers.
    /// </summary>
    Horacio Nunez
    protected override void ConfigureHandlers()
    {
        try
        {
            this.Handlers.Add( item: new MikobaCredentialHandler());
            this.Handlers.Add( item: new MikobaProofHandler());
            base.AddConnectionHandler();
            base.AddDiscoveryHandler();
            base.AddBasicMessageHandler();
            base.AddForwardHandler();
            base.AddTrustPingHandler();

        }
        catch (Exception ex)
        {
            Console.Write(ex.Message);
        }
    }
}
```



Burning Man 2020 - When Private Behavior Goes Quite Public

Thursday 23B
Convener: Jeff Orgel
Notes-taker(s):

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

The virtualization of a 70,000-attendee event that has manifested in the Black Rock Desert of Nevada threw the ceremony's ethics, boundaries, limits and norms into a reconfiguration. For the first time, the event came out to its community in their personal spaces.

How did the displacement of a real event fall into the helping hands of technology so this community could gather like never before. Physically, monetarily and time and distanced challenged could now hop over those obstacles for a somewhat realistic – but not real – version of the experience.

Specs:

I spent 80-90 hours on "the playa".

Visited 107 venues (not all populated upon my visit with…anyone or thing… 20% empty)

Blocked all normal media feeds and radio and only listened to the BMIR station and/or Shoutingfire.com, both directly associated with the immersion of the event.

there are observations as to how a space of behavior which holds sacred the "off line" (literally no internet for 9 days when it really happens in the desert)

What translated well?

- Being together at all
- Sharing stories and smiles and music
- art installations
- Tracking the experience via medallions and leaving messages in chats
- …etc., etc., …

What did not translate well?

- Gifting and sharing between individuals
- Feeding each other
- 1st person experiences at music,
- Physical intimacy with strangers
- The discomfort, life was too easy comparatively

Noted by Kyle (I believe) roughly: Things born of Real World translate rather well sometimes. Do things born of digital translate into Real World well?

SSI, Privacy and the disinformation ecosystem

Thursday 23E
Convener: Bill Aal
Notes-taker(s): Bill Aal (for more extensive notes, contact waal@toolsfochange.org)

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

Difference between what people consider traceability/attribution as a good thing for transparency and combating disinformation and people's security.and it has also a potential for being weaponized.

This was a wide ranging conversation discussion that revolved around the difference between the lived experiences of people of color, women and other people who are targets of oppression,and those of the people making policy and technology decisions.

Another part of the conversation was about the difference between manipulation by use of social graphs and " persuasion". Can SSI give us protection against manipulation? Or do the neuro-behavioral drivers of the technology over ride the old models that people operate as "rational" actors.

We also talked about "saviorism" as a theme in US culture and how it has been a driving force in the tech sector,thinking that the mainly white technological class can build tools and ecosystems that will fix the problems of society, when in fact they and the tools are part of the oppressive system.
Coming around to privacy again:"You can't decontextualize privacy."

The framework of privilege embedded in "Freedom of Speech" keeps white male technologists immune to change and people who are talking about the reality of their experience are made into "bad people"

In changing the way the narrative,
Its not just how things are said, but how things are heard. Those with privilege have got to give up their belief and stance that there is an " objective" knowledge that comes from white middle and upper class education and scholarship:

The conversation ended with both a call for white folks especially men both listen to "other" voices but as im analysis of things.

White technology and policy people need to take on the work of educating themselves (I am included in that of course!) and others about the ways in which privilege and oppression keep them in control. More than that to build into the daily business practices ways to learn and to interrupt those patterns.

There was a call to create a working group to work toward a different narrative around technology especially the identity ecosystem. Contact Bill Aal to be involved. (waal@toolsforchange.org)

This might be connected to the work of Drummond, Kaliya and others discussed in Session 24.

Explore Personal Data Collection - LifeScope Digital Memory (Encore Thurs)

Thursday 23F
Convener: Liam Broza, Dmitri Zagidulin
Notes-taker(s): Liam Broza

Tags for the session - technology discussed/ideas considered:
LifeScope, SSI, OAuth, Solid, DID

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

Presentation

- https://docs.google.com/presentation/d/17gyhrpX24PuAiDMD3Cub1W2nP5OT9NckC6RwuSyCL0s/edit?usp=sharing
- Lifescope.io
- lifescope.io/xr

Action Items

- Partners
- Use Cases
- Technology
- (Identity, Collection, Storage, Encryption)

Liam Broza
Data Architect, LifeScope Labs
liam@lifescope.io

Dmitri Zagidulin
Data Architect, Privacy/Trust/Storage, LifeScope Labs
dmitri@lifescope.io

Discovery: Solving the Kobayashi Maru of SSI

Thursday 23G
Convener: Daniel Hardman (daniel.hardman@evernym.com)
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:
#discovery, #ssi, #privacy, #agents, #tor, #mediation, #data-ownership, #regulation

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

How to allow discovery of personal information without running afoul of privacy, regulation, consent problems, and so forth is a conundrum in the context of SSI. We seem to have an unsolvable problem.

One way to address the tension is to change the rules. An important way to do this is to begin thinking of discovery as a collaborative effort that requires active participation of both parties (the party wanting to find, and the party wanting to be found). This is how Tinder works; both parties have to swipe right before any connection can be made. We could apply this same concept to discovery of DIDs or any other SSI data, such that a party wishing to be found is not looked up in an index, but rather is found by querying them directly. A decentralized matching service for discovery can be built that has cool properties that we haven't previously imagined.

Slides are here: https://j.mp/3obLky1

Paper with more technical details about the concepts: http://j.mp/ppred-paper

Chat transcript
From Neil Thomson : No good deed goes unpunished...
From Nathan_George : The Loan Officer Protocol needs to make it into the notes
From John Court : Isn't Catch22 the original version of all these things ? "a paradoxical situation from which an individual cannot escape because of contradictory rules or limitations. The term was coined by Joseph Heller, who used it in his 1961 novel Catch-22."
From RuffTimo : Love Star Trek. Brings back great memories. :)
From windley : This is a good idea for some of the chat spaces. We could just stream Star Trek in them. :)
From John Court : He cheated
From Jacob Siebach : There is a great clip from the game Star Fleet Academy where you can hack the simulator and the Klingons treat you well. Extremely funny.
From RuffTimo : Love IIW! Never know what you're gonna experience. :)
From Alan Karp : pre-Covid
From Ken Adler : If this was in Philipedlphia… I'm in the picture
From Jacob Siebach : "Please state the nature of the medical emergency."
From Nader Helmy : I think the example applies to any makeshift community
From Orie Steele : Resistance is futile
From RuffTimo : ^^ Perfect. :)
From Gabe Cohen : Or even worse…a PhD
From Bob Wyman : Being a doctor doesn't ensure your willingness to help. In some states, being a "good samaritan" can present significant legal risk.
From Orie Steele : AshleyMadison.com ; BigData leads to information asymmetry

From Wayne Chang : ^ a good point I heard at IIW about ashleymadison is that the lawsuits didn't fully capture the 2nd and 3rd order damages, such as suicides
From Orie Steele : TechnoViking… great story
From Vic Cooper : information asymmetry means that the market is ripe for disruption
From Orie Steele : See https://en.wikipedia.org/wiki/Techno_Viking ; Standing still is the best way to die in any FPS
From drummondreed : +1
From RuffTimo : Yeah, we quickly grew out of that perspective, thankfully. :) Maybe should've changed the name though...
From David Luchuk : Thank you for calling TechnoViking to mind. Truly.
From Orie Steele : Theory of negativity, is excellent branding ; Slack is another good example
From mitfik : Broadcasting discovery mechanism, you don't search but you let others to find you because of the need which you have.
From Ken Adler : Unless you pay Tinder Platinum…. Message before match :)
From Bob Wyman : Asking "Is there a Doctor in the house?" is polling. Polling is inefficient…
From Orie Steele : This is an example matching / clearing houses… there is entire division of economics dedicated to efficient matching of participant preferences
From Wayne Chang : In multi-sided markets you often have some legs that must be subsidized to make the model work.
From Ken Adler : yes
From Orie Steele : See also: https://en.wikipedia.org/wiki/Matching_theory_(economics)
From Nathan_George : (Right to be forgotten issues)
From Wayne Chang : Amazing book on market design https://www.amazon.com/Who-Gets-What-Why-Matchmaking/dp/0544705289
From Orie Steele : Everyone's favorite database of int devices… https://www.shodan.io/ ; IoT *
From Wayne Chang : https://twitter.com/internetofshit
From Orie Steele : What you want is to build indexes of authorized service providers… which you can ask interactively.
From Ivan Temchenko : inter-hub gossips?
From Orie Steele : And be careful about what you make publically crawlable
From Bob Wyman : I think what you want is "Prospective Search" not the "Retrospective Search" that you are describing. i.e. let people publish the queries that they are willing to respond to. See: https://en.wikipedia.org/wiki/Prospective_search
From Orie Steele : Sharing an email or twitter handle is an invitation to be contacted.
From Ken Adler : Similar to buyer intent broadcasting
From Wayne Chang : I wish I could tell amazon when I move as opposed to it trying to guess that about my life
From windley : So this session should have been titled "Tinder for DIDs"
From Orie Steele : lul
From drummondreed : That's a tweet there, Phil. Dare ya ;-)
From Dan Robertson (he/him) : Wow, Phil also a marketing savant... 😂
From RuffTimo : This could be a breakthrough for matching job candidates with jobs.
From drummondreed : Indeed
From RuffTimo : (without LinkedIn, Indeed, or other intermediary)
From Tyler @ Evernym : no Drummond, withOUT Indeed ;)
From Markus Sabadello : This example can even discover people who want a platypus as a pet AND as food!
From mitfik : basically this is what for we build "social platforms" those platforms are matchers in that case
From Wayne Chang : @markus RDF is truly powerful
From RuffTimo : @Markus Platypi are delicious. ;)

From Bob Wyman : This is “cross matching,” a combination of “prospective and retrospective” search.
From windley : https://twitter.com/windley/status/1319376968022855680
From Orie Steele : The problem is that greedy bots want to match with everything, and sybil lets them map the entire space…. These kinds of systems get terribly complex… they are almost always solved by relying on a trusted centralized clearing house.
From Judith Fleenor : There must be a way to revoke your desire to be matched by each key.
From Wayne Chang : @judith, would that requirement be dependent on how much info is exposed via match request?
From RuffTimo : Lovin' this... very exciting stuff, addressing a VERY tricky and problem.
From John Court : There was a DEC research project in the 90s called Each-to-Each which this reminds me of, except it was centralised matching and not diffused across Many to maintain privacy.
From Judith Fleenor : @wayne exactly
From drummondreed : He took the dare! Just retweeted, Phil.
From Gabe Cohen : +1 Orie this is incredibly noisy
From mitfik : Spamers would love it :)
From Orie Steele : Its a super hard problem in economics
From Wayne Chang : You could add friction to match requests ; The microeconomic problem you’re talking about is market congestion
From Adrian Gropper : Starting to sound like the Apple Google COVID proximity scheme
From drummondreed : Reputation plays a major role here
From Wayne Chang : https://hbr.org/2007/10/the-art-of-designing-markets
From Orie Steele : Yes, you need to make queries costly ; And joining expensive
From Gabe Cohen : I will pay 3 btc to find my dog the perfect pal
From Orie Steele : lul
From Wayne Chang : Are we queueing
From Adrian Gropper : q+
From drummondreed : Search bounties that are payable on success could work nicely
From Bart Suichies : so how is this different than MPC?
From Tyler @ Evernym : I require payment to be matched for certain things.
From Judith Fleenor to Daniel Hardman (Privately) : Love how organized this presentation is WELL Done presentation… and loved the fun elements such as the title and opening videos.
From Orie Steele : https://ieeexplore.ieee.org/document/6765218
From McCown : Doesn’t “Kobayashi Maru” imply success by surreptitiously reprogramming the system? ;-)
From Orie Steele : ^ there is a lot of academic research in this area
From Tyler @ Evernym : i.e., pay me first in order to have the privilege of matching with me
From Vic Cooper : I love this in the context of a telecommunications platform. Might solve the problem of who can ask to connect to me
From Wayne Chang : @vic I think this was earn.com’s business model prior to their acquisition & pivot
From Judith Fleenor : @VIC wouldn’t it be nice to solve the Robo Call issues…
From Wayne Chang : Pay to talk to someone, and the someone could direct that payment to a charity for a less socially awkward outcome ; But it solves the problem of lowering the noise floor
From Vic Cooper : yes or have some sort of attention token so that there is a cost to connect to me and I can decide on the price
From Adrian Gropper : context, crypto, agency
From Wayne Chang : That’s just setting your own price but with more steps
From David Huseby : key agreement “prekeys” from Noise can require the initiating party to do some computation work to calculate their half of the 3DH
From Wayne Chang : hashcash++
From David Huseby : by using something like PBKDF

From Gabe Cohen : Tl;dr advertising with didcomm
From Wayne Chang : I like the idea of sending a private key of a cryptocurrency account with a small amount
From David Huseby : so a person who wants to be discovered publishes their half of the prekey with the hashcash like challenge that has to be solved to calculate the other side
From Wayne Chang : See also some cool discussion: https://github.com/decentralized-identity/didcomm-messaging/issues/66
From Nathan_George : Sounds like some interesting papers could be linked in the notes?
From David Huseby : nature has interesting mechanisms for discovery
From Orie Steele : Slime mold is my favorite organic search system
From Wayne Chang : Vote rename TCP/IP to ANT PROTOCOL
From Bart Suichies : @David: pheromones?
From Orie Steele : There are also randomized solutions to traveling salesman that are based on ants.
From Wayne Chang : I love all sentences ending in “that are based on ants"
From David Huseby : @Bart, yes, scent marking, compressing space like salmon spawning in rivers ; those are different ways ; preventing enumeration is key. ; that’s pretty much all this idea prevents
From Bart Suichies : https://biomimicry.org/solution/slant/
From Adrian Gropper : Hence the need for powerful agents; Every query is a request with three components: ; - Claims ; - Scope ; - Purpose
From Daniel Hardman : @Adrian: +1
From Bart Suichies : powerful and logically distributed
From drummondreed : I’m a huge fan of agent-based discovery. That’s actually how Kirk solved the “is there a doctor in the house?” problem. An agent answered (in that case, the agent was a human)
From RuffTimo : Very cool point, Daniel, about matching with both privacy and verifiability of attestations.
From Orie Steele : If the matches collude they can recover related keys, which almost gives them the same information in a VDR
From Adrian Gropper : +1 Orie
From Nader Helmy : This solves a really important problem, gives sovereign individuals the ability to organize and cooperate in a way that’s typically reserved for formal organizations with their own governance
From Bob Wyman : Actually, matching is often more efficient if it is NOT sharded. But, it is easier to scale if shared.
From drummondreed : Nader, +1
From Bob Wyman : But, it is easier to scale if sharded. (autocorrect error)
From RuffTimo : Super insightful session, Daniel, and important for the space. IMO this will spawn a lot of great discussion in this community and elsewhere. Kudos!
From windley : Back in the day (2012), Drummond’s company (Respect Network, Cntl-Shift, and my company (Kynetx) built a pico-based, VRM-like system for Innotribe (SWIFT) that did this kind of matching. Here’s a video showing it (that Heather Vescent helped with). https://vimeo.com/51827693
From Nader Helmy : Social cooperation is at the core of what makes us human, its a failure if we dont solve this problem in a mainstream and easily adoptable way
From drummondreed : Wow, Phil, you found the video! Cool!
From windley : Blog search
From Nathan_George : Reminder that Wayne and Adrian are on the queue
From drummondreed : Intentcasting! That’s what I’ve been trying to remember this whole session.
From Adrian Gropper : q+ to point out this is important to inform our community'swallet vs. agent issues
From RuffTimo : Ooh... glad you brought up intentcasting, Phil... Isn't this fundamentally intentcasting?
From drummondreed : What Daniel is proposing is a very sophisticated version of intentcasting (and intent querying)

From RuffTimo : Interesting to think of how this could be used for nefarious purposes as well, allowing bad guys to find/connect... but as with all new tech, it can be used for both good and bad.
From drummondreed : This is very true. And believe me, some governments will remind us about that. Loudly.
From Nathan_George : “A horse, a horse! My kingdom for a horse!”
From David Huseby : IPv6 gives us an interesting opportunity. If we all have our own /64 then we have 64 bits to use for mapping content addresses to IP endpoints in our subnet. ; with mobile ipv6 it will be possible to literally broadcast ping all devices on a given access point to an endpoint in all devices
From David Huseby : so if I hash dog, then concatenate sushi and hash that to get the endpoint in my subnet, I can have my device listen there and then ping all other devices on that endpount
From Vic Cooper : http://bit.ly/ppred-paper
From Wayne Chang : @Dave I wonder what are some ways to make it more expensive to enumerate active possible matches by brute forcing those concat-hash queries
From David Huseby : it uses IP addresses to “compress” content addresses to an IPv6 address “bottom half” that I can use to ping devices with
From windley : More on intent casting:
https://www.windley.com/archives/2012/06/buying_a_motorcycle_a_vrm_scenario_using_personal_clouds.shtml
From David Huseby : @Wayne, default end point hands out prekeys with hashcash problems ; my device then drops all packets that aren’t the correct half of a handshake
From Wayne Chang : Ooh nice, I was suspecting some hashcash component but didn’t think of the prekey by the gateway ; cool
From David Huseby : so devices can essentially name their price
From Wayne Chang : Yeah I also like that the gateway isn’t doing the filtering ; The intermediary here is an “anonymizing” endpoint though
From David Huseby : @Wayne the noise 3DH zero round trip handshakes requires the connecting party to get the receiving party’s prekey and then they calculate the other half of the key agreement and encrypt the first packet
From Wayne Chang : To disintermediate this would need something like onion routing
From David Huseby : but a hashcash problem can also be mixed in so that the connecting party has to expend non-trivial computation cost
From Nathan_George : Note: Bob then Robert then Trev are still on the queue
From RuffTimo : Idea: those here most interested in this connect with Daniel for purposes of continuing the discussion after IIW, and push this forward without delay. This is a big piece of the SSI puzzle, IMO.
From Bob Wyman : How do we “connect with Daniel?”
From Laura J : Where can we find Dave’s papers?
From Wayne Chang : @bob hahahaha
From drummondreed : daniel.hardman@evernym.com
From Wayne Chang : But Drummond, where do I swipe right
From Daniel Hardman : “Connect with Daniel”: daniel.hardman@evernym.com
From RuffTimo : There's this discovery protocol for connecting with Daniel...
From Laura J : haha
From Bruce Conrad : Solve the problem and Daniel will come to you
From John Court : What is the load for listening on many addresses that way ? Energy and chip limits ?
From Orie Steele : Proof of work or proof of payment
From Colin Jaccino : Seems like a multicast scenario might work for this example as well
From Trent Larson : @wayne @bruce :-D Pure gold.
From Nathan_George : Queue: Robert then Trev ; Queue: Robert then Trev then Trent
From Nader Helmy : Hey Dave where can we find your papers?

From Orie Steele : Yes, one way of handling information compression is to register algorithms instead of specific tags ; And then deterministically generate the tags from the algorithm ; Btw this is how CBOR-LD works
From David Huseby : https://link.medium.com/iGXlkYcINab
From Joe Andrieu : Thanks, Daniel!
From David Huseby : principles of user sovereignty ; https://link.medium.com/TDdUMYeINab ; https://link.medium.com/IGPEVjgINab ; those three papers are ; principles of self sovereignty ; a unified theory of decentralization ; the web was never decentralized
From Nader Helmy : +1 ; UX is a huge part of this working
From David Huseby : another idea would be a "scavenger hunt" where searchers have to do proof of work to find the location of a piece of data that then gives them another problem to find the next ; to index all data they would have to tons of work
From Bob Wyman : Technology can't overcome prejudice.
From Nathan_George : Private connections means less consequences for refusing to cooperate — interesting
From Wayne Chang : @Dave capture the flag to use the service
From David Huseby : @Wayne...yes!
From Bob Wyman : A bigot with a computer is still a bigot.
From Phil Wolff : SEVEN MINUTE WARNING
From Nader Helmy : @Bob there's bias in all technology, incentives really matter at scale

Interoperability Working Group

Thursday 23H
Convener: Kaliya Young, Juan Caballero, Pam Dingle
Notes-taker(s):

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

WHERE OUR (DIF Interop WG) WORK HAPPENS:
https://github.com/decentralized-identity/interoperability/blob/master/agenda.md
Ongoing Work item:
https://hackmd.io/QZ0erBvsQzmUw00SmtfwJA

Aviary
Workday - IBM Walmart etc project
Vicki Lemieux - post doc looking at ledger interop.
Mike Jones - what's in and out of scope
Infominer - mostly listening
Chris Eckl (Condatis) - NHS project - HL-SIOP handshake protocol
Jakob Notland (PhD stude at Norwegian U Sci and Tech) - Seafood tracking
Todd Gehrke (ID2020, ex Luxoft) -
Taner Dursun (TUBITAK BILGEM) Blockchain Research Lab.
Akanksha (PhD stud, UCL) - SSI and DIDs - understanding interop scope

What to get out of this session.
Schema's is a headache.
What is the scope of interop
Curious
Getting stuff to work between different stacks
What is the scope

Share what we are doing
Q&A

- Issuance model
- Definitions of interop
    - Keith: Customers/clients - everyone's really worried about login
        - Wallet portability when
    - Keith: "just working"

Brian: How much people are investing in it
Arnon: What about interop hackathons? DIF-sponsored hackathon when?

Section of
Two vendors talk to each other
Sub Community Interop is happening

- Aries (ToIP)
- SVIP
- eSSIF

Asset Ownership Transfer using Verifiable Credentials

Thursday 23I
Convener: Ravikant Agrawal, Kalyan Kulkarni, Dave Mckay
Notes-taker(s): Ravikant Agrawal

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

- Ayanworks shared two use cases they are building for their client
- Forum is opened to discussed following:
    - How VC can enable ownership transfer?
    - What are the challenges?
    - Any alternative solution that could be considered?

"Physical Credential":Your best friend for SSI adoption

Thursday 23K
Convener: Philippe Page @The Human Colossus Foundation

Tags for the session - technology discussed/ideas considered:

Trust, Institutional trust, physical/digital credential,

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

This session was called to highlight the importance of existing physical credentials when developing SSI Solutions.

We first went through the fundamentals of "credentials" before moving on to describe how a system involving digital credentials can overcome some of its limitations and mitigates certain risks by introducing a physical credential.

We have illustrated the logic through an existing project of Digital Immunization Passport where digital limitations are overcome through a physical dedicated credential.

Notes of the sessions are below.

Building on insight from IIW31 sessions

- Overlap of authentication and consent
    - Active/Passive Identifiers - OCA
- Human interaction in a Dynamic Data Economy
    - TDA - Trusted Digital Assistant
- Physical - Digital Duality@work
    - Birth Attestation

These 3 sessions highlight the opportunities of SSI but also its limitations. In each cases the awareness of the existing physical trust framework helps defining how the digital solution should be designed. What is often overlooked is that a number of processes, particularly if they related to trust, rely on an underlying trust framework. The point of this session is to discuss when this is actually the main driver for adoption.

Physical & Digital
We know the

- strengths & weaknesses of physical credentials
- benefits of digital credentials

We (believe) we know

- limitations of digital credentials
- risks of digital credentials

But we tend to forget that centuries of evolution have evolved into the current society "trust" framework. "Limitations" are a red flag for looking for physical alternatives (e.g. inclusiveness) and certain "Risk" can be mitigated also through physical alternatives.

Start with fundamentals

- Human always required trust
- Information always had value

All societies have developed mechanisms to secure value and develop trust. These mechanisms evolved with technology. Reference made to the "SSI Primer" explaining SSI through this historical angle. The digital technological improvement

- Global reach
- High level of flexibility
- Low cost
- ……

But we still need

- Agreed Trust Framework
- Transport Information
- Access for all members of the community (i.e. not only the ones that are running the latest version of an OS !)

Then the session moved to show the benefit of a physical credential in the use case of the Digital Immunization Passport. Some slides presented during the sessions are below:

Digital Immunization Passport as an example

Why this example

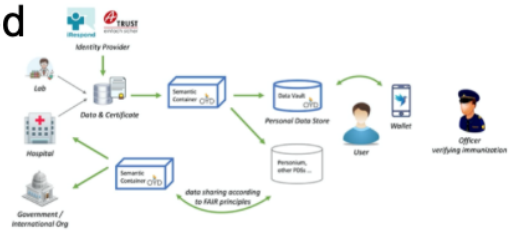
1. The "DIP" project (Yellow Fever)
   - ❏ Decentralized technology: **yes**
   - ❏ Decentralized Governance: **maybe**

1. "Aptos Credentials" Dealing with
   - ❏ Exclusion
   - ❏ Urgency

“DIP”
An open-source publicly funded project

Horizon 2020 Programme
DG CNECT
Next-generation Internet

Project acronym: **DIP**
Project title: **Digital Immunization Passport**

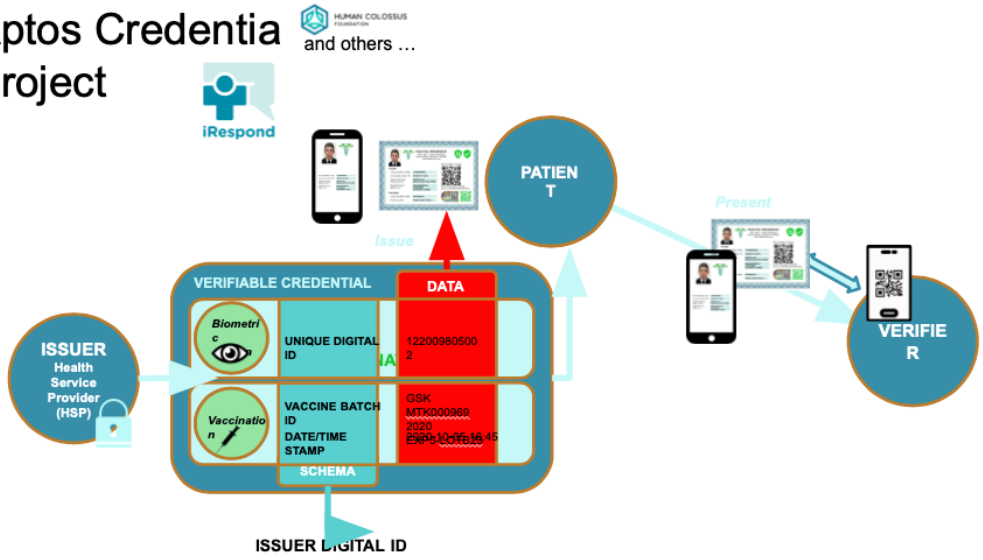


- Connects to various immunization information providers
- Aggregates, harmonizes, and semantically annotates the data,
- Makes this data-set available in an open format accessible for personal data stores (PDS)
- Provide a human-centric data management platform for health information,
- Allows to prove immunization status through Verifiable Credentials, and
- Packages selected data for processing by 3rd parties together with a well defined usage policy and governance trail

…..Good, but how do you take care of Life *«ImperfectionS»*

Aptos Credentia Project

and others …



SSI on paper is not about connecting a printer to your VC

It is recognising and leveraging the existing trust framework**S** that individual**S**, communitie**S**, countrie**S** have already build.
(even if not perfect….)

An Open-Source SDK Approach To Build A Mobile Wallet (Repeat)

Thursday 23M
Convener: Horacio Nunez
Notes-taker(s): Horacio Nunez

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

This Session is a duplicate of Session 22N. See notes provided in 22N from Horacio Nunez

Realizations About Diversity, Inclusion, and Our Industry

Thursday 24A
Convener: Drummond Reed, Darrell O'Donnell
Notes-taker(s): David Luchuk

Tags for the session - technology discussed/ideas considered:
Diversity, inclusion, representation, leadership

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

Challenging but necessary discussion to be had in our community.

Do we have a culture based on fighting problems out? … if so, it only works until it doesn't.

People back away from what some others are tempted to continue thinking of as "healthy" debate.

The risk and reality is that we are pushing voices out by "terrifying" people who might otherwise bring creativity and new ideas into discussions on important topics.

Too easy to stay away from this deep and systemic problem because it seems hard.

Being willing to admit that you don't understand is a starting point for many, even though the problem is obvious to many who experience exclusion every day.

Trust over IP - volunteer based membership but 100% of Working Group leadership is male.

How can we be part of a solution?

Recruitment and investment as opportunities to make choices - how do we find people if/when we don't even know how to look?

Women in Identity - run by volunteers, intend to help people and organizations understand unconscious decisions and steps to take to change behavior.

Research says that one woman or person of colour in a candidate group of four has a 0% chance of being hired because they stick out as unique and their credentials are erased. Having two or more women or people of colour significantly increases chances of hiring because recruiters are able to focus on merits.

When women don't speak - we don't realize the ways in which we do things to discourage women from talking. For example, women are interrupted with negativity 75% of the time they intervene.

Men in positions of influence have opportunities to make positive interventions to bring voices being pushed out back into conversations.

Though some issues are particularly unique to women, many other shared challenges apply to people of colour and people with disabilities as well.

Even when we think we are doing a good job, it is possible to consistently be doing all the wrong things.

When leadership is on board with change and inclusion, the effect is powerful.

Not trivial to ask how to get more diverse voices in the room. How do you find people and create an environment where they want to thrive and participate? We tend to focus too much on the former and not enough on the latter.

Pass the mic - when you don't know something or want diverse perspectives, give people positions where they actually have a voice.

Change the tenor of conversations by having it be hosted and led by people who wouldn't otherwise be in control.

"She's a mother so she can't be that serious." - men don't realize how frequently women encounter these attitudes and comments.

The woman's ghetto - not being allowed to speak to expertise but, rather, forced into "women's issues" panels at events.

Trust over IP - it isn't up to women to solve these problems for an organization.

Women, people of colour and marginalized persons are always interested and watching people's decisions and how they behave.

Shifting culture proactively means that more women, people of colour and marginalized people will join because a space becomes a bit less bad.

This conversation has been shut down several times and in several fora in the past.

Fundamental problem across the board.

Voices trying to be a bit louder so they can be heard are classified as problematic.

Trying to get rid of white-men only panels leads to white-women only panels.

Decentralization … who gets into the pipe and get to exit the pipe … who chooses to have their identity stripped, and who has that forced on them?

Threats of violence to women and women of colour - white men, white men and men from within same cultural groups. Affected women are always watching and aware.

Even five seats can be an opportunity for diversity. But claims of diversity often fail in a panel of mixed-men or a few women.

There is no tech fix for the human condition because we insert bias and disadvantage into our systems even though we may think we are being open to everybody.

Fundamental flaw - people in the design phase who are not as diverse as the people they mean to be serving. Who's in the room dictates what happens.

We keep looking for simple things to do, faced with a problem that isn't simple at all.

Challenge to understand the changes that are needed to treat people equally in an affirmative (not passive) way.

It isn't enough to seek out a different group of people. Need a culture change. Giving people the floor doesn't work if the audience isn't actively listening.

Pro forma change - "thank you for your service" has no real meaning. A version of this mechanical change can come when seeking diversity.

Part of valuing different perspectives is doping the hard work of accepting different ways of communicating. Undo wiring that builds up over an entire lifetime.

Aggression. Speaking up. Engaging debate. How are these valued over other ways of communicating?

Changing the way we are, what we are doing and how we are doing it is predicated on having greater diversity but that isn't getting the job done. It is so much more than that. It is about how we rejoin the human race through the work we do.

What is at stake when we talk about inclusion and diversity? Have a vision of something really different. Changing the table, not just who comes to the table.

These topics apply to all technology areas, especially for identity. Protocols, standards and data formats that describe who we are. Past IIW sessions have included discussions about how identity differs as a concept across cultures (e.g. not centred on the individual). The Buddhist pull-request.

The risk of getting it wrong is real for our community. We will not build an identity layer that works for everyone if it's not actually built BY everyone.

People have tried a lot of things but we haven't moved the numbers. A token person of colour in a candidate pool or on a committee yet, over time, it affects no change. Just checking the box.

Start with ourselves. Get educated. Try to open your eyes and make a commitment to learning.

A woman can be expected to make copies and get coffee even if they are the most experienced and educated person in a room. Yes to building the table differently.

This discussion requires people to dig deep.

Centuries, decades of experience, day to day experiences, and what people have to deal with just to walk through a door even when they are being "invited."

"Aren't you used to being the only black person in a room full of white people?"

" … there are black colleges?"

When we have to explain there are black, hispanic and native colleges, it reflects the assumptions that people bring with them into a space, and also their views on other people in that space.

Fundamental flaw in the technological system when we even have to debate whether Katherine Johnson (Hidden Figures) actually lived.

Thought experiment - imagine what a successful world would look like. Zoom allows us to suspend certain variables about our identity. Engineering out bias. What is this group's definition of success?

Should we aspire to suspend certain elements of our identities to democratize conversations? Is this what we aspire to?

Everyone has biases toward difference. Why would a person behave so differently from me? Understanding before judging.

Heard that Canadians are nice but still so hard to get into the community. Canadians not trying hard to understand non-native speakers, immigrants and help them be part of the cultural setting. Don't know how to respond to people who choose to see others based on their own biases.

Proposed directions …

1) Bring in critical thinking to process. Outsider disciplines (e.g. legal scholars, media studies) that can have an effect on the development of our concepts. Changes in technological design create power shifts that are hard to anticipate. Political aspects and hidden ideologies can be uncovered by academic disciplines focusing on digital and identity models. Involve this critical thinking without damaging the work.

2) Form of discourse inspired by, for example, political activism. The conversation takes on a radically different form. Our work will impact a multitude of groups around the world. Is there an opportunity to connect with groups that have a higher natural sensitivity to the issues we are discussing here? Enhance the discourse.

Counterpoint …

1) the concept that we are going to build bridges to a community that already exists is part of the fundamental problem. We don't need to save communities that already know where they're going and that we should be following instead.

2) a hostile wall is erected from the start of we enter into a conversation expecting someone else's voice to be disruptive.

Question: what can we do to improve IIW and the broader community?

http://humanfirst.tech

Chat log:

14:33:24 From Nader Helmy : I wouldn't want people to hold back *because* its recorded
14:33:34 From David Luchuk (ToIP) : Please feel free to jump in and add to the notes ... which I will be trying to assemble.
14:33:37 From David Luchuk (ToIP) : https://docs.google.com/document/d/1D-nE1vtc4IoX
14:34:45 From digitalsista : which camera is that.
14:43:57 From drummondreed : https://womeninidentity.org/
14:44:54 From John Hopkins : google, facebook, amazon…
14:46:31 From drummondreed : When you get a chance, tell us what time those calls are
14:47:49 From mary hodder : i;m sick of being in chats where the women's comments are only addressed by the women, and the guys just address each other.. we are having two conversations back and forth
14:48:08 From drummondreed : Let's not let that happen here today, okay?
14:49:26 From mary hodder : put link to book in chat?
14:49:38 From Michel Plante : @kay - thank you
14:49:46 From Michel Plante : enlightning
14:49:55 From Riley Hughes : +1 - thanks Kay!
14:50:06 From drummondreed : https://www.goodreads.com/book/show/42261227-tell-me-who-you-are
14:50:27 From Kay Chopard : Women in Identity coffee calls every Friday, https://womeninidentity.org/coffeebreak/
14:50:38 From Michel Plante : Another that I'm reading right now - Data Feminism - https://mitpress.mit.edu/books/data-feminism
14:50:54 From Kay Chopard : Thursday at 5:30 pm PST and Friday 7:30 am PST
14:53:12 From Kay Chopard : Here's a book about women speaking in meetings and groups: The Silent Sex: Gender, Deliberation, and Institutions by Christopher Karpowitz and Tali Mendelberg - shows how the gender composition and rules of a deliberative body dramatically affect who speaks, how the group interacts, the kinds of issues the group takes up, whose voices prevail, and what the group ultimately decides.
14:53:19 From Chris Raczkowski : Great comments, Nader!
14:53:41 From John Hopkins : +1 to diverse recruits being an emergent property of an inclusive culture
14:53:51 From billaal : Thanks Kay!
14:54:16 From drummondreed : Karen, you're next
14:54:25 From Kaliya Identity Woman : Karen has her hand raised
14:54:41 From Michel Plante : +1 Nader
14:54:43 From drummondreed : Anyone who would like to speak, feel free to put your hand up (on the Participant tab) to queue
14:55:52 From Marc Davis : Thank you @Kay for what you said and especially for providing a concrete example of a behavioral problem and a solution to address it (Behavior: Woman or POC gets cut off when speaking; Solution: Somoen in the conversation follows up immediately to ask pertain who was cut off to

expand on what they were saying to bring the group's focus back to the person who was cutoff). A longer list of these Problem:Solution pairs would probably help engineering-minded males to attempt to modify their behavior to be more inclusive.
14:56:00 From Kay Chopard : I'll stop sending you books but this one might be helpful. It's written by "two old white guys" but they are really good. It's a book written by men and for men but it's about working with women. Athena Rising How & Why Men Should Mentor Women by W. Brad Johnson, Ph.D. and David G. Smith, Ph.D.
14:56:31 From drummondreed : Kay, please KEEP sharing books and tips. It's very helpful (at least to me)
14:56:36 From Marc Davis : Ugh, sorry for typos. pertain should be "person"
14:56:53 From Nader Helmy : @Marc even better if engineering-minded males in the room actually creating the list collaboratively
14:57:17 From Marc Davis : @Nader. Great idea.
14:57:34 From Riley Hughes : +1 to book recommendations - I've added 3 to my list from this discussion already
14:57:48 From Kay Chopard : @Marc thank you for your kind remarks. I have a long list of things I'd be happy to share. I didn't want to inundate you. I did some training on this at Identiverse also and have proposed doing this at RSA as well. Happy to help in whatever would be beneficial
14:57:58 From Nader Helmy : @Marc :)
14:58:46 From Marc Davis : @Kay Awesome! Thank you!
14:59:01 From Marc Davis : Kay chopard
14:59:08 From Marc Davis : Sorry typo
15:00:16 From Bob Wyman : How do we forget always forget that the first coders were mostly women?
15:05:33 From Kay Chopard : Digitalsista's comment on algorithms reminds me of another good book - Weapons of Math Destruction by Cathy O'Neil – an American book about the societal impact of algorithms. It explores how some big data algorithms are increasingly used in way that reinforce preexisting inequality.
15:05:55 From Marc Davis : @digitalsista amazing quote : "There is no tech fix for the human condition."
15:06:06 From Kay Chopard : +1
15:06:16 From Carly Huitema : +1
15:06:26 From drummondreed : +++1
15:07:00 From Hessie Jones : Thanks Shireen!!
15:09:02 From Kay Chopard : @Dave Crocker agree about active listening. And listening for understanding
15:09:26 From Marc Davis : The bad behavior Dave Crocker is describing I call "Listening with your mouth."
15:11:31 From Marc Davis : The techniques of "Active Listening" and "Nonviolent Communication" (NVC) are truly helpful tools.
15:11:56 From Kay Chopard : +1 Nader totally agree. I think we all have to start with ourselves
15:13:12 From Nader Helmy : +1 Bilaal
15:13:16 From Nader Helmy : It's a spiritual change
15:14:06 From Judith Bush (she her) : +1 Bilaal
15:14:21 From Judith Bush (she her) : I like "really changing how the table is built"
15:14:30 From drummondreed : "Really change the way the table is built" <== profound
15:14:43 From Kay Chopard : +1
15:16:13 From Chris Raczkowski : Suggestion. Could we hear from anyone (everyone) who is not a white, male for at least the next 30 minutes - after Markus' comment? This needs to be a session of learning, where we hear the voices that are not normally heard. Or - more correctly - not heard enough.
15:17:53 From Karyl : +1 Markus - identity isn't static or narrow in scope or range, so diversity or the ability to build products that are flexible in scope and wide in range is sort of entailed in doing the job right. literally.

15:17:56 From drummondreed : Bill Aal said “build the table differently”
15:20:00 From Nader Helmy : @Karyl totally agree. What would IIW look like if all the companies building identity reflected identity in the real world?
15:20:20 From Carly Huitema : +1 being asked to make the coffee/service
15:20:27 From Nader Helmy : This community is amazing in so many ways, we should want to make it better
15:20:50 From Dave Crocker : What should IIW do differently?
What should IIW-related organizations do differently?
15:21:59 From Kaliya Identity Woman : So yes chris…and at last IIW we had a session about diversity and inclusion and it was basically only women and people of color… I’m suggested drummond calll a session to explain/share his recent eye opening and this is the first session every on diversity that I’m hearing white men talk about their culture and issues <— a big part of this problem is related to this culture and how men in leadership within our community now - to reflect and actively make change.
15:22:48 From Riley Hughes : Kaliya, I actually really liked last IIW’s session as well, because the few white men who were there learned a LOT from a more intimate group. FWIW.
15:22:51 From John Phillips : One of my favourite antidotes to blinkered thinking on Identity is the work of Kwame Anthony Appiah. Eloquent and erudite, and a fabulous story teller. His series of BBC Reith Lectures on how we mistakenly use colour, creed, country and culture as identities is wonderful to listen to.
15:23:54 From Judith Bush (she her) : argh
15:24:02 From Riley Hughes : However it is interesting to see the difference in attendance in last IIW’s session and this one.
15:24:52 From Judith Bush (she her) : The new table will be less comfortable for people who have been at the table all along.
15:26:39 From drummondreed : We need a movie about Shireen!
15:27:01 From Michel Plante : +1 Drummond +1 Shireen
15:27:06 From mary hodder : Using zoom means everyone gets to be just as big.. the women with our voices can be heard just as big, Shereen can be just as big.. we can follow her, just as big. Having this conference on zoom, really changes some things. She can be the leader now, and that’s hard to achieve in person.
15:27:26 From Nader Helmy : The key here is to listen to Shireen when you leave this session too
15:27:26 From Marc Davis : +1 Mary
15:27:48 From billaal : +1 Maureen and Nader
15:28:09 From Darrell O'Donnell : +1 Nader - and I’ll add support her and other’s when we see ideas being shot down instead of being nurtured.
15:28:09 From drummondreed : +1 to Mary
15:28:13 From Karen Hand : We know the IT community struggles with EDI (equity, diversity and inclusion) - a call to action - how does IIW and ToIP be leaders?
15:28:18 From Dave Crocker : The comfort at the table depends on one's priorities, notably 'winning' versus 'best' (or, at least, 'better'). Ego vs. Group benefit.
15:28:32 From Carly Huitema : +1 emails are totally different when the writer thinks I'm male. It blew me away, I didn't expect it.
15:28:36 From mary hodder : one metric for me is having POC leaders and the white people are willing to follow them…
15:28:56 From mary hodder : In one group I’m in, we have a black woman leader.. and a bunch of white people follow her
15:29:16 From Nader Helmy : Someone asked about concrete changes we can make... scholarships that come with positions of influence
15:29:42 From digitalsista : Karyl I don't think suspending identity is the solution

15:30:24 From mary hodder : and she told us she tells people that she has this one group, where most of her groups are a mix, of a bunch of white technologists.. and we follow her.. and it's kind of making her think too, because it's the first time
15:30:37 From Judith Bush (she her) : @dave, i'm thinking about having to be the one who has to bridge communication and attitude differences — instead of asking someone to speak up, or speak less emotionally, or or or — instead taking on the responsibility to understand without asking the other to change.
15:31:21 From Judith Bush (she her) : And Lucy is saying it well
15:32:10 From Karyl : I agree, and at the same time, I wonder about the implications of our newfound ability to do that online [the majority of our connections right now]. @shireen
15:32:34 From drummondreed : +1
15:32:52 From mary hodder : +1 Lucy
15:33:02 From Kay Chopard : +1
15:33:41 From drummondreed : Outsiders very welcome!
15:34:51 From Marc Davis : @Shireen, your voice and experience are so important for all of us to hear. To you, @Kay, @Kaliya, @Mary, and everyone: What are some things IIW can do differently on the level of individual behavior, group processes, and the community and unconferences, to address systemic racism and sexism in how we communicate and work together?
15:36:10 From Kaliya Identity Woman : Thats a good question marc
15:36:32 From drummondreed : Yes. Can we take that up next? We have 10 mins left…
15:36:53 From Chris Raczkowski : Great comments, Lucy. Thank you for this perspective! You're a qualified leader in the SSI space.
15:37:05 From Chris Raczkowski : (For all others - I have had the good opportunity to work with Lucy for the last 6 months)
15:37:08 From Marc Davis : +1 @kaliya @drummond
15:37:19 From Dave Crocker : @judith, after dropping out, I went back to finish college and had a psych class, taught by a newly-minted, Latino prof who knew his topic but wasn't a very good teacher. I was making up an incomplete, and so besides being older, also had some background for the class.
II would sometimes be unsure of his point and would ask him if he meant this or that, and he would say yes. I started noticing that a substantial part of the class had a marked reaction of relief. Their reaction was so pronounced, I started doing similar clarification questions, even when I did not need to for myself. The prof noticed this an eventually thanked me. (He also went on to learn how to teach well.) This was an early lesson in the benefits of facilitation.
15:37:21 From Kay Chopard : @Marc I think there are probably a lot of things if we think about it. Not sure we can tackle it now but we really need to do the work to make it happen. I'm the newcomer and I know @Kaliya, @digitalsista and @Mary probably have some great ideas.
15:37:35 From Lucy Yang : Thanks, Chris!
15:37:43 From billaal : Arnon, Scott David and a few others and I are just starting a conversation
15:38:17 From Kaliya Identity Woman : can you share where we can read about what you are saying?
15:38:36 From billaal : Like Kaliya said!
15:38:44 From Trev Harmon : This is a fantastic conversation, and I'd like to know what additional channels there are to continue to hear the diverse voices beyond this session. Women in Identity is a good start, but I want to know about more channels.
15:39:12 From Trev Harmon : In other words, I'd like more places where I can listen.
15:39:18 From Brent Shambaugh : Just Identity?
15:39:47 From Brent Shambaugh : identity is complex..it might be in ponds where you do not expect
15:39:48 From drummondreed : I'm hoping we can get to that Trev in the 6 mins we have left.
15:40:18 From Kaliya Identity Woman : Are some men in this community possibly open to getting more direct feedback on their behaviors and actions from women and people of color? Some names are being

shared about potential folks who are doing work - but not all of them are necessarily “allies” at least not yet - like how can we have pods of accountability or something (I’m thinking off the cuff here)
15:41:01 From Darrell O'Donnell : I am - be gentle though! I want to know how I can be an ally and supporter.
15:41:19 From Sam Curren : ^Same as Darrell
15:41:32 From Trev Harmon : I'm open to all channels, but I think I'm particularly lacking in the identity space.
15:41:47 From Riley Hughes : I definitely am. I’d be surprised if there are men who *aren’t* open to that.
15:41:57 From Dave Crocker : For difficult feedback, it can help to have designated mediators who are known to be available, provide a buffer (or even anonymity) and likely to communicate in a way that is non-threatening.
15:42:05 From Marc Davis : @Kaliya yes absolutely and always.
15:42:11 From Karyl : ^^Kaliya!
15:42:17 From Karyl : send Dave the mediator link
15:42:31 From billaal : I am in!
15:42:36 From Karyl : from the new code of conduct! I’ll drop it in the notes.
15:43:36 From Nader Helmy : One thing I learned in Engineers without Borders is the idea that you don’t sit and build solutions for people. You listen to people and help them build solutions for the things they care about
15:43:41 From drummondreed : Excellent - how will we keep this dialog going?
15:43:58 From drummondreed : Nicely said, Nader
15:44:06 From John Phillips : IIW has already built a "way of working" that includes reminders to people (closing/opening ceremonies, gifts etc.), why not consciously, deliberately, add in some elements that remind us of the need to encourage and respect diversity.
15:44:09 From Darrell O'Donnell : @nader - that must have been awesome experience!
15:44:31 From Trev Harmon : I've really enjoyed this session. Thank you to everyone who attended and especially to those who shared.
15:45:05 From billaal : Human First Tech
15:45:19 From Darrell O'Donnell : http://humanfirst.tech
15:46:01 From Kaliya Identity Woman : We want to convene an Inclusion and Interop Collab - http://humanfirst.tech/inclusion-interop-collab/
15:46:12 From Nader Helmy : @darrell awesome and humbling!
15:46:18 From drummondreed : Is there a date for that yet?
15:46:31 From Kaliya Identity Woman : we need some sponsors to put an anchor down
15:46:36 From David Luchuk (ToIP) : http://informedopinions.org
15:46:48 From Nader Helmy : ++++1 Kaliya
15:47:11 From Kaliya Identity Woman : also we are thinking about education/training for white folks and white men in particular to learn more about how to be allies but also history they don’t know
15:47:40 From Dave Crocker : The human first tech website seems not to indicate who any of the humans are who are involved with it.
15:48:06 From Michel Plante : Excellent session! THANK YOU!
15:48:31 From Dave Crocker : ah. sorry. finally saw 'leadership team'.
15:48:37 From digitalsista : Dave contacting humans is kind of my joke.
15:49:01 From digitalsista : but you found it.

Hyperledger Indy Identity Projects: How to get involved and what is missing?

Thursday 24B
Convener: Nathan George
Notes-taker(s):

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

See Indy, Aries and Ursa here https://wiki.hyperledger.org/
Newsletters about everything going on can be found here
https://wiki.hyperledger.org/pages/viewpage.action?pageId=39618905

The Identity WG and the implementers call are good places to get started asking questions and getting to know community members

You can subscribe to mailing lists and get a calendar of community events for the groups you are active in here https://lists.hyperledger.org

If you have questions please reach out on https://chat.hyperledger.org #indy #aries or #ursa

I Like Personalized Ads: A Discussion On How To Convince Laypeople to Care About Privacy

Thursday 24C
Convener: Gabe Cohen
Notes-taker(s): No one / saved Zoom chat

Tags for the session - technology discussed/ideas considered:
Privacy, digital rights

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

The session mainly focused on what information we have on individuals' privacy being eroded and tracking.

An idea was raised to increase awareness to more personally relate privacy erosion to personal harm. At the same time, it was recognized that individuals giving up their privacy has helped them and others much more than it has harmed, at least ostensibly.

We discussed it as a binary morality -- either you see a problem being “naked” on the internet, or “followed around” or you don’t. We agreed that legislation to protect privacy (similar to GDPR) could be beneficial in place of widespread moral agreement and/or technological proficiency.

The conversation was great and should be on-going as we embrace our friends and colleagues in discussions about the importance of privacy and digital rights.

Chat From Session:

From Doc Searls : Some links (for at least where I'm coming from): https://blogs.harvard.edu/doc/the-adblock-war/ , https://pagexray.fouanalytics.com/
From Alan Karp : RFID tags do track us when we walk down the street.
From Vittorio Bertocci : are we doing raise hands queuing or should we interject dynamically?
From Gabe Cohen : either/or
From Doc Searls : https://pagexray.fouanalytics.com/q/smithsonianmag.com — a good visualization of what happens behind the scenes at a website, in this case Smithsonian Magazine. ; Actually, there isn't much of a trade-off. The New York Times dropped most of its tracking, and there was no obvious difference for readers. While the paper made the same money.
From Hob Spillane : Doc, that's a mind blowing visualization
Doc Searls : The sell to muggles isn't that their data is being lost or misused. It's that they're being spied on by systems that never asked, and there is no way to know what the spies are doing with what they learn.
From Gabe Cohen : Without tangible harm they see only benefit (trade data for connect w/friends, or subsidies platform usage)
From Judith Fleenor : Welcome to your first IIW Divya, hope you are enjoying it.
From Divya Siddarth : Thank you!! It's been fascinating :)
From Doc Searls : In other words, the sell is manners. And morals. It's just wrong, even if it's not obvious. The cool thing about PageXray is that it shows what entities are using their x-ray vision to see through the clothes people wear (their browsers) on the Web.
From Divya Siddarth : Although lots to figure out
From Judith Fleenor : I loved that video!
From Doc Searls : Surveillance Capitalism is great research on one thing Google does. And it has given us a two-word label for a practice. A better book about what's actually going on is Reengineering Humanity: https://www.reengineeringhumanity.com/ ; FWIW, most of the college students I've talked with about this use ad blockers, and assume that takes care of the problem. ; A good "control" browser is Epic. Next to Tor, it's the most private browser. It doesn't even remember history. https://epicbrowser.com/
From Gabe Cohen : https://privacytools.io/
From Doc Searls : +1 on the echo chamber. Clubs are comfortable, and everything we see on Facebook, Google, Instagram and the rest are roughly clubs of people we're comfortable with.
From Vittorio Bertocci : cliques*
From Karyl : I often use the analogy of a "digital leash" to describe the certainty engineering aspect of social/ad algorithms to my friends & family.
From Doc Searls : Critical point by Judith. Different ads are bound to happen, because one's eyeballs are being auctioned in a real-time market to hundreds of advertiser robots. But the profiling of *you* by the publisher is different, and the pub shape-shifts to give you more of what you've already seen. ; By the way, the profiling of you by a publisher (website operator) may or may not be based on their own internal systems. ; : https://duckduckgo.com/?q=SSI+self-sovereign+identity
From Vittorio Bertocci : this was the clip I was referring to:
https://www.youtube.com/watch?v=F7pYHN9iC9I
From Doc Searls : DuckDuckGo uses google in a privacy respecting way.
From Judith Fleenor : But these are things that people like us may know about, but most people don't know about those.
From Doc Searls : I'm not sure it does much good to tell lay people how to protect their privacy, until we have tools that are easy to use. Those don't exist yet. Apple is moving in that direction, and there are changes happening with Firefox/Mozilla, Brave and others.

From Gabe Cohen : It's more likely they'll use it because it has a better UX, or is a "default" than any other tangible benefit
From Judith Fleenor : Almost all harms carry a benefit… but they just don't understand the harms. And also, if they know the how to avoid the harms to get the benefits they wants. So there is a feeling, "what else am I supposed to do"
From Vittorio Bertocci : the tools there are hard. Many of the measures Apple is putting in place aren't really working in practice, as RPs are refusing them (eg the email intermediation). They can maintain the virtual signaling because they aren't doing much "harm". If everyone would do that, it would be much harder for them to claim effectiveness in privacy protection ; @judith +1!! ; virtue* signaling
From Doc Searls : We need tools that work globally from our side. this is one that grew out of an IIW session two years ago: http://www.globalconsentmanager.com/
From Gabe Cohen : You've earned $4 for Facebook today!
From Doc Searls : See https://cyber.harvard.edu/projectvrm/VRM_Development_Work#Privacy_Protection ; That started here at IIW as well.
From Kasey Alusi : @gabe +1
From Vittorio Bertocci : network effect FTW ; you can't really change social norm tho... the fact that such a photo will damage you is true regardless of whether that's fair or otherwise
From Doc Searls : This at the W3C has promise. It's Do Not Track with teeth: https://globalprivacycontrol.github.io/gpc-spec/
From Gabe Cohen : +1
From Doc Searls : Look at the editors there. Unlike what happened to Do Not Track, the editors aren't Google, et. al.
From Gabe Cohen : Great to see the effort revived
From Vittorio Bertocci : "This standard is intended to work with existing and upcoming legal frameworks that render such requests enforceable."
From Vittorio Bertocci : technology is the easy part.
From Gabe Cohen : The privacy advocates falling back to legal enforcement on tech problems seems...troubling
From Vittorio Bertocci : @gabe, GDPR is pretty much that :)
From Gabe Cohen : True
From Judith Fleenor : +1 Jeff
From Vittorio Bertocci : @rory, @alan: ever used https://ground.news/?
From Gabe Cohen : https://www.google.com/maps/timeline
From Kasey Alusi : @vittorio, thanks for sharing, this is cool
From Jeff Kennedy : +1 that's a neat site
Vittorio Bertocci : @kasey you're welcome! I find it really useful. SOmetimes the ratings are surprising!
From Judith Fleenor : What is that X-ray thing you are talking about?
From Hob Spillane : Doc posted it earlier: https://pagexray.fouanalytics.com/q/smithsonianmag.com
From Doc Searls : That's the example of one especially exploitive publisher. And, by the way, they get kickbacks for all this. There is money in it for them. ; A way of looking at this (and explaining it to lay people) is that we are naked online, lacking even the fundamental privacy technologies which in the offline world we call clothing and shelter. Nor do we have ways of signaling to others what's okay and what's not.
From Gabe Cohen : To them, their nudity is a bargain for mode dopamine-inducing content
From Doc Searls : Of some relevance: https://cyber.harvard.edu/projectvrm/Privacy_Manifesto ; Actually, Gabe, I think they don't know they're naked. (As with all metaphors, there is a limit to the relevance.)
Gabe Cohen : Could be true. Putting on clothes is a process of being privacy-aware. And it's really cold out
From Judith Fleenor : I've enjoyed this conversation. Thanks for facilitating the Conversation Gabe. I have to sign off for now. I need to do something before the closing circle.

From Gabe Cohen : Thanks for joining!
From Jeff Kennedy : One example which isn't a harm only if you trust the government: https://www.statista.com/statistics/234867/government-requests-for-user-data-from-twitter/
From Gabe Cohen : "Data gone wrong news bulletin"
From scottmace : https://thehill.com/policy/technology/437399-facebook-delivers-housing-employment-ads-based-on-race-and-gender
From Jeff Kennedy : ^ Redlining reinforced
From Gabe Cohen : https://money.cnn.com/2018/02/20/media/internet-research-agency-unwitting-trump-supporters/index.html
From Gabe Cohen : ^ profiling to carry out political objectives ; Privacy is an act of self preservation, or insurance

did:web 201 - Risks & Mitigation

Thursday 24E
Convener: Dmitri Zagidulin, Oliver Terbu, Orie Steele

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

Slide deck: https://docs.google.com/presentation/d/1ST3-CiC_YvuY8AoMO96yWCVZFytfHica9CUjG6h4nsM

What are Our Questions?

Thursday 24G
Convener: Will Abramson
Notes-taker(s):

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

https://amorebeautifulquestion.com/
https://www.triarchypress.net/drc.html

- "How do we stay humble & act with precaution in the face of uncertainty and constant change?" - drc
- "What are we taking for granted?" - drc
- "What are the basic assumptions and beliefs that inform how we define the problem and offer solutions?" - drc
- "How can we nurture opportunities and projects the demonstrate viable and desirable alternatives to business as usual" - drc
- How can we incorporate long term thinking into our ideas

From Bruce Conrad : “What do you want to do about that?” ; From @Phil ; “What is this session about? ; From @Wip
From Phil Wolff : When is IIW32?

How do we improve collaboration?

History may be here, but it is unevenly distributed.

Why should I care what happens after I'm dead?

What is a DID's carbon footprint?

From Bruce Conrad : “Is it a good idea to give strongly encrypted point to point messaging to everyone?” ; “How many watts are consumed when a DID (i.e. a key pair) is created out of nothing?”
From Phil Wolff : What can technologists do to prepare society for a much more serious pandemic?
From Bruce Conrad : Can we avoid the future described in “The Machine Stops” (short story by E. M. Forster in 1909)? ; “If the best way to predict the future is to create it, what do we want to create?” ; “How can we reduce the gap between haves and have nots?” From @Mark
From Phil Wolff : How do we sip usefully from the firehose of knowledge?
From Bruce Conrad : “Will the world be a better place when the 2 billion people w/o an identity have one because of us?”
From Phil Wolff : How do we design and evaluate our systems for equity?
From Bruce Conrad : “How to ensure that our technical solutions benefit everyone in an equitable way?” From @Wip
From Phil Wolff : "May I tell a brief anecdote?" from @Bruce
From Bruce Conrad : “@Jacob do you have access to the chat history here?” From @Bruce
From Jacob Siebach : What did I miss?
From Phil Wolff : We solved world hunger. And climate change. Now we're fixing Quora.
From Jacob Siebach : Hahahahaha!!
From Bruce Conrad : “Are questions more valuable than answers?”
From Phil Wolff : "Why do you care?" by Jacob
From Bruce Conrad : A favorite question, from I forget which book, is, “What do you want to create?” ; “Are you trying/hoping to elicit the unspoken/hidden questions which drive us?” ; acta non verbal (sp?) actions rather than words ; From @phil
From Phil Wolff : Acta Non Verba
From Bruce Conrad : “How can I get better at asking questions?” From @wip ; “What is the real purpose of this session?” ; “Can you help me understand your opinion?” From @Jacob ; “Give a list of unsolved problems?” ; “Do you trust people enough to allow them to choose a solution other than the one we think is best?” From @Jacob ; “Is it okay with me if you smoke?” From @phil ; “How can we avoid doing harm in our intent to do good with our tech?” ; “What is our technology for?” From @wip ; “Is faster better?” ; “Are we short-changing ourselves when we only call electronic things technology?” From @Jacob
From Bruce Conrad : Session 23 room K “Paper: your best friend for SSI adoption”

Dynamic Data Economy: The Big Mountain Behind SSI Hill

Thursday 24K
Convener: Robert Mitwicki
Notes-taker(s): Robert Mitwicki

Tags for the session - technology discussed/ideas considered:
DDE, SSI, Data Flows, DID, MSP, PBS

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

During the session we gave a short introduction to the Human Colossus Foundation, presented the vision of Dynamic Data Economy, described what it is, briefly discussed major components.

The Human Colossus Foundation is a non-profit organization based in Geneva, Switzerland. The aim of the foundation is to build synergy within the ecosystem towards Dynamic Data Economy. Foundation actively designing, building and implementing core components.

Dynamic Data Economy - set of principles describing smooth data flows within the digital space
Data is like electricity
It has value when it FLOWS
It is costly when it STAGNATES

Major components of DDE are:

- TDA - Trusted Digital Assistant - user friendly interface for DDE. TDA for DDE is analogy to what Web Browsers have become for the modern internet. It is a user gateway to the digital space.
- Data Storage - Logical data storage for entities to store and manage their data
- Purpose based services - purpose oriented service providers which expose their interfaces to the network allowing users to discover and interact with them.
- Meaningful service provider - services focused on data enrichment

After describing the core components of DDE we delve into technical blocks which allows to achieve set goals:

- KERI - he first truly fully decentralized identity system.
- Authenticated Credentials (VC) - Verifiable Credentials - digitally provvable set of claims about the subject
- OCA - Overlay Data Architecture - meta language to describe semantic of the data
- Semantic Containers/Storage + Consent - portability mechanism for the data

SSI on its own with VC is just a teaser for what is coming. Identity itself is not enough to change the way we operate. Settling down just on those concepts brings a lot of risk into the community and the SSI itself. A lot of projects focus on monetization of the technology in the very early stage sometimes having negative impact on its adoptions. In HCF vision we believe that data flows which SSI unlocks brings much more value and opportunity to the community than anything else. Digital identity in a SSI form and VC are just enablers of the new coming dynamic data economy. DDE is the big mountain which is sitting behind the relatively small SSI hill which everyone is trying to climb. With that vision we are able to design and build much more sustainable models and build the technology to serve all.

An Open-Source SDK Approach To Build a Mobile Wallet

Thursday 24M
Convener: Horacio Nunez
Notes-taker(s): Trent Larson

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

Showed video of mobile wallet from Kiva.
- provides an iframe to insert code easily into legacy websites

Open Source Aries Frameworks from earlier IIW XXXI talk.

Horacio showed how they hoped to organize the code so that it's very readable and debuggable.

Q: With a use-case where people start their experience on a mobile browser, a new app pops up to ask them to sign which can be confusing. Thoughts?
- Apple is introducing AppClips
- Another way would be to show the web page embedded inside the app.

Everyone's making their own wallet app. Someday we'll probably have 3-4; for now we have dozens or hundreds and that's OK while we learn best practices.

Findy wallet connection chatbot.

Notes in this book can also be found online at
https://iiw.idcommons.net/IIW_31_Session_Notes

Demo Hour / Day 1 & Day 2

Thanks to our Demo Hour Sponsors!

Demo Hour Day 1: Tuesday October 20, 2:30 - 4:30
Demo Hour Day 2: Wednesday October 21, 1:30 - 2:30

DEMO Table/SPACE #

1. **DIF: Universal Resolver and Universal Registrar:** Markus Sabadello
   URLs: https://uniresolver.io/, https://uniregistrar.io/
   We'll demo the latest versions of the Universal Resolver and Universal Registrar, based on current developments in the DID Core specification.

2. **Business Partner Agent: Organizational Wallet to Exchange and Update Company Masterdata:** Moritz Kaminski, Robert Bosch AG
   URL: https://github.com/hyperledger-labs/business-partner-agent
   Instead of data exchange via email and manual verification, the authenticity of company data or certificates can be cryptographically verified and their exchange automated. The demo shows the exchange of company data including a verified bank account between business partners based on Verifiable Credentials and Hyperledger Aries.

3. **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.

4. **Trinsic - Integrate Self-Sovereign Identity with Thousands of other Applications:** Riley Hughes
   URL: https://trinsic.id
   Achieving SSI adoption through 2,000+ integrations & automated workflows for self-sovereign identity through Zapier. See how Phil Windley setup an IIW ticket verifiable credential issuance workflow in only ~20 minutes.

5. **Verity and Connect.Me / Evernym: Tyler Ruff**
   URL: http://evernym.com/products
   Connect.Me is a mobile digital identity wallet built for regular people. Evernym Verity makes it easy for organizations to issue and verify credentials. Together, these scalable and production-ready technologies unlock the power of SSI in an interoperable and open ecosystem.

6. **Kiva Protocol - EKYC and SII: Horacio Nunez, Jacob Saur**
   URL: https://kiva.global/protocol/
   The Kiva Protocol is a platform that enables the solution of identity challenges in the finance sector. In this demo we will see how frictionless EKYC can be realized thanks to SSI and open source.

7. **Tru Social Publishing: John Wunderlich**
   URL: https://www.tru.net/about for the Tru story or here **https://trunet.app/signup** to sign up.
   I will walk participants through the basic functionality of Tru: A social publishing platform, or socially verified network, that provides permissioned data and publishing with verified provenance for individuals and groups that are interested in reclaiming their authentic voices on the web.

8. **Demo of the KERI CoreLlibrary in Direct Mode: Sam Smith**
   URL: https://keri.one/
   KERI stands for Key Event Receipt Infrastructure. KERI is a ledger-less or ledger agnostic identifier system that is meant to be interoperable within the existing DID ecosystem, but not limited to the DID ecosystem. KERI has two modes of operation direct (one-to-one) and indirect (one-to-any). Direct mode is like did:peer. This demo will show a direct mode exchange of KERI events between two peers to bootstrap their identifiers and proof of control authority.

9. **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.

10. **SeLF & esatus Wallet by esatus AG:** André Kudra & Christopher Hempel
    URL: https://self-ssi.com/en/
    SeLF integrates Self-Sovereign Identity 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.

11. **Transmute:** Karyl Fowler, Guillaume Dardelet, Orie Steele, Margo Johnson
    URL: https://www.transmute.industries/
    Transmute's platform secures critical supplier, product, and supply chain transaction data using verifiable credentials and decentralized identifiers. This technical demo will highlight the role of the Universal Wallet as an open standard for wallet portability, including Transmute software integration examples with Encrypted Data Vaults and scalable identifiers.

12. **Privacy and Trust for Physicians and Patients:** Leah Houston, MD
    URL: https://hpec.io/ @HPECid
    HPEC is creating a decentralized network of practicing physicians. Our vision is to restore privacy, security, and trust to the doctor patient relationship. Our first use case will be building and connecting a qualified and credentialed physician social network using SSI.

13. **The Human Colossus Foundation / Argo, the DDE sandbox - Where *Identity* meets *Data*:** Paul Knowles & Robert Mitwicki **URL: https://argo.colossi.network**
    Where *Identity* meets *Data*. Human Colossus will demonstrate the merging of the Inputs and Semantic domains within the context of a Dynamic Data Economy. The demo will demonstrate a dynamic data flow with explicit consent between two Hyperledger Aries agents.

14. **humanID:** Joyce Liu
    URL: https://human-id.org/
    humanID is a non-profit identity for online communities free of abuse. Think 'Login with Facebook', but trustworthy & just as fast. Zero personal information is stored or shared. The path to a better internet is a user-centric digital identity that is accountable and anonymous.

15. **The Blinky Project: Brent Shambaugh**
    URL: https://theholo.space/
    "Early Explorations with LoRa extended WiFi networks, MCUs, and Cryptographic-Coprocessors"

16. **Spruce Systems, Inc. / DIDKit:** Charles E. Lehner
    URL: https://medium.com/@sprucesystems/spruce-developer-update-2-484368f87ee9
    DIDKit a suite of tools for working with Verifiable Credentials and Decentralized Identifiers. We will demo the Rust library and command-line tool, and present our current and planned integrations with our mobile app and server applications.

17. **UNiD Node App:** Ed Eykholt, iRespond Global
    URL: https://www.irespond.org
    We are a privacy-preserving biometric service provider. Our UNiD product creates a pseudonymous 12-digit numeric identifier associated with a person's iris scans. In an SSI context, biometrics are an excellent way for a credential holder to prove they are indeed the subject.

18. **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

19. **HYPR the Passwordless Company**

20. **Condatis – SSI-OIDC Bridge:** Chris Eckl and Richard Astley
    URL:
    Offering a simple out of the box SSI extension to existing federated systems. Can make an enterprise SSI agent available for any digital service that already used federated identity. Allows abstraction to one SSI technology stack and will offer interop between SIOP and Hyperledger Aries.

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.

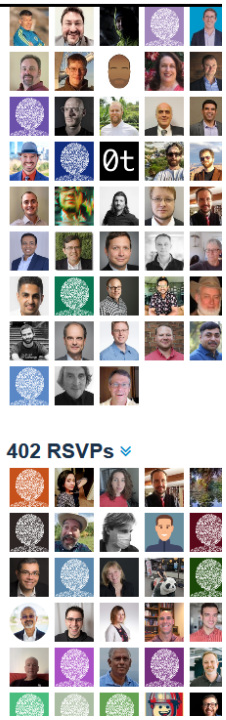
Planet Identity Revived ~ @identitywoman & @#InfoMiner cleared out & updated Planet Identity (see links below) you can support the work here:
https://www.patreon.com/user?u=35769676

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/

IIWXXXI #3! Screen Shot Album by Doc Searls

Check out Doc's great variety of 'Screen Shots' from our time together! @dsearls

https://www.dropbox.com/sh/5m6bkj3od4f78db/AADIHJvJQwDlxm_apG4wN4tfa?dl=0



See you April 20, 21 and 22, 2021

for

IIWXXXII

The 32nd Internet Identity Workshop

REGISTER HERE

www.InternetIdentityWorkshop.com