IIWXXXIII

INTERNET IDENTITY WORKSHOP 33

October 12-14, 2021

Book of Proceedings

www.internetidentityworkshop.com

Collected & Compiled by
LISA R. HORWITCH, DOUNIA SAEME, HEIDI N. SAUL

October 12, 13 and 14, 2021
On Line, Near You ~ via QiqoChat

The Internet Identity Workshop Global Community / Attendees at IIWXXXIII

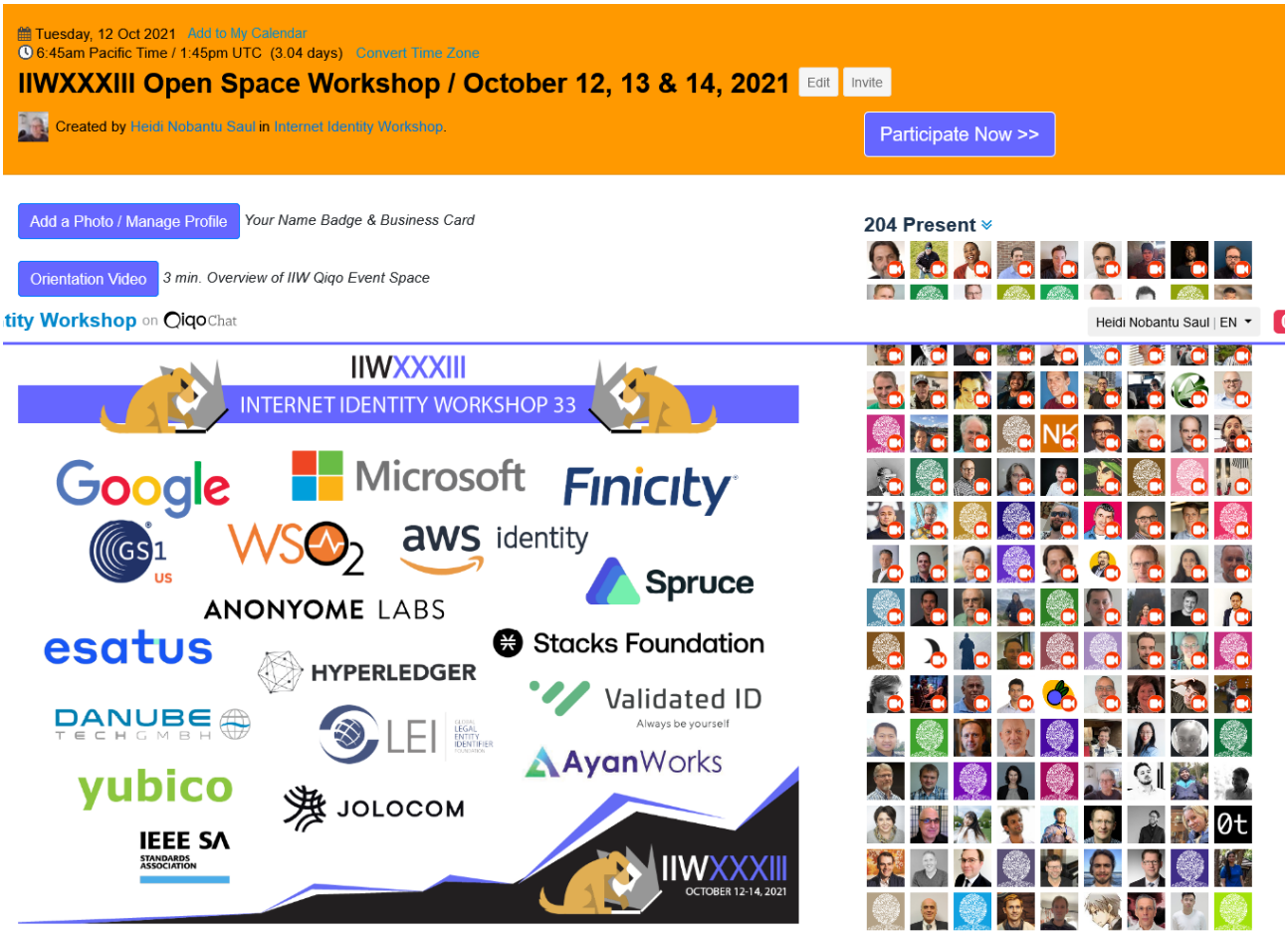
IIW founded by Kaliya Young, Phil Windley and Doc Searls
Co-produced by Heidi Nobantu Saul, Phil Windley and Kaliya Young
Facilitated by Heidi Nobantu Saul, Kaliya Young, Lisa R Horwitch, Dounia Saeme

IIWXXXIV In Person in Mountain View, CA
April 26 - 28, 202
REGISTER

Thank You! Documentation Center & Book of Proceedings Sponsors: JOLOCOM – AyanWorks – IEEE Standards Association

@GETJolocom **@ayanworkstech** **@IEEESA**

Contents



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 17th year and is Co-produced by Phil Windley, Heidi Nobantu Saul and Kaliya Young. IIWXXXIV (#34) will be April 26,27 and 28, 2022.

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

IIWXXXIV #34
April 26 - 28, 2022
In Person in Mountainview, CA
https://internetidentityworkshop.com/

IIWXXXIII 3 Day Global Schedule

Time Zone Converter *find your local time* Sessions 1hr & 15min	West Coast USA	East Coast USA	Central Europe	India	Indochina (Thailand)	Japan	New Zealand
	PDT	EDT	CEST	IST	ICT	JST	NZDT
Grand Opening Agenda Creation	7 am OCT 12	10 am OCT 12	4 pm OCT 12	7:30pm OCT 12/13	9 pm OCT 12/13	11 pm OCT 12/13	3 am OCT 13
Session 1	8:30am	11:30am	5:30pm	9:00pm	10:30pm	12:30am	4:30am
Session 2	9:45am	12:45pm	6:45pm	10:15pm	11:45pm	1:45am	5:45am
unSession Hour	11:00am	2:00pm	8:00pm	11:30pm	1:00am	3:00am	7:00am
Session 3	12:00pm	3:00pm	9:00pm	12:30am	2:00am	4:00am	8:00am
Session 4	1:15pm	4:15pm	10:15pm	1:45am	3:15am	5:15am	9:15am
Demo Hour	2:30pm	5:30pm	11:30pm	3:00am	4:30am	6:30am	10:30am
Closing / Open Gifting Agenda Announcement	3:30pm OCT 12	6:30pm OCT 12	12:30am OCT 13	4:00am OCT 13	5:30am OCT 13	7:30am OCT 13	11:30am OCT 13
Session 5	4:30pm	7:30pm	1:30am	5:00am	6:30am	8:30am	12:30am
New Day	OCT 13	OCT 13	OCT 13	OCT 13	OCT 13	OCT 13	OCT 13
Session 6	1:45am	4:45am	10:45am	2:15pm	3:45pm	5:45pm	9:45pm
Session 7	3:00am	6:00am	12:00pm	3:30pm	5:00ppm	7:00pm	11:00pm
Session 8	4:15am	7:15am	1:15pm	4:45pm	6:15pm	8:15pm	12:15am
Session 9	5:30am	8:30am	2:30pm	6:00pm	7:30pm	9:30pm	1:30am
Opening Circle Agenda Creation	7 am OCT 13	10 am OCT 13	4 pm OCT 13	7:30pm OCT 13/14	9 pm OCT 13/14	11 pm OCT 13/14	3 am OCT 14
Session 10	7:45am	10:45am	4:45pm	8:15pm	9:45pm	11:45pm	3:45am
Demo Hour	9:00am	12:00pm	6:00pm	9:30pm	11:00pm	1:00am	5:00am
Session 11	10:00am	1:00pm	7:00pm	10:30pm	12:00am	2:00am	6:00am
Session 12	11:15am	2:15pm	8:15pm	11:45pm	1:15am	3:15am	7:15am
unSession Hour	12:30pm	3:30pm	9:30pm	1:00am	2:30am	4:30am	8:30am
Session 13	1:30pm	4:30pm	10:30pm	2:00am	3:30am	5:30am	9:30am
Session 14	2:45pm	5:45pm	11:45pm	3:15am	4:45am	6:45am	10:45am
Closing / Open Gifting Agenda Announcement	4:00pm OCT 13	7:00pm OCT 13	1:00am OCT 14	4:30am OCT 14	6:00am OCT 14	8:00am OCT 14	12:00pm OCT 14
Session 15	5:00pm	8:00pm	2:00am	5:30am	7:00am	9:00am	1:00pm
New Day	OCT 14	OCT 14	OCT 14	OCT 14	OCT 14	OCT 14	OCT 14
Session 16	1:45am	4:45am	4:45am	2:15pm	3:45pm	5:45pm	9:45pm
Session 17	3:00am	6:00am	6:00am	3:30pm	5:00ppm	7:00pm	11:00pm
Session 18	4:15am	7:15am	7:15am	4:45pm	6:15pm	8:15pm	12:15am
Session 19	5:30am	8:30am	8:30am	6:00pm	7:30pm	9:30pm	1:30am
Opening Circle Agenda Creation	7 am OCT 14	10 am OCT 14	4 pm OCT 14	7:30pm OCT 14/15	9 pm OCT 14/15	11 pm OCT 14/15	3 am OCT 15
Session 20	7:45am	10:45am	4:45pm	8:15pm	9:45pm	11:45pm	3:45am
Session 21	9:00am	12:00pm	6:00pm	9:30pm	11:00pm	1:00am	5:00am
unSession Hour	10:15am	1:15pm	7:15pm	10:45pm	12:15pm	2:15am	6:15am
Session 22	11:15am	2:15pm	8:15pm	11:45pm	1:15am	3:15am	7:15am
Session 23	12:30pm	3:30pm	9:30pm	1:00am	2:30am	4:30am	8:30am
Session 24	1:45pm	4:45pm	10:45pm	2:15am	3:45am	5:45am	9:45am
Closing Circle	3:00pm	6:00pm	12:00am	3:30am	5:00am	7:00am	11:00am

IIW 33 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.

- **Share your Name**
- **How are you & where are you?**
- **What are you most proud of accomplishing since the spring (IIW32) ?**
- **Looking Ahead - what are you concerned about?**

08:23:03 From @PrivacyCDN to Everyone: New phrase from Drummond: The Wallet Wars are here

08:23:23 From Gillian Delaunay to Everyone: Everyone is working on such cool, important things! Feels like I found my tribe, alignment, very empowering, thank you everyone!

08:23:28 From Paul Trevithick1 to Everyone: Hear tons of concerns about interoperability

08:23:33 From Kevin Griffin1 to Everyone: The common theme of concern from room 18 was wait for it... interopability :)

08:23:36 From Mike Ebert to Everyone: We had more than one person concerned about the misuse of modern technology

08:23:37 From Paul DIetrich to Everyone: pride in our learnings for IIW. Concern for UX, interoperability and maturity
08:24:01 From John Phillips - Sezoo to Everyone: @gillian just summarised IIW! :)

08:24:01 From Paula Berman to Everyone: Someone mentioned concerns about Zoom.

08:24:23 From Paul Trevithick1 to Everyone: The thing I'm most proud of is a paper I finished last night for this conference (https://medium.com/meefound/exclusive-self-ownership-9917cb6bdd8c)

08:24:45 From Andrew Hughes1 to Everyone: In Group #17 we were all concerned with the development of factions and 'camps' - and how to prevent this from happening. Also seeking for a business model. We were generally concerned that if we don't reach across the aisle now and work together, the factions will become hard-coded and we will all lose

08:24:51 From Darrell O'Donnell to Everyone: premature interoperability / premature standardization is a big problem

08:25:00 From George Fletcher to Everyone: @Paul that link gives me a 404

08:25:26 From Timothy Ruff to Everyone: Interop is key, but secondary to security. SSI just had some embarrassing things just happen re: security in Europe that threaten to undermine SSI's global momentum. Security first, always. Then interop. :)

08:25:32 From Tom Atlee to Everyone: Someone mentioned how do we preserve human identity as we are increasingly interacting with increasingly human AI - a dimension of digital identity I never thought was included in this field….

08:25:55 From Sivaraman Swaminathan to Everyone: Interoperability of identity is what I looking to learn from this group

08:26:32 From George Fletcher to Everyone: Concerns: for existing identity flows -- browser changes in the name of privacy protecting users, for decentralized identity -- bootstrapping an ecosystem that is large enough to gain wide-spread adoption (same concern I've had for a few years now:)

08:26:55 From Paul Trevithick1 to Everyone: @George Fletcher: https://medium.com/meefound/exclusive-self-ownership-9917cb6bdd8c <— does that work?

08:27:20 From George Fletcher to Everyone: @Paul Yes that works, thank you!

08:27:21 From Johannes Ernst (Indie Computing) to Everyone: Darrell: “premature optimization is the root of all evil in programming” (Knuth). He didn’t know about premature standardization.

08:27:22 From Roy to Everyone: This is my first time ever, I only heard of the term SSI like a month ago. I’m prolly looking for a kindergarten primer to all this decentralised stuff 😄

08:27:50 From Chris Kelly (DIF) to Everyone: Join my decentralized identity 101 in Session 4 :D

08:28:02 From Erica Connell to Everyone: Welcome, first timers!

08:28:06 From Sivaraman Swaminathan to Everyone: This is my first time ever.

08:28:14 From eliastrehle to Everyone: Concern (or question, rather): Is there a production-ready implementation of DIDComm?

08:28:14 From Robert Mitwicki (Human Colossus Foundation) to Everyone: I would like to thank the "COVID-19" sponsor by bring IIW to the world virtually to each country instead of limiting it just to suny California.

08:28:56 From Kaliya Identity Woman to Everyone: virtual jet lag is a real thing :)

08:30:00 From Shigeya Suzuki1 to Everyone: Ah. I new word -- virtual jet lag... :< it's real. I know well :<

08:30:02 From Sivaraman Swaminathan to Everyone: I am concerned as Privacy and protecting my data and the bottlenecks that exist to make it happen

08:30:10 From Marc Davis to Everyone: Our breakout room shared two major concerns: the future of humanity (climate change, disinformation, civilizational breakdown, species survival, etc.) and concerns about how to bring about the wide adoption of SSI technology.

08:31:06 From Jeff O to Everyone: @Roy: First time I came here I felt like a kindergartener in a college lecture space. My ears would be so big from listening I figured I wouldn't be able to turn my head because my ears would go wall to wall.

08:31:32 From NickyHickman to Everyone: Love the idea of an un-session hour, thank you for this precious gift!

08:32:12 From Brent Zundel to Everyone: Once again, Vic's excellent camera setup makes me feel dodgy and pixelated.

From Darrell O'Donnell to Everyone: @brent - it's the hoody not the camera
From Tim-from-IAMX Icebreaker-Questions
1. Most proud of life and work
2. Concerns regarding the future

A. Rob Aaron
1. SSI government onboarding, improve open source
2. competition in W3C to high, better work toghether

B. Noah Bouma
1. anonymous credentials
2. privacy to priority

C. Oliver Tebu
1. groundwork in many international standardiaztion organisations, re-issuance of credentials

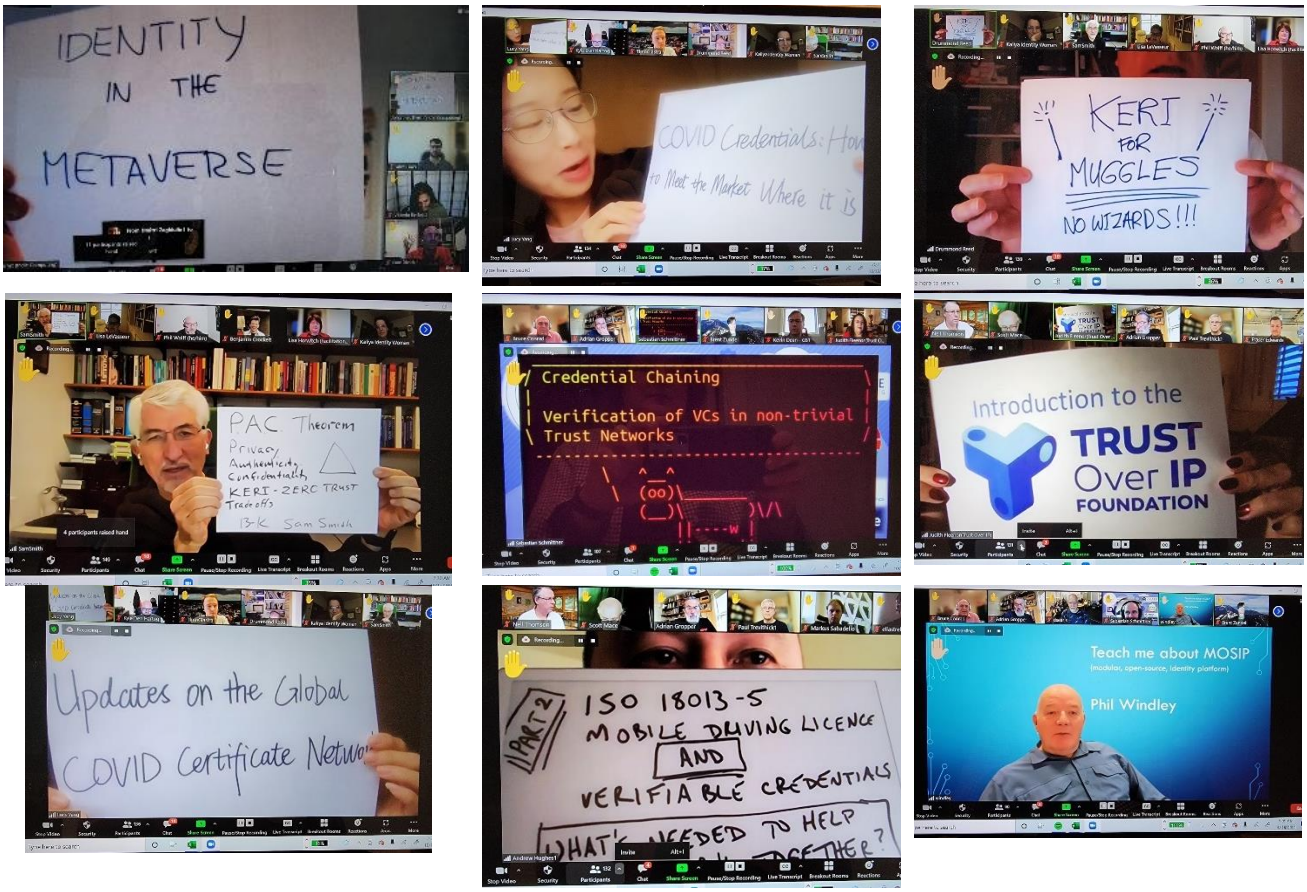
D. Ominad
1. Open Source ID solution ecosystem

E. Maneesha Indrachapa
1. graduated bachelor

F. Tim from IAMX
1. father for the 4th time and allegra credential model
2. do it right; use this IIW to challenge approach and work to consensus because of our standardization responsibility

G. Chris
1. award winner canadian government, progress on interoperability

IIW33 Agenda Creation = Schedule & Workshop Sessions



111 distinct sessions were called and held over 3 Days
We received notes, slide decks, and/or Zoom Chats
for 107of these sessions.

Tuesday October 12, 2021 ~ Day 1

Session 1
1A/ I Co-chair the DID WG and VCWG, AMA
1B/ IIW 101 Session: All About OAuth2
1C/ A proposal for SSI Interoperability based on the German SDI projects with >70 participants
1E/ DIDComm Mythconceptions: understanding the most misunderstood opportunity in SSI
1F/ DID and SSI in the NGO and Non-profit sector (I'm trying to learn)
1G/ Citizen precinct voting, data, & comms w/SSI
1H/ Group Discussion: What does NOT get adoption for SSI? AKA Failures in SSI
1K/ Digital Identity with LEIs - Update on the Verifiable LEI (vLEI)

Session 2

2A/ Human Rights Impact of Identity Protocols
2B/ IIW 101 Session: OpenID Connect
2C/ VC Metaphors - Containers and ?
2D/ DIDComm reference implementations
2E/ OpenID Connect 4 SSI
2G/ Evolution and Structure of Cryptographic Thought
2I/ Premature Interop/Standardization
2K/ GLEIF vLEI: Distributed Multi-Sig Delegated Credential Issuance with KERI & ACDC

UnSession Hour

Session 3
3A/ Need for hardware backed crypto on the web! (Would enable SSI with no mobile apps required.) Why we need to advocate as a community
3B/ IIW 101 Session: UMA/User Managed Access
3C/ HumanOS & IIW: Fit & Finish of Neuro/Technology at IIW
3E/ VC Issuance using OpenID Connect
3F/ User Stories for the VRM Intention Byway. A way to develop that starts with happy users. We'll be creating them.
3G/ GS1 License Credentials for Global Trade Identification
3H/ Microledger: data provenance log for authentic data economy

Session 4
4B/ IIW 101 Session: Self Sovereign & Decentralized Identity
4D/ Introduction to DIF Universal Resolver / Registrar
4E/ Semantic Interoperability with Layered Schemas and Semantic pipelines
4F/ Identity in the Metaverse. (It's coming, Zuck says so!) How does what we've learned apply?
4G/ Picos, DIDComm, and Decentralized SSI Agencies
4K/ What is ToIP ACDC? Authentic Chained Data Containers

Closing Circle – Open Gifting & Opening for next 5 Sessions

Session 5
No Sessions

Wednesday October 13, 2021 ~ Day 2

Session 6
No Sessions
Session 7
No Sessions
Session 8
No Sessions

Session 9
9A/ ISO18013 **AND** VC – Better Together!

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

Session 10
10A/ cheqd: Payment rails, customisable commercial models and decentralised governance for SSI (pressie & AMA)
10B/ COVID Credentials: How to Meet the Market Where it is
10D/ Fantastic DIDComm Protocols, and How to Write Them
10E/ Exclusive Self-Ownership
10F/ An Extended LDP-BBS 2020 and ZKP-LD Playground
10H/ Introduction To Trust Over IP
10J/ Global State of VC Adoption

Demo Hour

Session 11
11A/ Bridging Digital and Physical to Make Identifiers Identify (a terrible gap in web standards...)
11C/ Is the smart home a dictatorship, co-op, or homesteading?
11E/ Controlling your medical data via DIDComm - discussion and feedback on our system architecture
11F/ GoDiddy.com - Create, Resolve, Search DIDs
11G/ "Authentic" Auditing and Logging - Microledger lite?
11J/ The Future of Governance 🚀
11K/ Sign-In With Ethereum (AuthN)
11M/ Identification Minimization and other Respectful Tech Principles

Session 12
12A/ You MUST have a Choice of Policy Managers - Credential Issuers MUST NOT be able to impose the policy manager
12B/ Where do We Work on Interop as a Community?
12C/ DID Registration Architectures
12D/ Strategies For Bridging to Next-Generation Identity Systems (from the bottom up)
12E/ Some problems with JSON-LD and Content Based Addressing
12F/ DIDComm Messaging using IPFS/libp2p as a transport
12G/ DID Tethics & Mandatory Vaccine Passports
12H/ KERI for Muggles - A basic intro to KERI IDs & key mgmt.
12J/ VCs meet reality - custom VC evaluation w privacy

UnSession Hour

Session 13
13A/ Mobile Driving License AND Verifiable Credentials PART 2 << see notes from session 9A for ISO
13B/ Crossing the chasm – mass market adoption of SSI and VC. What is needed to make triangle of trust work?
13C/ Updates on the Global COVID Certificate Network
13D/ California - Verifiable Credential Policy Committee (Help us get legislation for a trust framework in California)
13E/ Time is Running Out - Get to Market - revenue, costs and who pays for what
13F/ Taking the adoption of SSI to the next level

13H/ Privacy Signal Standard Update (IEEE P7012)
13J/ Working with JSON-LD and best practices to make it easier
13K/ Privacy Authenticity Confidentiality Tradeoffs: KERI and Zero Trust Architecture

Session 14
14A/ Privacy Enhancing Mobile Credentials (building on prior Kantara report: https://kantarainitiative.org/download/pimdl-v1-final-html/)
14B/ UX: continuing the mid-2021 IIW UX conversation
14C/ Formal Objections on the DID Spec
14D/ Privacy Broadcasting for Privacy Awareness & Assurance
14E/ Have we forgotten to design for consent while we've been busy building for SSI?
14K/ Practical Intro to KERI: What can you do today?

Closing Circle - Open Gifting & Session Announcements for next 5 Sessions

Session 15
No Sessions

Wednesday October 14, 2021 - Day 3

Session 16
No Sessions
Session 17
No Sessions
Session 18
No Sessions

Session 19
19A/ Let's Talk About Layer 1

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

Session 20
20A/JSON Web Proofs - JWTs with Superpowers
20B/ CCG 101: get involved with standards/pre-standards at the W3C
20C/ Teach me about MOSIP
20D/ The Self Sovereign Identity Revolution will Not be B2B
20G/ did:dns and did:dnssec
20H/ Decode IT For Me - Magic explained with human langauge - no-techies!!! bring your questions
20K/ Digital Identity with LEIs: Update on the Verifiable LEI (vLEI)
20N/ Explainers needed - Brainstorming topics/outlines for missing explainers for digital identity and self-sovereign Identity (similar to the VC flavors explained paper)

Session 21
21A/ID Token as VP (OpenID Connect 4 Verifiable Presentations)
21B/ The 7 Deadly Sins of Commercialized SSI 😈
21D/ Decentralized Reputation
21E/ Transatlantic Interop (DHS SVIP + EBSI/ESSIF)

21G/ Mapping Verifiable Credentials to Hierarchical Identification and Declaration
21I/ We're building digital gates to keep people out. Why identity *cannot* be an input to verifications.

UnSession Hour

Session 22
22A/ Power, Politics, Hamlet & Harms
22B/ A Useful Revocation Scheme for BBS+ VCs
22C/ VC Issuance with OpenID Connect (using Credential Manifest?) Part 2
22D/ Privacy Broadcasting #2 Consented Surveillance (including identity management), Lessons from the Physical World
22E/ Decentralized identity for financial inclusion. Field notes from Kenya
22G/ Does login = identity?
22I/ Person schema design — Doing it Wrong? @nytimes
22K/ Safe Internet Use with KERI: Percolated Discovery OOBIS and Spanning Trust Layer

Session 23
23A/ Passwordless Login: The Keys to Secure Logins
23B/ QR codes for Wallets - Threats & Opportunities
23C/ What does Hybrid IIW Look Like?
23E/ Privacy Broadcasting #3 (postponed to next session) Consent by Default - with- A Privacy Controller Credential
23F/ Have we forgotten to design for consent while we've been building for SSI (round 2)
23G/ The Byway
23H/ Trust Taize -Time to Breath and Trust (Quotes and Music)
23J/ Credential Chaining - Verification of VCs in non-trivial Trust Networks (open discussion)
23K/ PAC Theorm Reprice: Economic incentives for Privacy. PAC Layering
23L/ Verifiable Credentials for the Workforce – PoC
23M/ Considerations & Trends in Children's Data Governance & Age Appropriate Design
23O/ Scuttlebutt - the gossiping protocol

Session 24
24A/ Microledger Hands-on - tools and libs where to start and how to use it
24C/ Machine Readable Governance: Theory, Code, and the Future
24D/ Privacy Broadcasting #3 Consent by Default - with- A Privacy Controller Credential
24E/ Killer Whale Jello Salad (WACI PEx update)
24G/ Achieving Full Global Decentralization with the KERI Protocol
24I/ Self-sovereign Applications on “Authorized P2P” Infrastructure: Kepler Design Progress Report
24L/ How to make SSI systems that inspire people to act rather than be acted upon?
24N/ Explainers Pt 2: After Brainstorm -> Planning/Outlining Explainers, Curriculum

Notes Day 1 Tuesday April 20 / Sessions 1 - 5

I Co-chair the DID WG and VCWG, AMA

Tuesday 1A
Convener: Brent Zundel
Notes-taker(s): ?, Charles Lehner

Tags for the session - technology discussed/ideas considered:

DID WG, VCWG, W3C, Verifiable Credentials, Decentralized Identifiers, Open Standards, Q&A, AMA

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

What is the current process?

At this point, the W3C process calls for the Director to determine if the formal objections against the DID Spec will stand.

What role do the people involved in DIDs have in the rollout of vaccine passports?

The participants of the W3C process and their conversations are public, so anyone can take that set and compare it with the set of those involved in vaccine passports

Is the primary objection and dispute resolution primarily related to Mozilla's objection?

Talking about objections to DID (TH Edit: moreover making enquiries about advancements over recent years).
Timothy Holborn To Everyone 11:49:54 AM other work: https://medium.com/webcivics/permissioned-commons-7fc33a1ce23e
https://medium.com/webcivics/tech-for-permissive-commons-c0961b77249e
some old DID related works (noted as Quins, suggesting quads + DIDs)
https://lists.w3.org/Archives/Public/public-schema-gen/2017Feb/

(TH Edit: re below - i didn't ask if blockchain (or moreover Decentralised Ledger Technologies, as to include DHT Hybrids, etc.) was unethrical - not sure who asked.).
Is technology related to blockchain unethical? Some say if it's based on Proof of Work, yes; some say it's more nuanced. Hard to reach agreement. Positive direction with W3C Ethical Web Principals: not official guidance for W3C Working Groups, just a set of ideas that folks in the TAG (Technical Architecture Group) wrote.
Response about Ethical Web Principals: DIDs enhance several: personal accountability, individual control, verifiable data…
If W3C wants to add horizontal review requirement for energy usage, we're happy to try to do that… although it's hard because it's just a data model… none of the methods are official specifications. Bulk of conversation.

Argument: we can't determine if the spec is good enough until there are specified DID methods. Until there are specifications with multiple interoperable implementations, we can't… When chartered the group, that was considered too large a scope - so we are prohibited from specifying DID method specifications. So we're caught (in a Catch-22). We're hoping that the ultimate decision will be that this group did what it was chartered to do, and future groups can do more.

Timothy asks question about "Cool URIs don't change"...
(TH Edit: nb: https://www.w3.org/Provider/Style/URI)
Energy use… could an ontology be created to quantify the energy payload?
(TH Edit - NB: per 'permissive commons' documents above, was part of the design IMO)
Brent: totally possible. But why are we being singled out in particular? Web pages with fancy CSS (and videos, JavaScript) are computationally expensive). Introducing features into CSS increases the computational requirements of web pages. Should this be quantified too?
We think energy use will be one of many criteria to determine appropriate DID methods… along with various decentralization requirements, censorship resistance… a number of concerns any user/implementer ay be concerned with.

Timothy Holborn To Everyone 11:58:34 AM per: https://lists.w3.org/Archives/Public/public-schema-gen/2017Feb/0006.html NB: google doc noted in linke

Brent: … So the DID WG created a Rubric… so implementers can compare.

Rabble asks about Secure Scuttlebuttt… low resource requirements, can run on Raspberry Pi…
Is this the only W3C thing having to with blockchains?

Brent: I think that's a safe assumption

Timothy: respectfully, I disagree…. (TH edit - comments out of context… can provide links if deemed useful) Carvello… linked data ledger stuff… RDF… huge falling-out between Henry(?) ?... can see in the legacy between Turtle notation and JSON-LD… Commercial vs. network aspect… SOLID… Acamy(?)... Legacy about decentralizing discovery… part of the purpose about getting the golden handcuffs out… providing the ability to consume linked data in a decentralied and private manner, as well as having a better provenance over the assets. I can't say (TH Edit: 'I can't see', (different to 'say') - provenance important, re: HTTPA, etc.))how that vision has carried on…. Universal Declaration of Human Rights…

Timothy Holborn To Everyone 11:58:34 AM
per: https://lists.w3.org/Archives/Public/public-schema-gen/2017Feb/0006.html NB: google doc noted in link
Timothy: … excluding beyond the traditional scope of W3C work… perhaps there are threats to international law (EDIT: Inter-national world-order, ie: support for jurisdictions, etc.) and order… to transcend concerns… to have human agency. (TH Edit: "Inforgs" vs. 'Identifiers' as 'identity')
Brent: I would say that desire for individual agency is what drives most of the decentralized identity work that I've been a part of…
… Mobile Driver License already incorporated into Apple and Google Wallets… requires verifiers to contact issuers… doesn't describe what the protocols are for verification of those drivers licenses… that requires different vendors to set up their proprietary processes… a prime example of those golden handcuffs… Once a vendor sets it up and gets it going with Apple and Google, if we get DIDs and VCs and interoperable way

to request and present them, are the driver license authorities going to change from something that's already working for them? We fear not...

Timothy: 2013..2014… no KYC… Identity Credentials… HTTPA 2010… with accountability… built on a DHT… Intention to create an ecosystem… You're not an identifier, you have a semantic input(?)... identifier you have agency over…. Observer… semantic agent… not by an identifier linked to someone else's system…. Don't see how… translates to human rights…
A true worry for me… seeing protests around the world… I want to raise it…

Brent: There are lot of people involved in the community who share your concerns. Generative Identity Group has lots of position statements and guidance. Phil Sheldrake leads that effort…

Kazue: I've been out of contact with W3C - you mentioned VC WG - I thought it was a community group?

Brent: current status: Credentials Community Group (CCG) - a place for anyone to come (W3C member of not) to incubate ideas around credentials and digital identity. CCG created first draft of VC spec… VCWG was created to guide that spec through the W3C process. VCWG published VC Data Model v1 as a standard 2 years ago. CCG also incubated DID Core specification… DID WG spun up to do that… That's the group you took out to dinner in Japan

Kazue: 2019, good times.

Brent: My favorite...
… Passed DID specification through wide review… multiple review periods… In final phases, a number of objections have come up… mostly focused on difficulties in testing how truly interoperable the spec is… We're addressing those objections and anticipate having a resolution by the end of this year. While the DID WG has been working hard, the VCWG has been maintaining that spec, fixing bugs… hope to have a new version of it published by end of year. Future: original plan was for VC WG to begin working hard on version 2 of that specification, along with subspecifiations on signature types for the way VCs interact with DIDs/keys… but now in a holding pattern, waiting for resolution about the DID WG…

Kazue: thank you. Another question: I don't quite remember which draft I read; I had a difficulty understanding the difference between the holder and data subject. Probably my question is…. DID… they should have a secret key corresponding to the public key in the DID document? …. Is it a holder or the data subject?

Brent: Really good question… It's part of an ongoing conversation with the VCWG… The VC Data Model talks about issuer, holder and verifier as roles that entities can play when interacting with VCs… but the specification itself only talks about issuers and credentials subjects. The issue of who or what the credential is about versus who is presenting it is unfortunately something that still needs clarity and to be resolved. For most use cases, the holder and the subject are the same identity… or it's very clear…. For example in supply chain use cases, the subject is "this pallet of steel" - not a person so can't hold keys. So it needs more clarification, I think. Definitely an ongoing conversation.

Kazue: Thank you. One scenario I read about is parent and children… the parent could be the holder, and the children the data subject… something like that.

Brent: Right. We believe the Data model is flexible enough to support use cases like that for guardianship and delegation…. But it's not prescriptive enough [for interoperability]...

Kazue: Thanks
Timothy:
per: https://lists.w3.org/Archives/Public/public-schema-gen/2017Feb/0006.html NB: google doc noted in linke
FWIW: from 2015: https://www.slideshare.net/Ubiquitousau/trust-factory-slides-2015
this might help too: https://www.slideshare.net/Ubiquitousau/human-identity-inforg
started in WebPayments CG which led to: https://www.w3.org/community/credentials/2014/08/06/call-for-participation-in-credentials-community-group/

TImothy: … Golden handcuffs…. Given objections, vaccine passport mechanisms…
(TH - Sought to identify who was involved with VaccinePassports & what market saturation DIDs have with respect to VaccinePassports world-wide).

Brent: No… Patent exclusions, IPR protection… At every step in the process, folks get to call out patent exclusions… Candidate Recommentation… then Proposed Recommendation (current status) another round… This is using a specification that is patent and royalty free, even though it's not yet an official recommendation.

> Timothy: So does that mean… they can take it up with W3C?
> Timothy Holborn To Everyone
> per: https://lists.w3.org/Archives/Public/public-schema-gen/2017Feb/0006.html NB: google doc noted in linke
> FWIW: from 2015: https://www.slideshare.net/Ubiquitousau/trust-factory-slides-2015
> this might help too: https://www.slideshare.net/Ubiquitousau/human-identity-inforg
> started in WebPayments CG which led to:
> https://www.w3.org/community/credentials/2014/08/06/call-for-participation-in-credentials-community-group/
> https://web-payments.org/minutes/2014-09-04-igf/workshop-report.html is also historically relavent...

Timothy: people did a bunch of work… (TH Edit, i noted also - freely - as…) to make sure there is royalty-free patent-? Standards…
A handover system? When a project is started, and when a legal support for that standard is brought about… at the moment, DIDs is not a W3C standard…

Brent: As I said before, the step from going from Proposed Recommendation (PR) to Recommendation involves the same patent exclusion round that other steps involve…
… My reading of the process doesn't differentiate any particular decision… At several points in the process, all the AC members were presented the spec, and given a time period to declare patents. In PR, same thing. As of this moment, the doc is a proposed recommendation, and not encumbered by any patents… To my understanding, there aren't any further moments for people to come in and introduce patent concerns… I think we've gone through all of them.

Timothy: Respectfully, I don't think the W3C… (TH: defines (secured, ie: patents was the inference)) prior art… the respondents… (TH Edit - pre vs. post 'standard' acceptance', is it vendors or is it W3C as the patent-pool management entity) when we did payment standards, we did …. And then IPA (TH Edit: Payments led to Credentials, which was initially defined as 'verifiable claims task-force' as to support focus'), and we split out credentials… effectively the browser companies said… rewrite the thing… (TH Edit - referring to the Payments Spec, produced via webpayments CG) Then Credentials CG was established… for

verifiable claims/passports… (TH Edit - NQR - comment - verifiable claims had a bunch of intended applications, concern has been expressed about Vaccine Passports specifically; alongside concern that other use-cases have seemingyl been set-aside (ie: ontologies on ledgers, etc.) Thank you for the response.

Brent: Luckily, we haven't had that happen with VCs and DIDs… but yes I've heard those horror stories from Manu about Credentials for Web Payments.

method registry: https://github.com/w3c-ccg/did-method-registry
https://miro.medium.com/max/3258/1*iGzdEyUWAzT7TDjU6IUvTQ.png from
https://medium.com/webcivics/inforgs-the-collective-info-sphere-67a660516cfd might also be helpful.
Frederico Schardong To Everyone12:17:43 PM

https://www.w3.org/blog/news/archives/5862 linked http://manu.sporny.org/2016/browser-api-incubation-antipattern/
Kazue Sako To Everyone12:19:18 PM
Thanks, @Frederico. I will take a look
Christian Paquin To Everyone 12:20:46 PM can't hear me?
@Kazue, it took me a few minutes to find... this research paper is quite related to your question:
https://ieeexplore.ieee.org/document/9333857

Timothy Holborn To Everyone 12:19:14 PM
https://www.w3.org/blog/news/archives/5862 linked http://manu.sporny.org/2016/browser-api-incubation-antipattern/

Kazue Sako To Everyone 12:19:18 PM Thanks, @Frederico. I will take a look
Christian: … at airport… reading notes… … Question about VC in general… The VC system…. In a way we tried to build it 10 years ago with …. And failed…. Wallet form factors…
… I see a lot of blink…. Very tied between DID space…. Often considered the same… I see a lot of use cases for VCs outside of decentralied identity… Enterprise scenarios… blockchain related.
… Are there efforts geared toward more enterprise scenarios using VCs?

Brent: I appreciate you pointing out that often VCs and DIDs are talked about hand-over-first, and while they are related standards and seen as components of SSI architecture, each of them has use cases beyond that. I.e. David C., in UK, building for use cases with certificate authorities and X.509 certificates… not using DIDs at all… The VC spec describes a data model that allows any data to be passed along in this envelope in a way that we hope is interoperable… it allows a verifier to have the assurance that the [payload] was not tampered with.... Any use case that can make use of it should look at it, regardless of it is DID-based.

Christian: I see a lot of use cases for … That use VCs… but not aware of any use cases...

Brent: will put link in notes… At this point, because the community that standardized VCs is also the community that standardized DIDs, many use cases are holding them together, but I will be surprised if that stays the case going forward… [many use cases going in different directions]

Christian: …. Vaccine credential… like the CDC card… just a bearer token… in the spec draft, VC with a DID, it got removed half-way, because too much… was needed for that use case.
… There was a lot of… security/identity people saying "What's that".
VC an empty shell… an artifact of what was there before… signed JWS…

… Introduced some friction.... But smart health cards are wrapped in VCs… in a form that might not feel optimal for the VC community…

Brent: I know you said you're not involved in that work anymore, but I think it would be beneficial to raise issues in the VC spec… it has guidance on how to use VCs as JWT… I think for VCI Smart Card creatorse to jump in the VC spec to jump in and say, "here's how we've done it with JWT…." let's work together to make sure it is reflected in the specification…. That would help everyone out… Personally I think the JWT section of the VC spec could be improved.

Christian: … health-care related… FHIR… medical community… that's why it got adopted fast… I guess it might be worthwhile to do a post-mordem to see what could be done better…. A miracle that all these people talked and were able to agree on something… we couldn't because of the time frame… Retrospective… what could be done better… Maybe conflicting with JSON-LD and …. Lower level crypto primitives… pushing for the privacy-preserving signatures and whatnot - don't really care how they're wrapped...

Brent: Give me the data that needs to be signed, and we'll figure out how to sign it in a privacy-preserving way…

Christian: … Containers important… for standards to be adopted…

Brent: I was pleased to hear you were involved with the YouProve(?) work at Microsoft…. I was involved in the first round of designing anonymous credentials in Hyperledger Indie… We liked YouProve…

Christian: …. Blog post…. BBS+... also looking at it again more recently…
… Early on Chaumian signature being used… privacy… blind signatures… for some use cases, all the way to very complicated credentials with some predicate functionality that is hard to specify and implement… as something in between, YouProve is something closer to the simpler thing… but still have feedback that it's too complicated and too slow... Hard to get anything other than …. Adopted. Goal is to get a good use case….

Brent: Applied Cryptography Working Group at Decentralized Identity Foundation has a work item to implement a BBS+ incubation as an incubation as IETF draft.
Kazue: … Surprised to see you here… along time ago… small world…
Christian: I've been away for a few years… now scaling down…. May go back to some more experimental work.
Brent: I hope we can go to real world crypto this year
Kazue: you mean next year. Not sure if will be physical or hybrid… Japan in 2023.
Karim: no question, just attending…
Charles: asking about DID in New York State Excelsior Pass
Brent: I had heard about that… but haven't looked more closely yet… not sure.
Christian: … about verifiable …. Group pushing for …
Brent: Charles was asking about Excelsior Pass… we've also talked about Vacciations… Good Health Pass
Christian: Was anyone here involved in Good Health Pass?
Brent: I was... Got support for BBS+ signatures
Christian: … I would have liked to see such a standard adopted. I heard that in Holland they shipped….
Digital Cooperative Certificate… Surprised…
Karim: but in the end the system got hacked… couldn't get credentials out… don't know how robust it is…

Christian: probably built by some specialized people…. Have some risks there.
… Felt like too urgent to introduce credential there… but now have credentials in our hands…
… A better stepping stone.

Brent: In my view, the VCI and Good Health Pass are not conflicting, just approaching the problem from two different directions. VCI: get it out fast. GHP: what's the best way that people should do this. I think if GHP is right, then both groups will converge anyway. If GHP is wrong, VCI will head in a better direction.

Christian: Yes… the VCI (Vaccination Credential Information) - goal is not to be a COVID "Pass" or "certificate" - it just attests to the clinical fact that you got vaccinated. Then there are different entities/industries that could use that as input…. The travel industry… could give you a "pass" / "green checkmark".... So it just means you got these two doses on these dates, not that e.g. you are allowed to enter restaurants… Not a pass…. Larger than just COVID…. Any immunizations, any … more general than just COVID.
… Now, especially because of the absence of any other passes, people are showing these directly…. Ideally they would be used as input to other passes...

Timothy Holborn (TH) note: whilst i did not highlight it in the DID session, part of the design was to obtain / transcode media (ie: https://www.mico-project.eu/) undertake phonetic analysis, then package it as a 'verifiable claim' - ie: police interview, or law-enforcement interaction with various media, etc - as to ensure, persons are able to take digital evidence (of lived experiences) to a court of law. I've made some corrections above, as may illustrate the merits of said use cases. Otherwise. Cheers. Tim,.

A DID project that does have anything to do with Verifiable Credentials:
https://identity.foundation/didcomm-messaging/spec/

A VC project that doesn't have anything to do with DIDs: https://verifiablecredentials.info/

IIW 101 Session: All About OAuth2

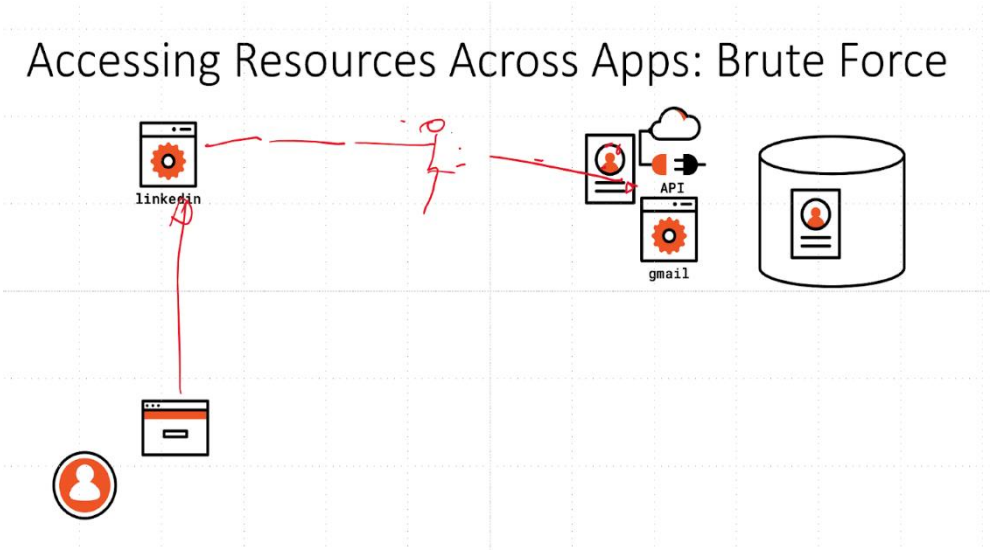
Tuesday 1B
Convener: Vittorio Bertocci
Notes-taker(s): Nuttawut Kongsuwan

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

- Goal — to help absolute beginners to learn about OAuth2.
- The session will discuss terminology, common scenarios, framework, etc.
- The session will not discuss Centralized/Decentralized Identity or SSI.
- Comments on SSI: SSI products are likely to be successful if they are built upon existing technologies.

Scenario 1: Naive Approach

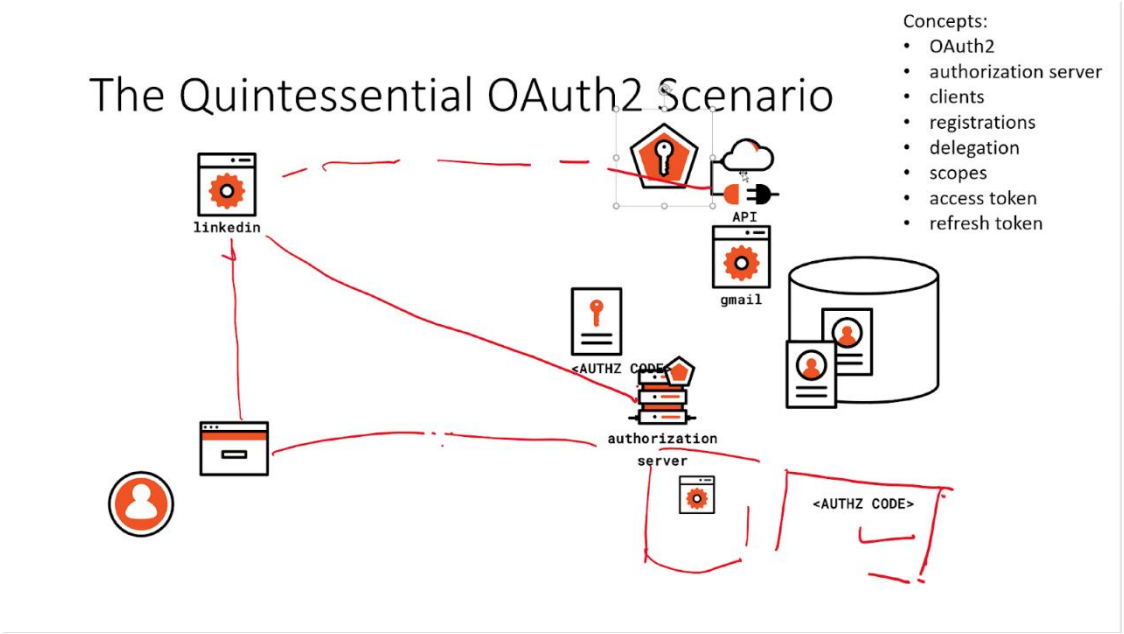
- A user signs in to Linkedin
- Linkedin asks a user to send invitations to all of users' contacts via their gmail.
- User sends their gmail login credential to Linkedin so that Linkedin can send emails on the user's behalf
- This naive approach is problematic as Linkedin will get unlimited access to the user's account



Scenario 2: OAuth 2 Approach (Delegated Authorization)

- Linkedin is registered to the Authorization Server
- Linkedin writes an authorization message to the Authorization Server, asking to send emails for the user
- User's gmail login credential is sent (correctly) to the Gmail server (Resource Server)
- Authorization Server then send a Consent Dialogue to the user asking for the user's permission to perform the request
- If the user consent, the <authz code> will be sent to Linkedin
- Linkedin then sent <authz code> to the authorization server to obtain an access token

- Linkedin sends the access token to Gmail. Gmail will only allow Linkedin to perform the task as specified in the access token and nothing else. Hence, Linkedin will be able to perform only the task that the user consented.

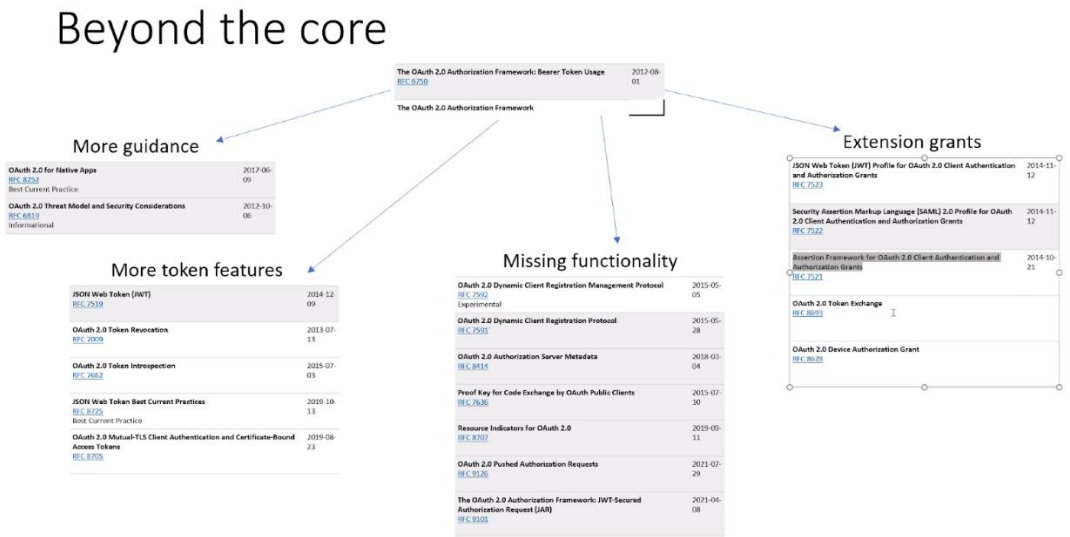


Comments on standards

- Conventional standards arise from pre-existing technologies where lots of people use similar approaches to solve the same problem. Then, these people come together to write a standard.
- Nowadays, some standards arise from non-existing nice-to-have technologies.

Note

- OAuth is not a layer where identity federation occurs.
- Other applications/standards are built on top on OAuth to provide identity federation



A Proposal for SSI Interoperability based on the German SDI projects w/>70 participants

Tuesday 1C
Conveners: Eugeniu Rusu, Hakan Yildiz, Kai Wagner, Andreas Freitag
Notes-taker(s): Eugeniu Rusu, Hakan Yildiz, Kai Wagner, Andreas Freitag

Tags for the session - technology discussed/ideas considered: SSI; Interoperability

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

We started with a presentation on the German SSI projects that initiated this concrete interop project.

PRESENTATION Link (link valid till Oct.13, 2022): *https://jolocom365-my.sharepoint.com/:b:/g/personal/andreas_jolocom365_onmicrosoft_com/EYOzZpPMjjZPoLBSzKIqgOIBCPjURAqD58_ku67Eoz0pOQ*

The participants were widely aligned with our perspective on how to achieve interop across projects and implementations. The discussion itself emerged around the following topics:

The approach with the matrix has been seen as positive, along with the alignment towards AIP 2.0. Questions came regarding:

- Why not BBS+ as of now?
    - Product readiness
    - Revocation (possible solution: https://hackmd.io/kj223D1ZQN29WiusmnPFMA?view from Stephen Curran)
    - Is in clarification for IDunion
- Revocation:
    - Discussed in the wg-applied crypto@DIF https://github.com/decentralized-identity/revocation
    - The discussed approaches are collected in the working group
    - If you want to participate pls. Join the working group!

- What about OIDC Stack?
    - Will be supported in Phase 2
        - SIOP DID Profile 2.0 instead of DIDComm
        - OIDC4VP
        - etc.

Level of interoperability between showcase projects: What will be the level of interop?

- AIP2.0 and then some more incl. OIDC Stack

In the end we recorded the areas of interest for potential follow up session:

- BBS+
- Revocation
- DIDComm v2
- Device Binding
- Where do we work on interop as a community?

For the follow up session we agreed to propose the following questions:

- Where do we work on interop as a community?
    - It would be great to have a single point to work on it
- Which interop type / layer do we address at which community?

The conversation could start with a mapping of existing places:
- DIF Interop WG
- Hyperledger aries
- ToIP
- W3C
- CEN / ETSI

DidComm MythConceptions: de-myth-tifying the most misunderstood opportunity in SSI

Tuesday 1E
Convener: Daniel Hardman
Notes-taker(s): Charles Lanahan

Tags for the session - technology discussed/ideas considered: DidComm, Myths, Implementations

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

Session Slides: https://docs.google.com/presentation/d/1wz1cqUDI8M9w1Q8-gvJ_8zCjefTOd68LmrGj2UCBgI0/edit#slide=id.gefc9b12ddf_0_142

- Myth: Security and Privacy of communications mechanism is only *one* feature of Didcomm it is not the central focus. Security and privacy of communications are considered table stakes in the modern internet
- Myth: Didcomm is re-inventing its own security/crypto
    - Didcomm uses a variety of IETF RFCs and RFC drafts, some of which adhere to NIST specs.
    - Influenced by Jose specs and a variety of mature standards. Mostly focused on structure and high-level conventions in regards to the crypto/security.
- Myth: MITM Gap
    - Didcomm focuses on transport mechanism, the “pipe”, and not necessarily the agents using those dids. MITM is a problem that operates outside the scope of the spec. Very similar to TLS spec.
    - VC’s are where the “human/agent trust” comes from while Didcomm represents the “cryptographic trust”. Mitm attacks usually focus on violating that “human trust”.
- Myth: For Hyperledger Only
    - Did methods, cred types, blockchains/ledgers/kv stores, governance models are all outside the scope of the spec. None of these is hyperledger specific
- Myth: “Not ready”
    - Didcomm v1 has been in production since 2018

        - V2, spec is 4 years old. Dozens of contributors, thousands of man hours at Hyperledger and DIF heading to IETF
    - Interop proven, multiple vendors, implementations in multiple languages, multiple forms of cryptographic support, and multiple crypto dependencies that can be chosen
- Myth: Just another cred exchange approach
    - Undersells the potential within the didcomm spec. The difference between old style apis and didcomm is the generality in terms of what can be done. Old style apis are much more constrained with what's possible in terms of communicating with other humans/organizations/agents.
- VCs are a standard way to say **something** about an identity whereas Didcomm is a standard way to **interact with** an identity. This is one of the primary features of Didcomm.
- "Without requiring institutional facilitators" one of the primary features of didcomm.

Q&A / Comments

- Really cool because Didcomm generalizes and overlays what could be the whole Internet
- Comment on Didcomm design. Security Protocols are incredibly difficult to design and implement. Long history in example TLS of specs being broken not because crypto failed but because protocol was broken. Didcomm could have been implemented using TLS 1.3 instead of Jose.
    - The reason Didcomm team didn't do that (although they started with TLS 1.3) was that they made an intentional design decision not to use TLS 1.3 because they wanted to move away from basing their spec on a transport protocol. They thought about finding a place in TLS spec to put dids but the difference between implementations and specs (in TLS) remain somewhat far apart in the world (some things in the spec aren't implemented in most of the TLS libraries) and so for ease of design they decided to start from scratch.
    - Another reason Jose was chosen over TLS was because Didcomm wanted to be session-less (TLS spec a lot of the time requires a session to exist).
- Jose has many feature requests for perfect forward secrecy but none exist yet. Not sure if that should or should not exist yet.
    - There is a PR against the spec for this feature currently in discussion.
- Privacy / anonymity not addressed in the spec. Do you think this is appropriate?
    - Privacy / anonymity hygiene is typically where privacy/anonymity requirements are often violated in the real world. Didcomm starts there so at least the possibility of privacy and anonymity is potential within the spec.
    - Didcomm cannot enforce restrictions/requirements on Bob's use of Alice's data as that was considered out of scope.
- We're used to ephemeral communication channels on the current Internet. However, with Didcomm we face a future of lifetime communication channels that represent a challenge in logistics, representation, and management between entities (like ATT and customer).
    - This represents a challenge for the future.
- Re-authenticating control of a did by a person for example is a challenge for the future. Assuming Alice has given Bob a did, how does Bob later validate that Alice is actually in control of the Did he gave to Alice?
    - This is def a challenge, there was a recent issue with a didcomm implementation where this issue arose. Will require ongoing work.
    - This link has details but may require wayback machine as current link had them removed https://www.bundesregierung.de/breg-de/themen/buerokratieabbau/e-id-1962112
- Risks of security of storage credentials among other things require thinking about that "human trust" and "cryptographic trust" on multiple levels.

DID and SSI in the NGO and Non-Profit Sector

Tuesday 1F
Convener: Sze Wong
Notes-taker(s): Sze Wong

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

Biometric is one of the way to identify individuals in areas where there is no infrastructure nor other means of identity, the problem is how to secure biometrics raw data so they can be securely stored, e.g. through biometrics templates where only NGO can recreate biometric checks.

Human Colossus Foundation is a working on technology stack which addresses the most sensitive information in unstable ecosystems where addressing privacy is crucial for the citizens.

Assuring data portability and authenticity are key characteristics to try to tackle problems of NGO "revisiting" a location to avoid data de-duplication and onboarding users all over agains.

Example of Digital Identity Architecture designed by HCF
https://docs.google.com/presentation/d/1xbh-XewHxl1LYwoClnn1u6RscpfZlyimhTOwdBX7gWc/edit#slide=id.p

Data is not always under your control (you not always own your data):

Think about the right to be forgotten, when turning it around, how about the right to remember. If someone commits a crime why should society not preserve that information.

Data is not always under your control (or owned by you), and does not belong only to you. Especially in an unstable environment. E.g. did you already subsidize it as support?

This is why in this architecture above you have environment which defacto is observer which holds a bite on some of the data in the ecosystem

There is interesting mechanism which we talk about last IIW about "Break glass for SSI" what if everything goes wrong. And how to take control in case of an extreme situation.

https://www.linkedin.com/in/nickyhickman/
https://www.ontario.ca/page/digital-id-ontario
https://www.happycounts.org/

Should SSI be used for Onboarding process?
Need a separate conference all together

Citizen Precinct Voting, Data, & Comms w/SSI

Tuesday 1G
Convener: Kent Bull
Notes-taker(s): Kent Bull, Trent Larson

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

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

Proposed flow:

- Get a voucher from the party.
- Attendees with a voucher are able to cast a ballot in the meeting.
    - They may use their voucher to attend the meeting.

Started out planning for AGPL to enforce sharing, but Nathan recommended Apache 2.

- Companies won't touch AGPL. Choose a license that allows for companies to expand it with respect for copyright & patents.
- The benefits of building adoption & network is more important than forcing code sharing.

Talk about voting with:

- Dave Hughesby
- Brian Behlendorf - Board of EFF & Mozilla Foundation, experience with licensing

Other players:

- Kent talked with BigPulse about blockchain but they're not interested.
- Votaz is built on Hyperledger Fabric, and Kent doesn't trust that for voting: only the CA nodes can generate keys, and Fabric requires that only the CA can allow key generation/management.

Kent told a story of how a particular Utah party vote was counted by a selected politician's friends.

Group Discussion: What does NOT get adoption for SSI? AKA Failures in SSI

Tuesday 1H
Convener: Kamal Laungani
Notes-taker(s): Phil Wolff, Kamal

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

Barriers

- Onboarding for humans
- Onboarding for IT and devops and IAM
- Short term barriers vs clarity of immediate benefits
- Legacy integration
- Career risk: who goes first
- Career risk: wrangling internal buy-in when the project costs/risks are large
- Lack of control/power over all the participants

Other considerations

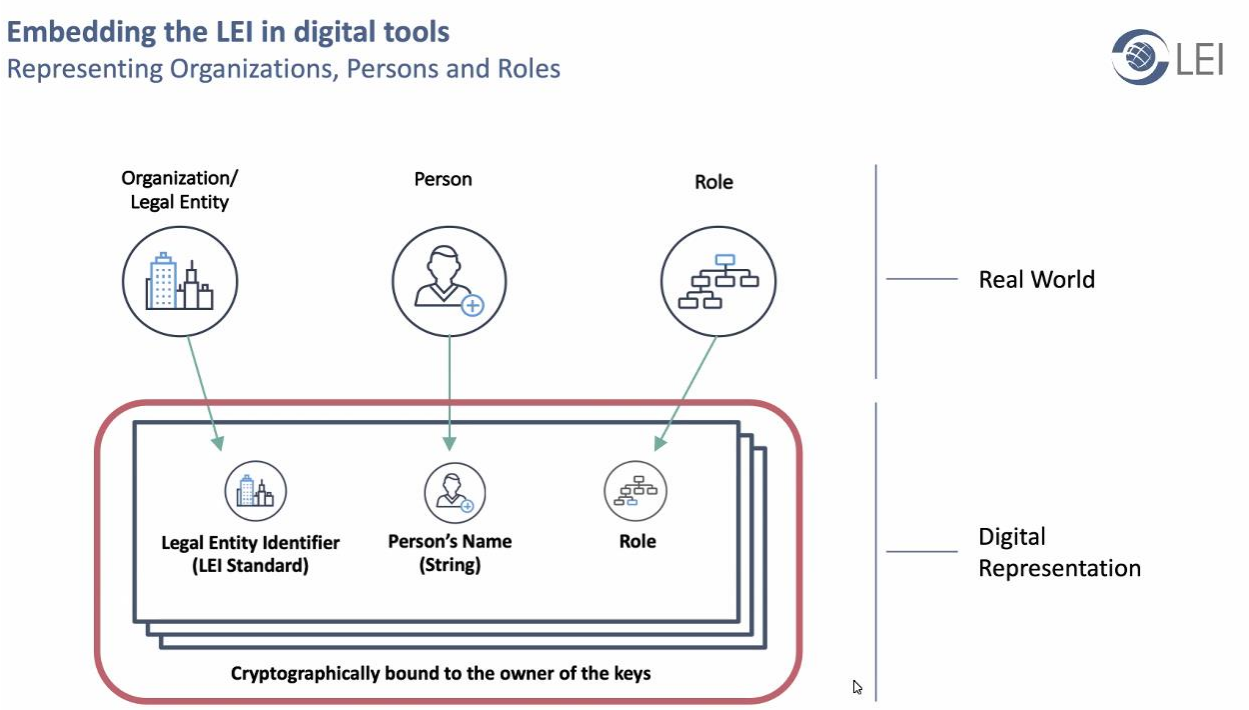
- How hard is it to adopt?
- Cost of adoption
- What are the key drivers of adoption
- Where's the need?
- People don't necessarily care for privacy, until there's a big problem

Digital Identity with LEIs - Update on the Verifiable LEI (vLEI)

Tuesday 1K
Convener: Karla McKenn, Christoph Schneider
Notes-taker(s): Andrew Hughes

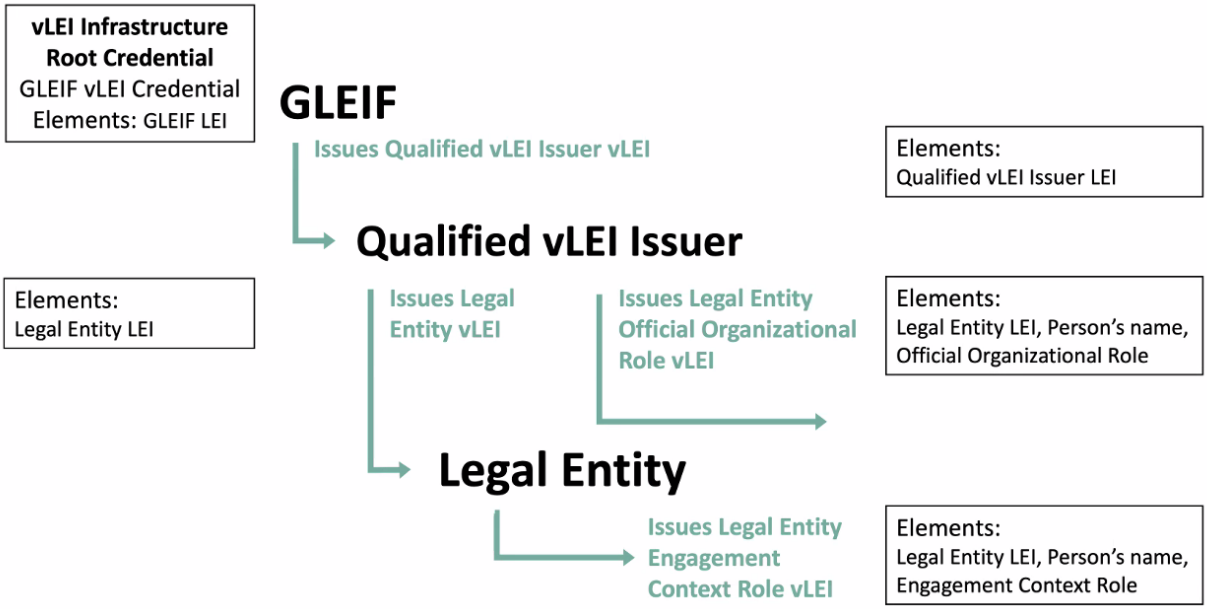
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- **Slide deck**: https://github.com/WebOfTrust/vLEI/blob/main/docs/2021-10-12_Update-vLEI-IIW_v1.1_final.pdf
- Overview of vLEI progress from GLEIF
- Presently LEI require manual verification - vLEI is an attempt to use decentralized identification and verification instead
- vLEI represents Organization/Legal entity & Person & Role



- Waiting for ISO 5009 to be published - Financial Services - Official Organizational Roles

The LEI as a Verifiable Credential – Chain of Trust of vLEI Credentials



vLEI Issuer Qualification Program

Establishing a trusted network of partners

- Preliminary review of the vLEI Issuer Qualification Program
  - Organizations took part in the review
    - 9 LEI Issuers
    - 1 external organization
  - Feedback from the review has been incorporated into program design

Qualification Program Content:

- vLEI Issuer Qualification Agreement
- Appendix 1: Non-Disclosure Agreement (NDA)
- Appendix 2: vLEI Issuer Qualification Program Manual
- Appendix 3: vLEI Issuer Qualification Program Checklist
- Appendix 4: vLEI Issuer Contact Details
- Appendix 5: vLEI Issuer Services Catalog (TBD Service Level Agreement)
- Appendix 6: Qualified vLEI Issuer TrustMark Terms of Use
- Appendix 7: Qualified vLEI Issuer-Legal Entity Required Contract Terms

Qualification testing of the vLEI Beta software
Participating in the sandbox

- Organizations confirmed for the review
  - 8 LEI Issuers
  - 4 external organizations

  (additional participation is expected)
- Functionality covered
  - vLEI Credential issuance scenarios (creating vLEIs)
  - vLEI Credential presentation scenarios (using vLEIs)
  - Identifier and Key Management scenarios

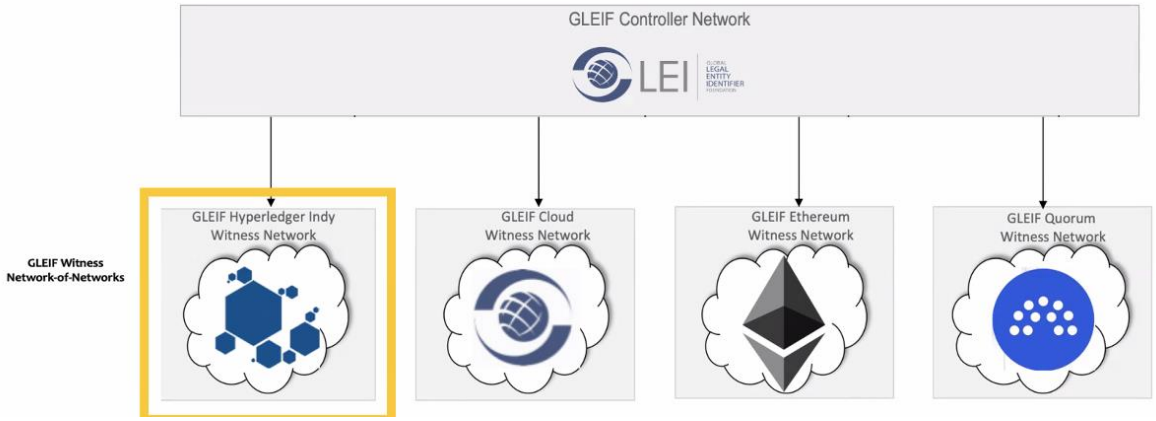
    (ensuring a secure vLEI infrastructure)
  - vLEI Credential revocation scenarios ('retiring' vLEIs)
- GLEIF looks forward to the feedback received for GLEIF to consider for incorporation into the version to be used for the vLEI pilots
  - Feedback encouraged until mid-November
  - Sandbox will be in place until year-end 2021

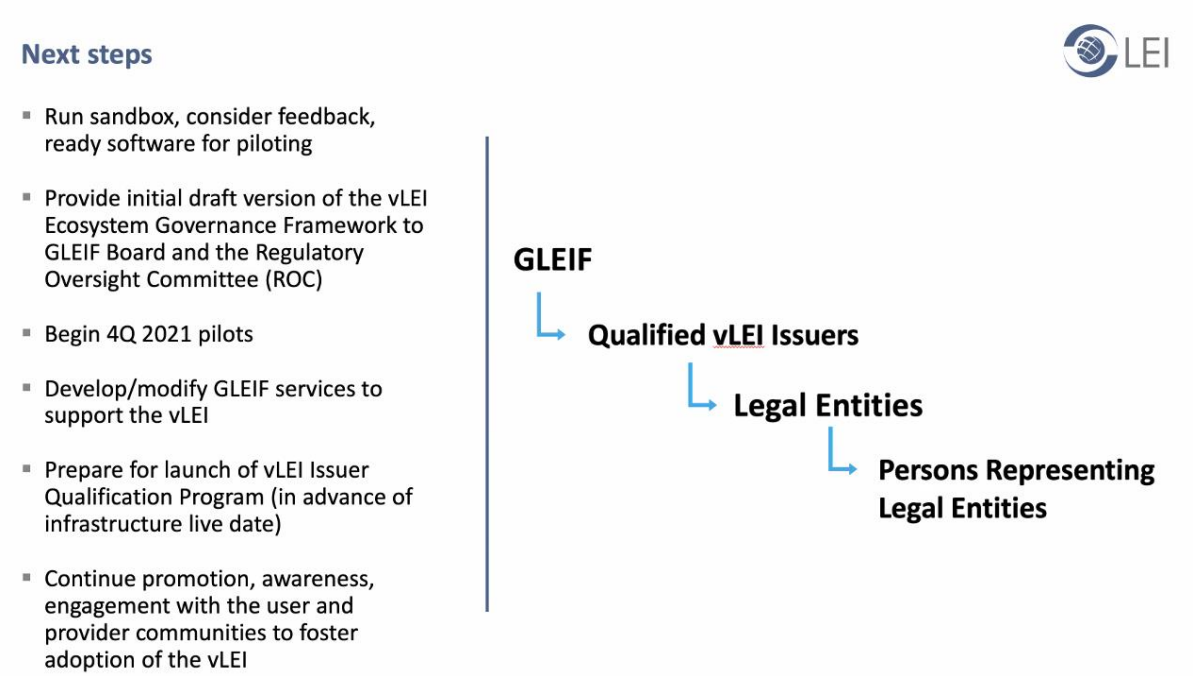
- LEI Issuers can be any organization that passes the qualifications - not just financial institutions or governments - e.g. Bloomberg, Corporate Registries, banks, etc
- Generally attempting to set up a similar governance structure for vLEI Issuers

vLEI Beta software demo – separate IIW session

- Demo entry point

  As a starting point for the vLEI Beta software demo:
  - GLEIF has simulated the issuance of a Qualified vLEI Issuer vLEI Credential by GLEIF to an organization that successfully has completed the vLEI Issuer Qualification Program;
  - and has added this credential to the Qualified vLEI Issuer's enterprise digital wallet.





- Have worked with TOIP to develop initial versions of the ecosystem governance framework
- Pilots start 4Q2021

Discussion

- GS1 comments - GS1 Identifier is very similar to GLEIF/vLEI - doing their own POC and moving forward
    - Question about the data model used - seeking to share code and models
- Deeper dive will happen in Session 2K
- **Self-Addressing IDentifier (SAID)**
- Verifiable Credential chaining spec - VC spec variant
    - https://github.com/WebOfTrust/ietf-said
    -
- Lots of the work is happening in the TOIP ACDC WG
- https://wiki.trustoverip.org/display/HOME/ACDC+%28Authentic+Chained+Data+Container%29+Task+Force
- vLEI is based on KERI for key management infrastructure
    - Look for more KERI sessions this IIW
- Key Event Receipt Infrastructure (https://Keri.one <— everything about KERI)
    - Provenances the key state
    - Provenance logs - Witwicki session today
    - Cryptographic root of trust then all changes to key state are visible
    - **Duplicity-evident key state (to determine if there's duplicity in the key state for any Identifier)**
- vLEI governance includes specification of how entities are managing their keys - and KERI allows visibility
- Discussion about security perceptions about SSI - must put security first
    - GLEIF has been working 'security-first'
    - Note: German government weak security article in Der Spiegel today - not good for the overall ecosystem

https://www.spiegel.de/netzwelt/apps/id-wallet-was-nach-dem-fehlstart-mit-dem-digitalen-fuehrerschein-passiert-a-f4bc10bc-08ab-42b4-9325-5de5cdc66e05

    - Should have interoperable security before interoperability semantics
        - A problem is that we have many security models - and they are not necessarily compatible
        - The security model should be transparent and inspectable
- Self-addressing Identifier
    - If all the major parts of a VC are labeled with a SAID then if any part of that VC are changed, then it's detectable.
    - SAID is content-addressable identifier for VC (so changes to content are obvious)
    - SAID is embedded and bound to the VC content - guarantees no-tamper
    - And now, the reasoning about SAIDs does not rely on the content of the VC - you can work with the SAIDs - like "hidden signatures" in Ricardian Contract literature
    - THis allows the existence of "chained credentials" - hash chained data structure
    - Means that an ACDC is a fragment of a tree of credentials - which can be assembled into a graph of credentials - and allows reasoning on the graph
    - https://weboftrust.github.io/ietf-said/draft-ssmith-said.html
- Privacy - who participates in an exchange (i.e. metadata exposure)
    - Confidentiality - what was exchanged
    - Can protect confidentiality with strong legal guarantees
    - The SAID allows chaining/binding to any legal constraints (boilerplate and contract text)
    - Allows high authenticity and high confidentiality

Human Rights Impact of Identity Protocols

Tuesday 2A
Convener: Adrian Gropper
Notes-taker(s): Adrian Gropper

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

Human Rights Issue:

- How is the efficiency of digital identity going to impact human rights?
    - Rental applications streamlining - diversity of tenants - **forced disclosure and credential design flexibility** -
    - NeonID - Everybody's avatar - **personality science - based on test** - broadcast as with profile photo but also an invisibility cloak - advertisers pay - "test can tell" + behavioral data
    - India DigiLocker provided by gov - is gov the owner? How do I avoid **intermediaries owning our identity**
    - **Need contextual silos** - loss of control over our presentation - business model concerns - reputation -
    - Information Bank creator: Nobody has published human rights as a semantic ontology - human factors have been set aside - **curate your own AI agent to limit (TH: nb - https://medium.com/webcivics)**
    - **distortions** - psy ops - use the courts -
    - Need a guideline - preservation of human rights - **responsibility** -
    - Interface between communication needs RDF - **a fabric** - needs legal interpretation?
    - **Social threats** to an individual
- Why?
    - Efficiency vs. Sabotage
    - A "fabric" of related and unrelated contexts -
    - Quality, quantity, context,
    - Each digital twin produces their own ontology
    - The semantics opportunity for confusion / error and too much data
    - Who decides? Who decides who decides? on the linked data ontology
    - What is the efficiency vector
    - Efficiency tends to be brittle
    - The trap of efficiency is we sacrifice other things
    - Sustainability is important - vs. efficiency
    - Ensuring that people have a rich enough digital identity - not too black and white - as in credit scoring income assessment - diversity of expression
    - Business process integration becomes a problem - talk to a human being is good
    - Ontology vs. decision making does not have to exclude human decision making
- What are possible mitigations to this at the protocol level?
    - Delegation - is it fundamental as in the law of agency -
        - Separate from guardianship
        -
    - Biometrics - added - as in passive facial recognition -
    - Linkage of possession to control
    - Onboard plastic and paper credentials -
    - ACDC - Authentic data / post VC /

IIW 101 Session: OpenID Connect

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

Tags for the session - technology discussed/ideas considered:

OpenID Connect; OAuth 2.0; Claims; Login; Logout; OpenID Certification; Digital Identity

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

OpenID Connect is a simple, widely-used authentication built on Internet standards: OAuth 2.0 and JWT. The presentation described accomplishments, work in progress, and OpenID Certification. There was a good discussion among the attendees about the use of passwordless authentication with OpenID Connect.

See the presentation at https://self-issued.info/?p=2196.

VC Metaphors: Beyond "Shipping Containers"?

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

Tags for the session - technology discussed/ideas considered:

VCs, communication, product management,

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

How do you talk to folks outside of IIW about VCs and DIDs?

DIDComm Reference Implementations

Tuesday 2D
Convener: Alexander Shcherbakov, Vyacheslav Gudkov
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

DIDComm, peerdid, DID, JOSE, JWE, JWS, Python, Kotlin, Java, Rust, ECDH-1PU

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

Reference implementations of DIDComm v2 and Peer DID specifications have been presented.
The following topics have been discussed:

- Brief overview of DIDComm v2 and Peer DID
- Why we need the reference implementations
- What libraries have been implemented (languages, releases, features, examples)
- Interoperability demo
- How to use the libraries in your application

Slides from Session:
https://cloud.dsr-corporation.com/index.php/s/kZEMQeMR5c2sxG5

Open ID Connect for SSI

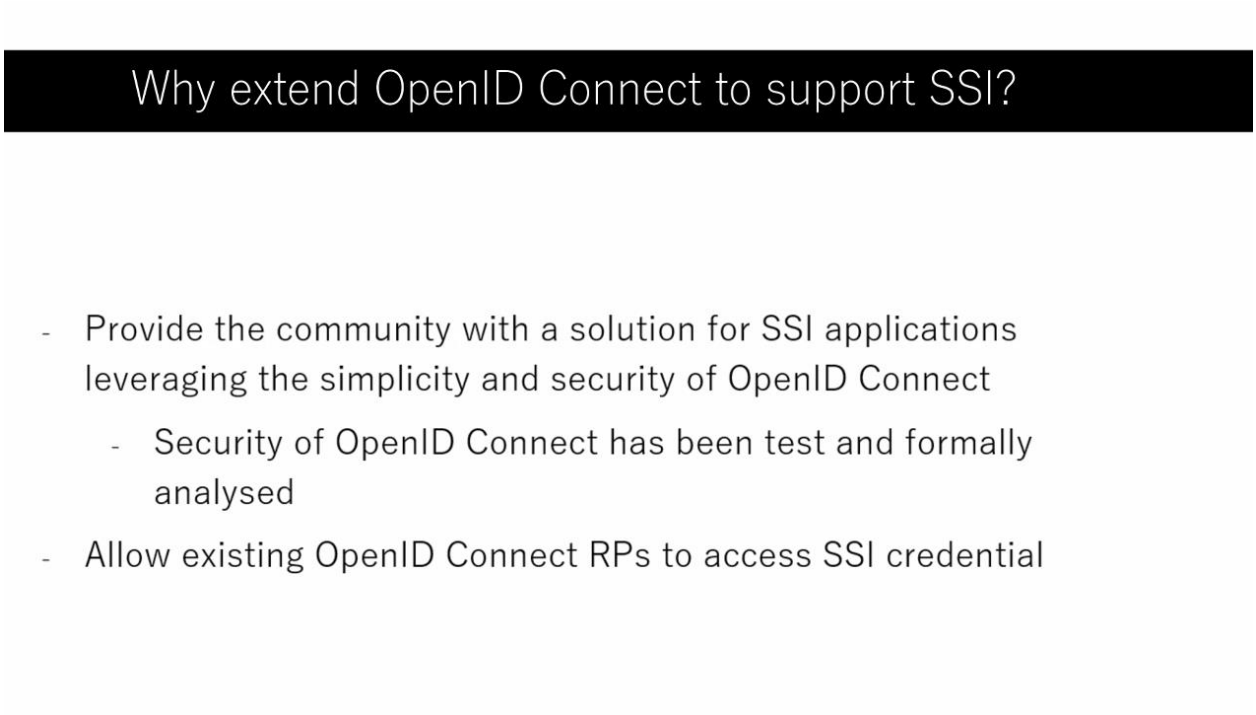
Tuesday 2E
Convener: Kristina Yasuda, Torsten Lodderstedt
Notes-taker(s): Andrew Hughes

Tags for the session - technology discussed/ideas considered: SSI, OpenID Connect, VCs

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

Presentation here:
https://openid.net/wordpress-content/uploads/2021/09/OIDF_OIDC4SSI-Update_Kristina-Yasuda-Torsten-Lodderstedt.pdf

- https://github.com/microsoft/VerifiableCredential-SDK-Android
- https://github.com/microsoft/VerifiableCredential-SDK-Android
- Torsten explains the rationale for OIDC for SSI



- Simplicity is a key success factor
- The components:
    - SIOP v2 (Self issued OP)
    - OIDC for VP (for presentation
    -
    - Claims aggregation (issuance)

What Each Specification Provides

SIOP V2

- Proof of possession of signing keys
- Self-Signed Claims
- Supports on same-device and cross-device flows

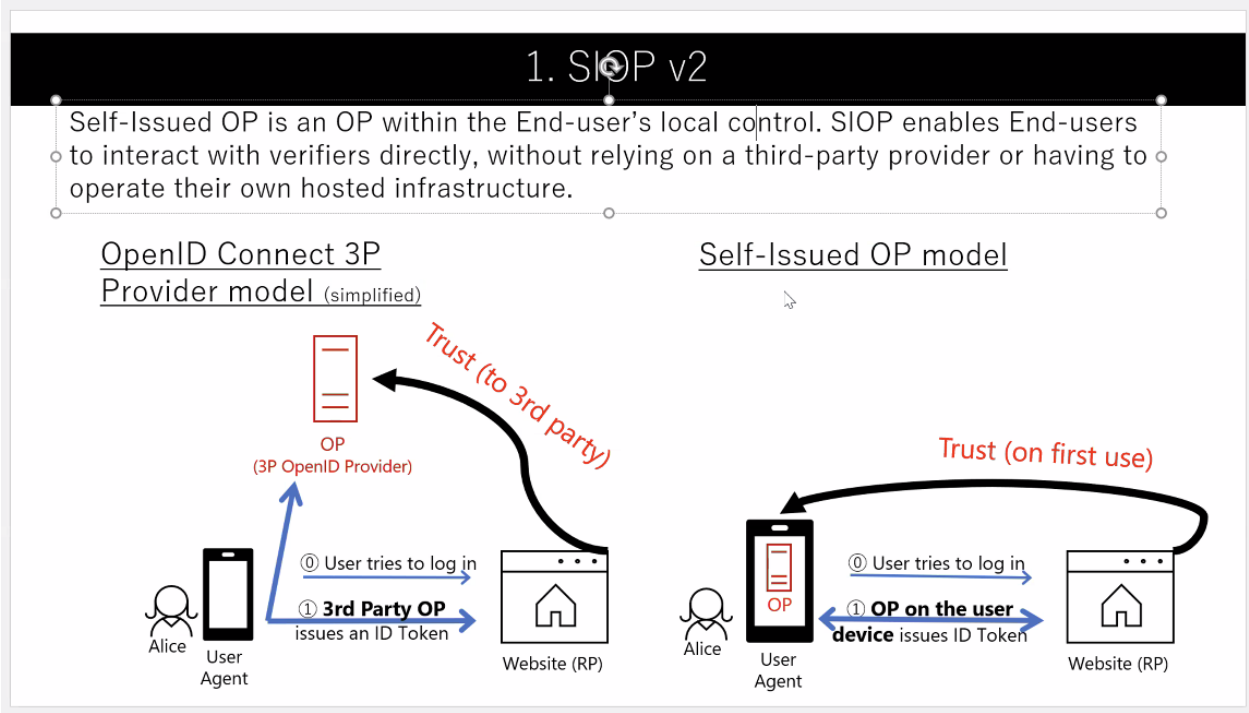
OIDC4VP

- Presentation of verifiable credentials issued by trusted third parties
- Can be used with SIOP v2 and "traditional" OpenID Connect

Claims Aggregation

- Unified approach for intermediaries (Identity Agents) to obtain claims and credentials from trusted third parties
- Will support issuance of verifiable credentials

- This part of the presentation focuses on SIOP v2

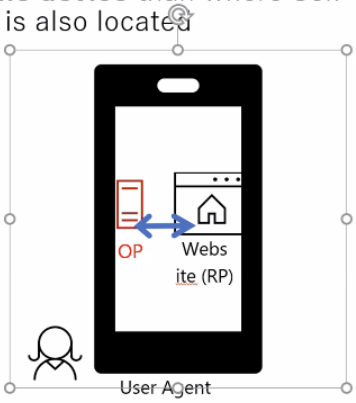


- Comparison of typical OIDC flow vs SIOP flow - example is SIOP as Native app on mobile device
- Trust model requires Trust on First Use for the RP - no prior awareness
- Same-device and cross-device SIOP behave slightly differently - different controls and information are available in each mode

Same-device and Cross-device SIOP

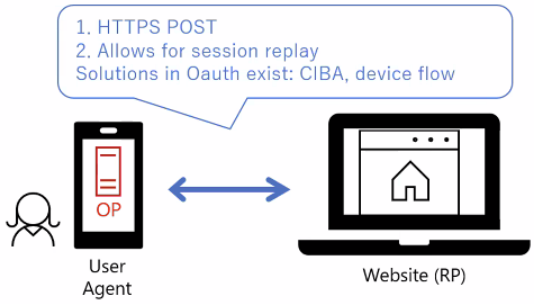
- Same-device

User opens up a RP Website **on the same device** than where Self-Issued OP is also located



- Cross-device

User opens up a RP Website **on a different device** than where Self-Issued OP is located



Kyle Den Hartog To Everyone, 12:54:23 PM

I noticed the self issued identifiers work isn't mentioned here. Is that being delayed at this point while these work items move forward?

Kristina Yasuda (US) To Everyone, 12:54:45 PM

which draft do you have in mind?

Kyle Den Hartog To Everyone, 12:54:53 PM

https://bitbucket.org/openid/connect/src/master/SIOP/draft-jones-self_issued_identifier.md

That's the only one I could find

SIOP request–response example

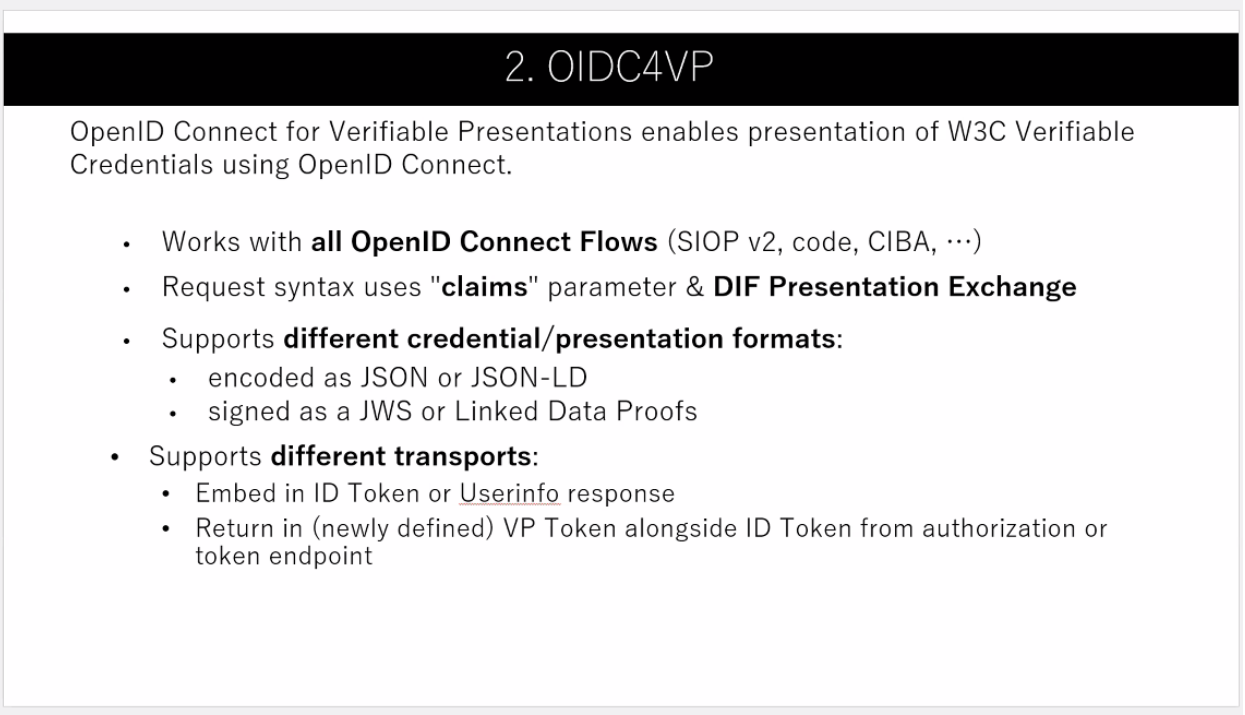
SIOP Request

```
{
  "response_type": "id_token",
  "response_mode": "post",
  "client_id": "did:example:A6YL8ld6k...sNaXniJVu",
  "redirect_uri": "https://client.example.org/cb",
  "scope": "openid",
  "nonce": "acIlfiR6AKqGHg",
  "registration": {
   "subject_identifier_types_supported": ["did", "jkt"],
    "did_methods_supported": ["did:key:", "did:example:"]
    "client_name": "Decentralized Identity Team",
    "client_purpose": "DID Authentication",
    "tos_uri": "https://client.example.org/tos.html",
    "logo_uri": "https://client.example.org/images/did_logo.png"
  },
  "exp": 1311281970,
  "iat": 1311280970
}
```

SIOP Response – ID Token

```
{
   "iss": "https://self-issued.me/v2",
   "sub": "did:example:EiC6Y9_aDaCsI",
   "aud": "https://client.example.org/cb",
   "nonce": "n-0S6_WzA2Mj",
   "exp": 1311281970,
   "iat": 1311280970
    }
```

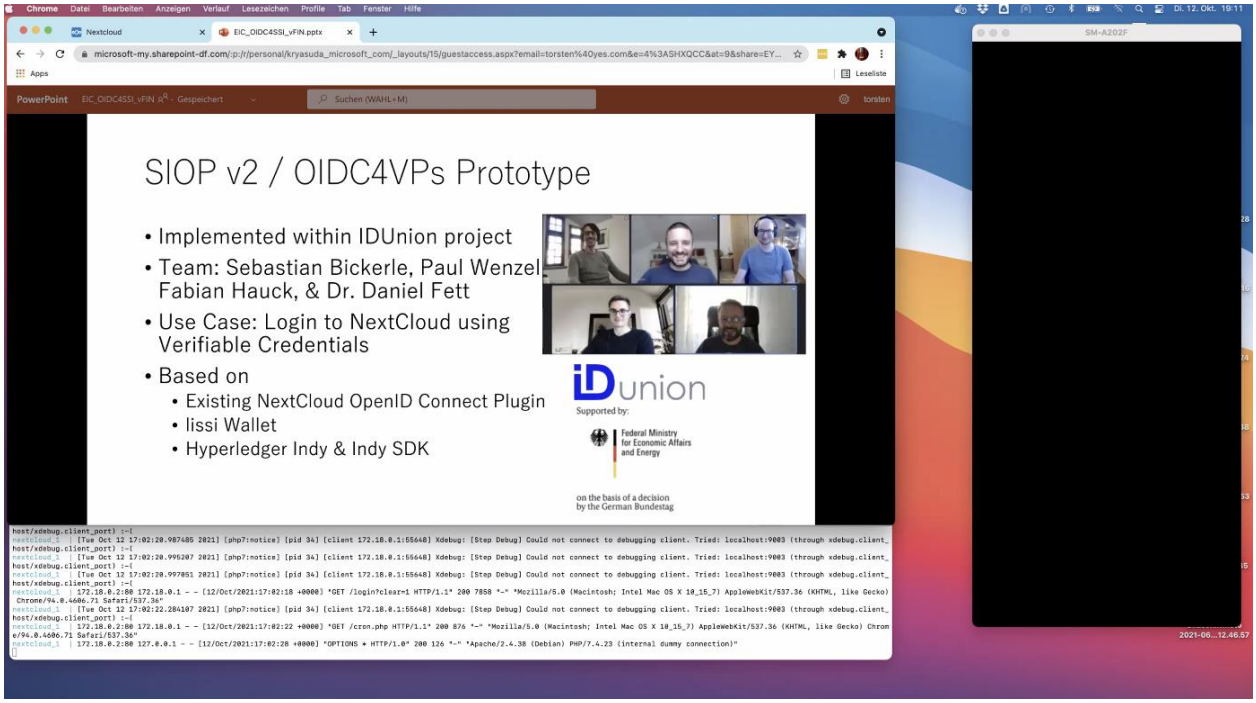
- Note that Form POST and redirect are not possible cross-device
- Note that the sub: in response is critical to the SIOP model

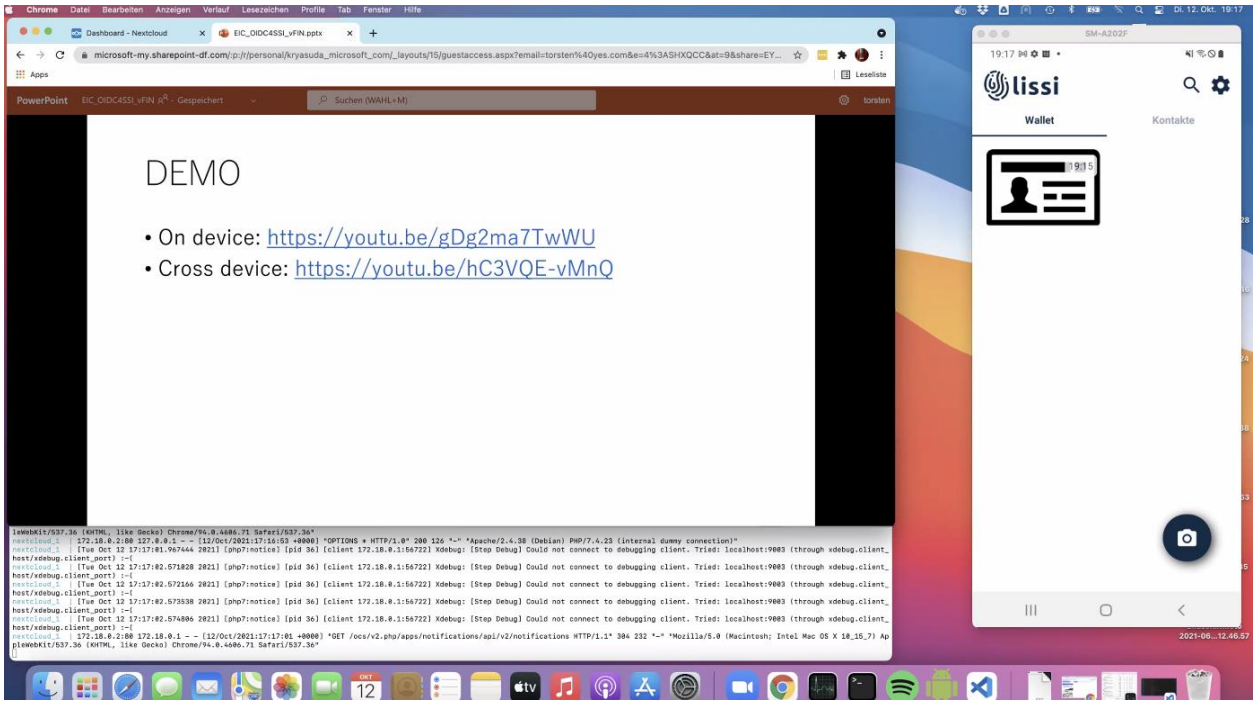


- If you need to assert 3rd party attested claims, OIDC4VP comes into play
- DIF PE is a rich syntax

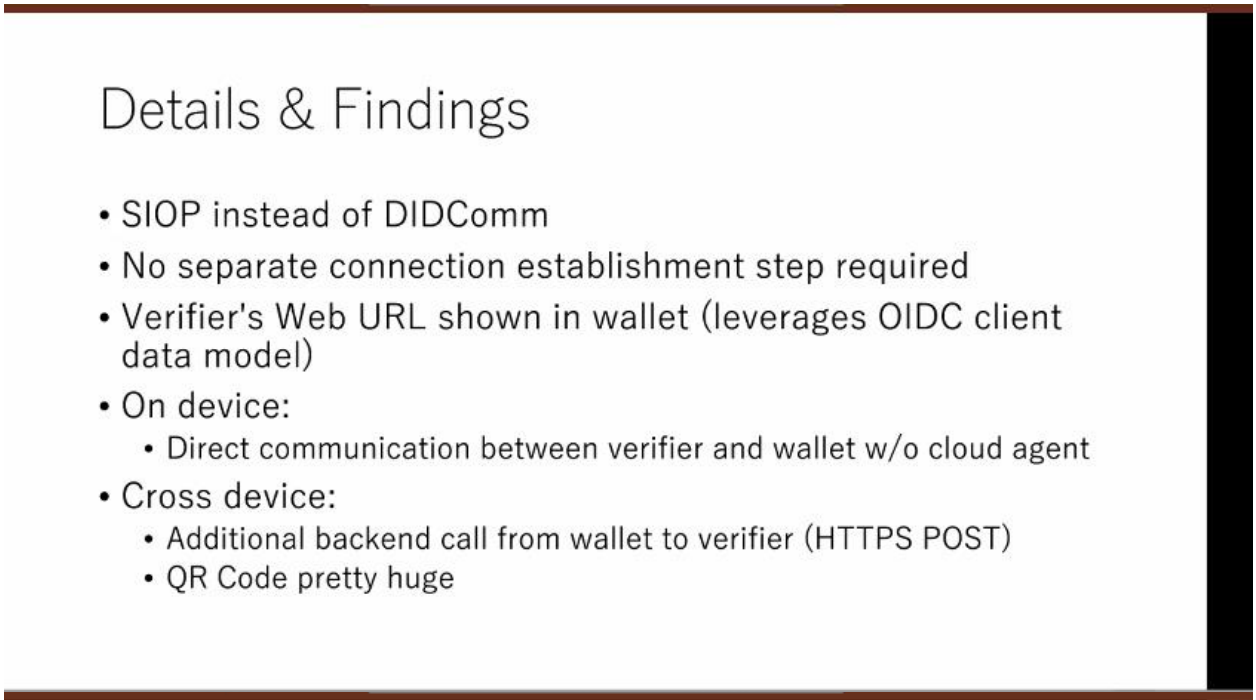
- Note the “claims”: this structure is new
  - “Presentation_definition” is a result of lots of discussion with DIF PE wg
- The example is out of date…

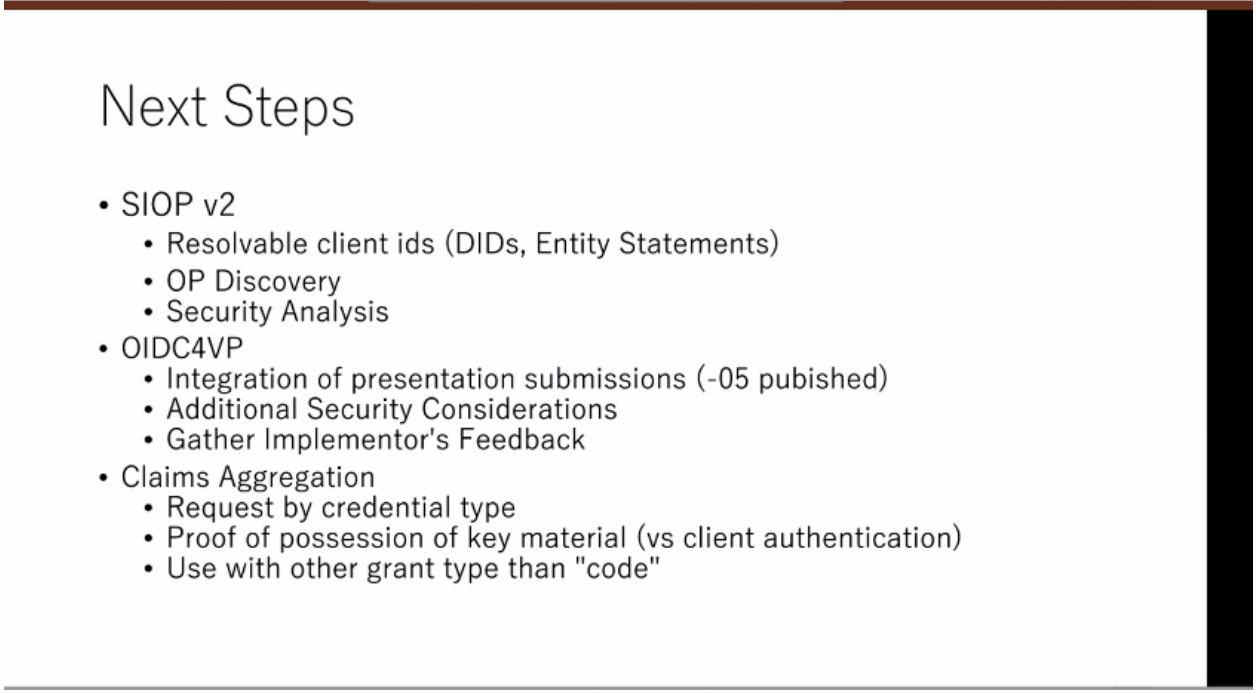
Demo





- On device: https://youtu.be/gDg2ma7TwWU
- Cross device: https://youtu.be/hC3VQE-vMnQ





- Implementors feedback requested:
- https://openid.bitbucket.io/connect/openid-connect-4-verifiable-presentations-1_0.html
- In the prototype, anoncreds were used - to show that W3C VC is not mandatory

Discussion

- Q: what's the history of rolling self-issued identifiers into SIOP?
  - Thinking about replacing the sub identifiers that are scoped to the OP in a way that allows it to be globally unique to allow migration of identifiers to other OPs
  - A: Portable Identifiers (abandoned draft) - allowed traditional OPs to assert sub values that are 'portable' under user's control. Was abandoned because WG didn't see a use case
  - Is the question about normal OPs? Or SIOP OPs?

        - Primary case would be to migrate from Login with xxx to a SIOP
        - But sounds like focus on VP first then if portable identifiers turn out to be useful then work on that
- Q: in the OIDC4VP req-res example slide
    - The response sub: does not have to match the did in the Response VP (verificationMethod)
- Q: is it theoretically possible to implement SIOP as a hosted service e.g. hosted wallets?
    - A: a limiting factor is use of custom scheme
    - But use cases do exist
- Q: is SIOP focused mainly on same-device flows?
    - A: Look at the PARM PR
    - Also security considerations are very different between same/cross device
    - SIOP is optimized for the situation where the OP cannot receive connections

Zoom chat (edited):

09:48:56 From Kristina Yasuda (US) to Everyone:
@Paul - https://github.com/microsoft/VerifiableCredential-SDK-Android
09:49:04 From Kristina Yasuda (US) to Everyone:
https://github.com/microsoft/VerifiableCredential-SDK-iOS
09:49:42 From Kristina Yasuda (US) to Everyone:
it's open for transparency, but please do not take dependency, we might be introducing breaking changes
09:54:23 From Kyle Den Hartog to Everyone:
I noticed the self issued identifiers work isn't mentioned here. Is that being delayed at this point while these work items move forward?
09:54:45 From Kristina Yasuda (US) to Everyone:
which draft do you have in mind?
09:54:53 From Kyle Den Hartog to Everyone:
https://bitbucket.org/openid/connect/src/master/SIOP/draft-jones-self_issued_identifier.md
09:54:58 From Kyle Den Hartog to Everyone:
That's the only one I could find
10:03:27 From Markus Sabadello to Everyone:
The nonce doesn't match here?
10:06:28 From Torsten Lodderstedt1 to Everyone:
correct. Thanks for pointing out.
10:11:40 From Kristina Yasuda (US) to Everyone:
nonce in VP token and ID Token?
10:11:51 From Kyle Den Hartog to Everyone:
Nonce in the request and response
10:12:01 From Kyle Den Hartog to Everyone:
For the SIOP example
10:12:09 From Kristina Yasuda (US) to Everyone:
it did not match in the example? oops, it should, pardon
10:12:50 From Kyle Den Hartog to Everyone:
Was the subject did in the response supposed to match the client_id as well? I wasn't sure about that part
10:14:00 From Kristina Yasuda (US) to Everyone:
sub in the response is user DID. aud matches redirect_uri of the RP
10:15:36 From Kristina Yasuda (US) to Everyone:
iss (who is issuing the ID Token) - self-issued aka SIOP

sub (about whom ID Token is issued) - holder DID
aud (intended recipient of the ID Token) - verifier RP's identifier (redirect_uri)
10:16:06 From Dirk Balfanz to Everyone:
In OIC, normally the Issuer signs the ID Token. I assume this isn't the case here? Is the subject (which is a DID, so it has a signing key) signing the ID token instead?
10:17:12 From Kristina Yasuda (US) to Everyone:
yes, ID Token is self-attested, signed by the user controlled key material (JWK thumbprint or DID), hence self-issued flow
10:17:41 From Kristina Yasuda (US) to Everyone:
@kyle, re self-issued identifier draft, it has been absorbed into SIOP spec
10:17:43 From Dick Hardt to Everyone:
Please post demo links to chat
10:18:01 From Kristina Yasuda (US) to Everyone:
On device: https://youtu.be/gDg2ma7TwWU
10:18:07 From Kristina Yasuda (US) to Everyone:
Cross device: https://youtu.be/hC3VQE-vMnQ
10:18:24 From Kyle Den Hartog to Everyone:
Ahh ok that makes sense - is the general assumption that current OIDC providers won't want self issued identifiers?
10:18:37 From Kristina Yasuda (US) to Everyone:
why?
10:19:05 From Kyle Den Hartog to Everyone:
One of the things I was thinking might be done is the current OPs add support for self issued identifiers which then allow for migration between OPs including migrating to a SIOP provider
10:19:06 From David Waite to Everyone:
Dirk: SIOP is self-asserted authentication and self-asserted claims. Verifiable Presentations enable us to also present third party claims
10:19:50 From Dick Hardt to Everyone:
I scanned the QR code that was shown, and the MS Authenticator app was loaded on iOS. Hmmm!
10:20:06 From Kristina Yasuda (US) to Everyone:
migration is another interesting topic. I would assume SIOP and 3P OPs will co-exist depending on a use-case for a certain period - given we get ISOP correctl
10:20:07 From David Waite to Everyone:
Formerly if you wanted claims by a particular party, you typically had to SSO directly with them.
10:20:37 From David Waite to Everyone:
Dick the wonder of the openid:// uri scheme 😄
10:20:45 From Kristina Yasuda (US) to Everyone:
SIOP discovery on iOS is the known issue - why we recommend universal links in the spec
10:20:46 From Vittorio Bertocci to Everyone:
"for a certain periond"? Do you expect SIOP to replace existing tech?
10:20:58 From Kyle Den Hartog to Everyone:
Yup agree with that assessment
10:21:32 From Kristina Yasuda (US) to Everyone:
Android, allows wallet selection even among same custom schemas
10:22:52 From Kristina Yasuda (US) to Everyone:
-05 https://openid.bitbucket.io/connect/openid-connect-4-verifiable-presentations-1_0.html
10:23:55 From Markus Sabadello to Everyone:
Anoncreds over OIDC? wow!
10:23:59 From Kristina Yasuda (US) to Everyone:

thank you PE for allowing to request not just VCs, but also anon creds is the trick here I guess
10:29:12 From Ivan Basart to Everyone:
Please, don't forget to share the ppt! Is a great presentation :)
10:29:27 From Kristina Yasuda (US) to Everyone:
https://openid.net/wordpress-content/uploads/2021/09/OIDF_OIDC4SSI-Update_Kristina-Yasuda-Torsten-Lodderstedt.pdf
10:31:15 From Oliver Terbu to Everyone:
imo, they do not necessarily have to match
10:31:47 From Kristina Yasuda (US) to Everyone:
the examples in the one above are a little outdated - will put a link to an updated one in the slides to the updated one
10:32:18 From Kyle Den Hartog to Everyone:
You could use the subject did in the ID Token as a communication did, where as the verificationMethod is a persistent did used for different personas
10:32:33 From Kyle Den Hartog to Everyone:
The separation allows for crossing personas if needed
10:32:41 From Oliver Terbu to Everyone:
in case VCs have DIDs (pairwise), and one want to have a pairwise DID per RP, then all DIDs don't have to match. sure, it will at least those DIDs but would preserve privacy in case you don't use bbs+ w/ privacy-preserving holder binding
10:34:25 From Markus Sabadello to Everyone: Thanks, makes sense

Evolution and Structure of Cryptographic Thought

Tuesday 2G
Convener: Will Abramson
Notes-taker(s): Will Abramson

Tags for the session - technology discussed/ideas considered:

Cryptography. Evolution of knowledge. Genesis and development of a scientific fact.

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

Cryptography emerged as an academic discipline in the 1970's with the introduction of public key cryptography by Whitfield Diffie, Martin Hellman and Ralph Merkle. Since then it has become a highly systematised area of human knowledge, built on strong mathematical foundations that have been developed across the last 500 years. At least.

This systematisation of knowledge was directed by conceptual descriptions of ideal distributed digital systems that researchers throughout the 80's anticipated would be useful and important for an advanced information society. They were looking to the future that we now inhabit and imagining the tools and technologies that would empower individuals, protect privacy and promote decentralisation.

David Chaum in his 1985 paper Security without Identification stated.

“The architecture chosen for these systems may have a long-term inpact on the centralization of our economic system, on some of our basic liberties and even on our democracy”

In this paper Chaum proposed developing a cryptographic credential mechanism that has many parallels to the work of SSI.

This session reflected on how cryptographic primitives and protocols have been developed to meet the requirements of the conceptual idea proposed by Chaum. It also questioned whether the identity community really acknowledges or appreciates the rich fund of knowledge that has and continues to be produced within the cryptographic discipline.

Cryptographic thought products have matured from abstract theoretical concepts, to well defined, provably secure and efficient cryptographic protocols realised in a concrete mathematical setting.

Not only that but these thought products are now transitioning from theory to practice, with implementations and the experience of implementing these protocols increasing exponentially. It is now possible to design software artifacts that can guarantee some of their properties such as security, forward-secrecy and non-correlation from well understood mathematical equations as opposed to trust that must be placed in an organisation to act responsibly.

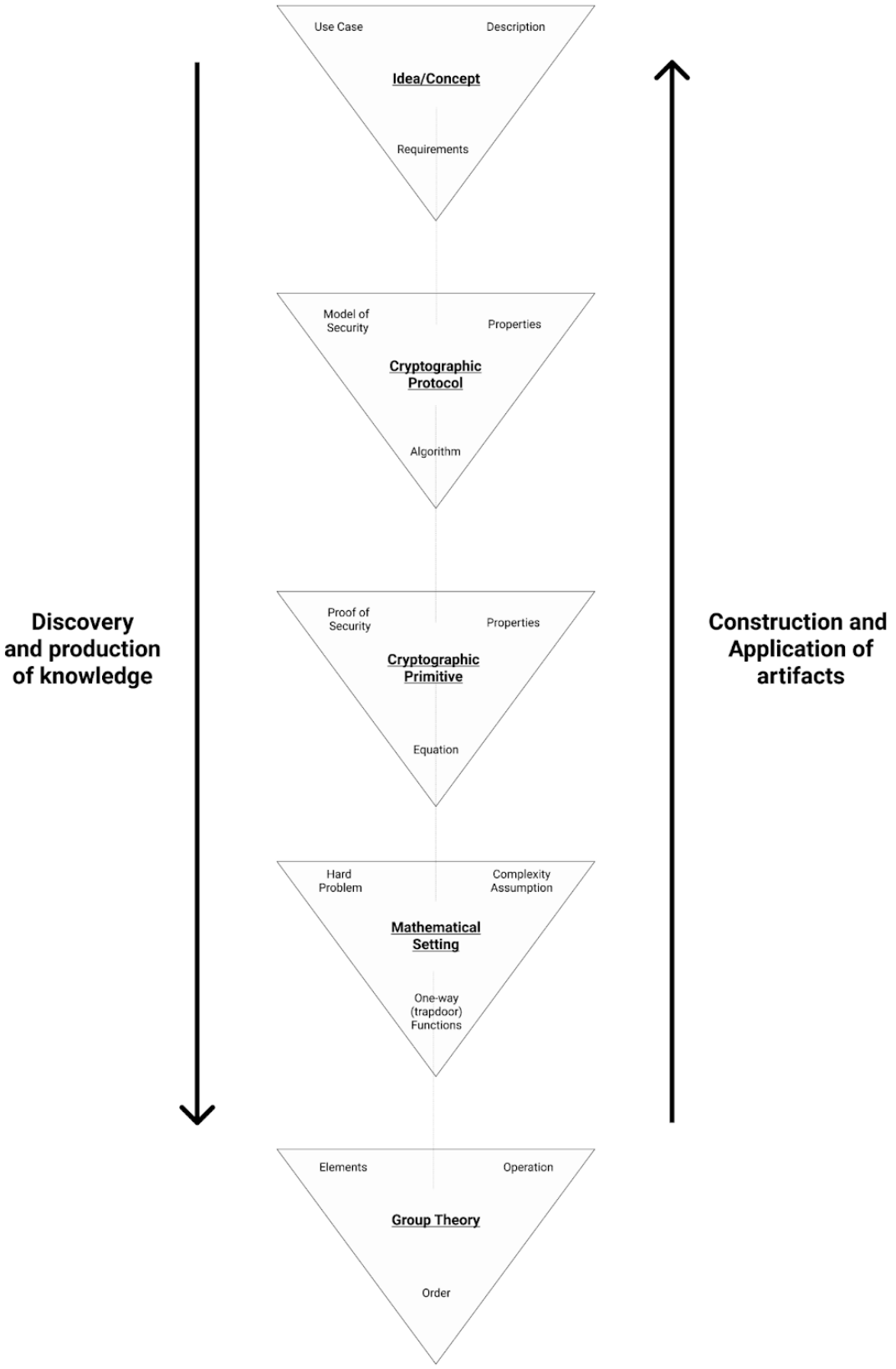
I just wonder if we as a community really understand and appreciate what cryptography can do, and what it will be able to do for us in the future.
Digital signatures are only the beginning.

Related Material

- Must read series. This is our history. People have been working on these problems for a long time https://pet3rpan.medium.com/history-of-things-before-bitcoin-cryptocurrency-part-one-e199f02ca380
- My thoughts are influenced by this book https://press.uchicago.edu/ucp/books/book/chicago/G/bo25676016.html
    - Are cryptographic and identity communities two distinct thought collectives? Do they share enough intercollective interaction?
    - How do the “facts” within the identity community change the way we perceive the those from the cryptographic community?

Questions

- What can our community learn from the work within the cryptographic discipline?
- How do we ensure we are building systems that are flexible enough to incorporate the cryptographic innovations coming down the line instead of restricting them?
- Why are advanced cryptographic techniques that have been developed over the past 50 years specifically to preserve privacy within digital interactions so often overlooked or dismissed in favour of a basic digital signature scheme?


Use Case
Description
Idea/Concept
Requirements
Model of Security
Properties
Cryptographic Protocol
Algorithm
Proof of Security
Properties
Cryptographic Primitive
Equation
Hard Problem
Complexity Assumption
Mathematical Setting
One-way (trapdoor) Functions
Elements
Operation
Group Theory
Order
Discovery and production of knowledge
Construction and Application of artifacts

Premature Interoperability/Standardization

Tuesday 2I
Convener: Darrell O'Donnell
Notes-taker(s): Darrell O'Donnell

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

PRESENTATION: https://continuumloop.s3.amazonaws.com/PrematureInterop-ContinuumLoop-Strategy-Standards-and-Interop.pdf

Other notes:

- https://github.com/decentralized-identity/waci-presentation-exchange
    - Last IIW called -> WACI-PEx "killer whale jello salad"
    - A place for Aries to go
- GoodHealthPass - some examples of conformance.
    - https://www.goodhealthpass.org
    - https://trustoverip.org/get-involved/good-health-pass-implementation
- DID formal objections raised by Google, Apple, Mozilla
    - https://msporny.github.io/did-core-formal-objections
    - https://www.w3.org/2021/09/21-did10-minutes.html
- Canadian Government had a good starting project on interoperability
    - https://github.com/canada-ca/ucvdcc
- Suggestion for interoperability profiles.
- It might be good to have interoperability working before going to standards (such as W3C).
- General feeling that things are going in the right direction - there are no proprietary guard rails going up.

GLEIF vLEI: Distributed Multi-Sig Delegated Credential Issuance with KERI & ACDC

Tuesday 2K
Convener: Phillip Feairheller, Kevin Griffin
Notes-taker(s): Charles Lanahan

Tags for the session - technology discussed/ideas considered:
GLEIF, vLEI, multi-sig, KERI, ACDC, delegated credentials, chained credentials

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

Presentation Slides

Qualified vLEI Issuer vLEI Credential => QVI
Legal Entity vLEI Credential => LE
Legal Entity Organization Role vLEI Credential => OOR
Legal Entity Engagement Context Role vLEI Credential => ECR

- Demo
  - Need something that is always on. **Witness Network**.
  - Need an identifier.
    - Transferable identifier in keri (means we can rotate the keys). The witnesses in the network are picked, we then derive a key from the witnesses' keys
  - Agent then has multi-sig group identifier
- ACDC Feature overview
- Overview of ACDC Credential compact field labels.
- Overview of how an LEI - Chain of trust is laid out.
  - GLEIF -> issues -> Qualified vLEI Issuer -> issues -> vLEI
- Overview of various credentials produced in above chain
- KERI features
  - Autonomic, transferable, non-transferable ids
  - Witness/watcher networks
  - Async distributed multi-sig protocols
  - Delegation
  - Public transaction event logs
- vLEI arch overview

Q&A / Comments
- Store and forward capabilities will exist via witness networks because not all agents will always be online.
- There is a trade off between authentic communication and irrefutable communication
- Management of keys in a decentralized world will always be a problem to solve for the user in regards to usability.
- Is multi-sig really necessary in the real world?
  - For entities operating as roots of trust probably, for individuals probably not.
- Is there "vendor lock in" in regards to keri?
  - Not so much, KERI is attempting to become an IETF spec without vendor lock in.

- Comment: Multi-sig as a term means something different from what cryptographers mean. Everyone has to trust each delegator. By using a cryptographically defined "threshold signature" we gain features in the protocol that don't need governance frameworks.
    - Delegation and issuance is different.
    - KERI was implemented with an objective to be able to plug and play various protocols and cryptography that may arise in the future so its very generic and built to be extensible. These types of schemes could (and probably will) be added in the future.

Presentation deck can be can be found here:
GLEIF vLEI: Distributed Multi-Sig Delegated Credential Issuance with KERI and ACDC

Need for Hardware Backed Crypto on the Web! (Would enable SSI with no mobile apps required.) Why we need to advocate as a community

Tuesday 3A
Convener: Liam McCarty (Unum ID)
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:
W3C, WebAuthn, WebCrypto, DIDs, wallets, VCs

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

SESSION INFO:
tl;dr:
We need community action to advocate for general, hardware backed cryptographic signatures on the web! This would make it possible to build decentralized identity wallet web apps, not just mobile ones, dramatically improving the odds of adoption.

Short Summary:
Decentralized identity efforts have typically relied on mobile app wallets, since mobile operating systems offer crucial functionality, especially hardware backed cryptography and device biometrics. But mobile app wallets face enormous barriers to adoption because people are unlikely to install new apps they don't yet know the value of. Mobile SDKs only partly address this problem because they must be embedded in host apps that many people may not yet have installed, and they must work largely behind the scenes, complicating the "sovereignty" of users over their identities.

Imagine if a web app could do the cryptography and biometrics a mobile app can. This would enable web app wallets, which have almost zero barriers to adoption, as users can access them from a URL rather than through an installation process. The result would be a dramatic increase in the usability of decentralized identity tech and therefore the odds of its adoption.

The problem is, current web standards don't support what's necessary! WebCrypto enables general cryptographic signatures but not tied to device hardware. WebAuthn enables hardware backed cryptographic signatures but only for the very narrow use case of authentication. I've made proposals to each of these groups to effectively combine the two functionalities to achieve general, hardware backed cryptographic signatures on the web, but each group is in a bind. WebCrypto committed awhile back not to focus on hardware, and WebAuthn in its very name has a mandate only for authentication.

So, at this point, we need to rally the community to support expansion/combination of these specs! It would be a true game changer for decentralized identity tech.

Links:
My presentation to the DIF Identifiers & Discovery WG on this topics (September 13): https://github.com/decentralized-identity/identifiers-discovery/blob/main/agenda.md#meeting---13-september-2021---1400-et-recording
WebAuthn W3C spec: https://www.w3.org/TR/webauthn-2/
WebCrypto W3C spec: https://www.w3.org/TR/WebCryptoAPI/
My proposal on WebAuthn GitHub issues: https://github.com/w3c/webauthn/issues/1608
My proposal on WebCrypto GitHub issues: https://github.com/w3c/webcrypto/issues/263
(Abandoned) Hardware Based Secure Services W3C group: https://www.w3.org/community/hb-secure-services/
(Abandoned) Hardware Based Secure Services W3C spec: https://rawgit.com/w3c/websec/gh-pages/hbss.html

Slides:
https://drive.google.com/file/d/1o7VuanEdJqnqVZGvzfgHmGp1eO17ETWd/view?usp=sharing

IIW 101 Session: UMA/User Managed Access

Tuesday 3B
Convener: Alec Laws
Notes-taker(s): Alec Laws

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

Session Slides presented: https://identos-public-dropbox.s3.ca-central-1.amazonaws.com/uma/2021-10-13+IIW+UMA+101.pdf

Highlighted key differences between standard OAuth and UMA. Including the difference technical, business, legal and privacy goals and outcomes

Discussed the role of data schemas and standards
- uma doesn't specify data standards
- RSs own the definition of resources and scope, and their registration at an authorization server
- authZ server follows authorization assessment set math to make policy decisions over registered resources and user policy

- some profile/extension work has been done to consider an AuthZ Server that defines or coordinates data schemas to drive RP/RS interop in wide ecosystems

Discussed the intersection of UMA with SSI and verifiable credentials

- UMA is separate from identity systems by design
- Has hooks and patterns to work with existing identities (OIDC, SAML, SSI or otherwise)
- Through claims gathering or pushing depending on the ecosystem size

HumanOS & IIW: Fit & Finish of Neuro/Technology at IIW

Tuesday 3C
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:

Discussed: Where and/or how does our neurology dovetail or collide with technology at the data and code level.

Discussed: Is the body's complexity as a functional model re-delegating/bounding functional data points (like cells in a living system) a benefit in data-scape/data system management?

O – rigid compartmentalization of "relying systems" (read as human areas of knowledge/awareness) may cause incongruent outcomes. If you are a doctor who is expressing political sensibility which interferes with valuing other scientific truths sensibility may go rather sideways. (AJ)

O - hormones>catalyzing reaction (generation of data)

O - hormones are pervasive as they travel through the bloodstream and therefore affect the system at large through a version of saturation whereas nerves have distinct endpoints directed at specific sensory or notification function. (AK)

O - email 1 to 1, 1 to many more nerve like

O - providence of data is like the immune system in that it recognizes self and non-self

O - unlike the body, data can exist in a number of distributed, potentially boundless systems and therefore it is subject to that number of idiosyncrasies, each possibly with different data priorities and sensory characteristics.

O - design of systems and spaces in the digital landscape are well served by modeling real world analogues regarding UX and human behavior. To design a digital system, space or tool in the digital landscape without a real-world tether may create process/awareness short-sightedness with great implications.

O - at what layer does who/what get to apply and influence the optics/lens through which HumanOS (raw experience) data is compiled? Our brains have already processed by the time we experience something.

O – excellent trust as a relationship w/the future diagram (per Wip)

O - trust is rather contextual regarding risk assurance so thinking vulnerably may put the brain in a more base nature space of consideration. "I trust my sister with my kids but not my bank. I trust my bank with my money but not my sister."

O - is assurance of the risk outcome of a situation a formulaic encouraging or discouraging trust (investment a risk reward choice)? If I'm standing next to policemen in a public space I may have more assurance (therefore I trust them that I'll be cared for. In that space if I make a comment exposing my misalignment with an opinion or action (a vulnerable/risky position sometimes) somebody will not grab my hat and pull it down over my head because I am likely assured that law-enforcement would "break it up", probably before the risk cost went beyond my comfort. If I was an outlier expressing divergent thinking in the midst of an intimate community, my sense of a positive risk reward assurance of not catching some heat may suggest that I can't trust my relationship/position with the group. Vulnerability lives in this space?!

O - what functions are we creating w-VR? Maybe moving to tier two re-metaphysics through these opportunities?

O – Re: force of technologies (VR): What about the idea of the technical precariat? Those showing sensitive psycho-metrics suggesting deep & non-real world internalization experiences may not be healthy for them or those around them… How well does an individual segregate and restrain the values developed in those spaces from leaking into real world actions and implications?

If tech is there to help us know who we are, it's not the idea that the opposite happen". Magic Leep 3 minutes scrambled mind affect. "Maybe to understand multiple realities I would prefer to speak with my medicine man friend."

VC Issuance Using OIDC

Tuesday 3E

Convener: Kristina Yasuda, Oliver Terbu, Tobias Looker, Torsten Lodderstedt
Notes-taker(s): Andrew Hughes (1st half), David Schmudde (2nd half)

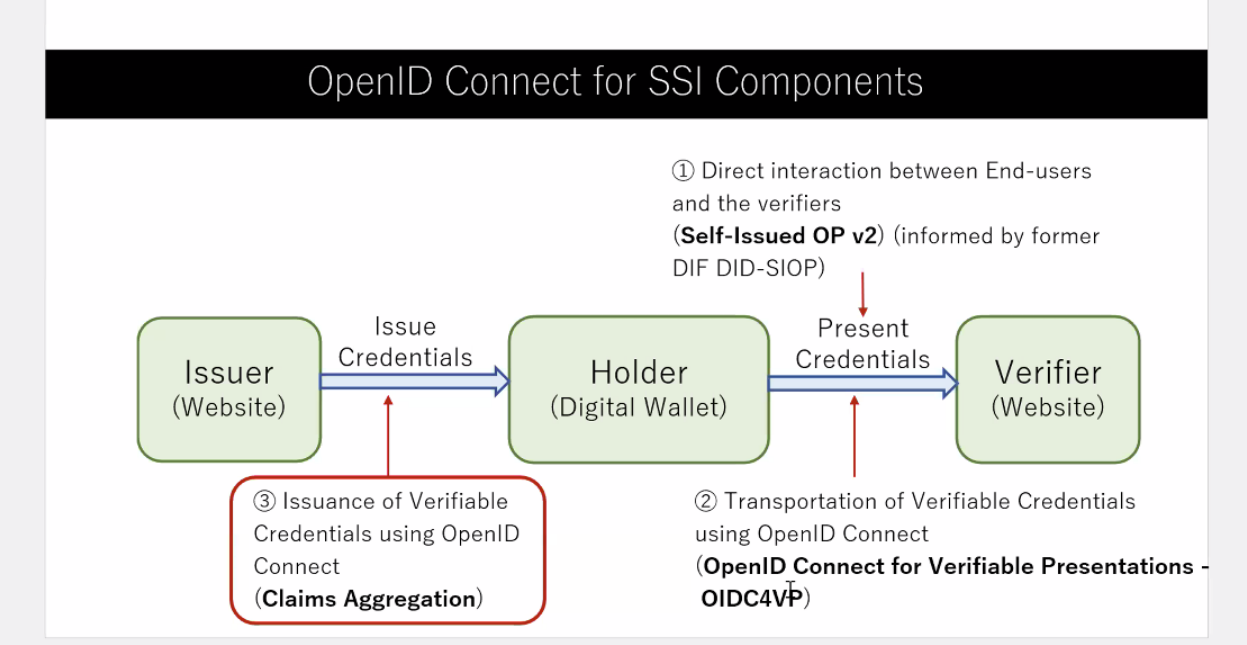
Tags for the session - technology discussed/ideas considered:

VC, OpenID Connect, Credential Provider, Claims Aggregation

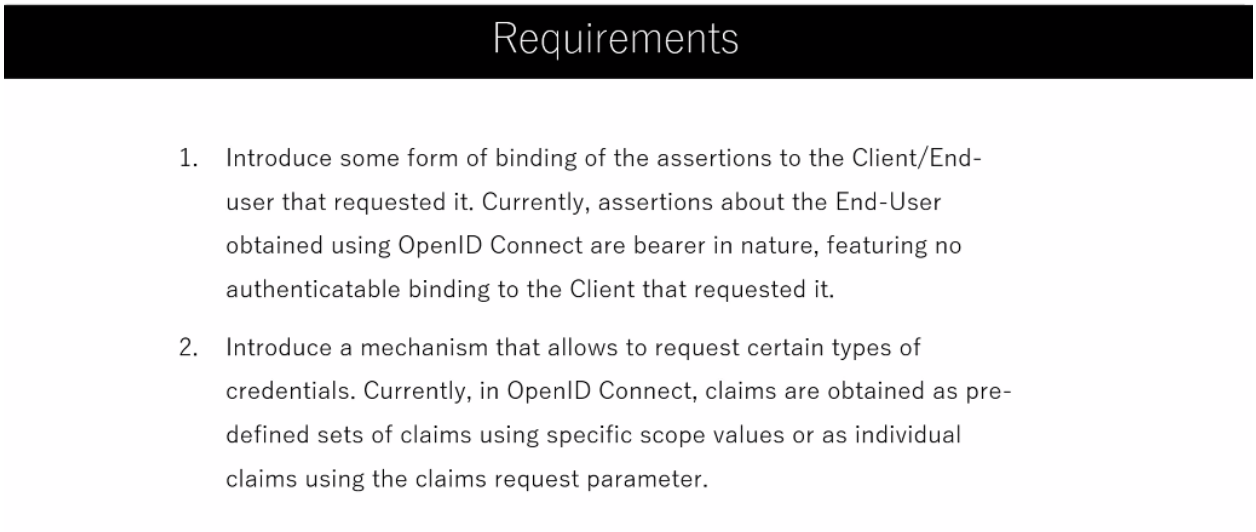
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The session was recorded

- Torsten gives overview
    - At OIDF work is going on for a protocol suite for SSI
    - Also Credential Issuance topic - that's why this session
    - To find out how implementers are using OIDC for Issuance
    - Seeking to get to a 1st draft of OIDC for Issuance, starting with inputs like this session
- Kristina gives more background



- Claims aggregation and credential provider are being merged in OIDF as a starting point



    - "Credential" in this session should be viewed in the Verifiable Credential sense, not the OIDC sense
- Requirements for the spec
    - Issuance needs binding of a credential to a Holder/person
    - Also new mechanism for requesting specific types of credential
    - (need a "Proof of Possession" aspect for the assertion - how to introduce a cryptographically bound credential to OIDC)
- Credential Provider uses Signed Request Object for POP today
    - (the Holder needs to prove control over key material)
    - SRO should work - but the way OIDC uses SRO today, SRO signs with the CLIENT key, not the person's key
    - NEW: add additional parts to the protocol flow to show control of holder key
        - What are others doing?
- FIDO - Issuser sends a challenge to the wallet. Wallet responds utilizing the private key.
    - JSON messages (WebAuthn)
    - Can also provide key metadata (attestation, location, etc)
- Who is the Client in an SSI configuration? Isn't the Client the User?
    - Don't assume that the User is the Client - in certain cases there are legal requirements for issuance - and the Issuer might have to have assurance of the person, not only the software assurance
- NOTE: In Issuance, the Client and device are the RP - and the Issuer is a normal OP. (Not the same capabilities as in the SIOP presentation flows)
- In the issuance flow, the client_id could be the sub of ID token
- Discussion about 'call home' and linkability concerns
- The identity of the wallet/client should be distinct from the identity of the person
    - Lifecycle of each is different
    - POP of the keys of the VC should occur after the OIDC request (which authenticates the user and gets consent)- wallet should use a back channel to request a VC issuance
    - Prefer that the demonstrated POP is an aud constrained nonce that is client bound (versus a server-generated nonce)

Decoupling between authentication and authorization.

There is a need for metadata. Something that is registered with IANA. It's specific to the issuer.

The latest OpenID Connect draft uses scopes for the OpenID credential. It shifts to the backchannel model.

- OpenID request - user request is based on the protocol so user consent is the best way to do this.
- Different from the normal kind of release

This exists because people see value in different kinds of claims. Before they erred on the side of less complexity. But now they believe that the solution is possible.

Q: FIDO authenticators or sign in with Apple, etc... , any of these authenticators generally don't have a plugin to ask for consent. The consent piece is usually missing from a FIDO 2 authenticator. Is it combined in this flow being described.
A: User agent doing authentication and client doing consent.
Q: At a protocol level, how do the two agents (authentication/consent) interact with each other?
A: ? Related: Microsoft Authenticator in VC issuance does request user consent JFYI

Q: One vs. many VC types? What is presented to the user for consent. A VC can do whatever it wants. Example: "You got 10% off a ~~bakery~~ manufacturer's product. The Terms of Use says that you can only use this at XYZ Market. But going to ABC Market, they decide the VC as well."
A: It should be part of the flow. But the example doesn't. There is a price match policy, but if the VC is presented to the coupon redemption center, it will not work. So the store is out of that 10%. The redemption is never made.

In the implicit flow there is no token endpoint.

User Stories for the VRM Intention Byway. A way to develop that starts with happy users. We'll be creating them.

Tuesday 3F
Convener: Doc Searls, Joyce Searls, Johannes Ernst
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

User stories, VRM, intentron, byway

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

Doc is giving overview over the ideas behind the Byway.

A very incomplete FAQ for the Byway is here: https://customercommons.org/solutions/tools/intention-byway/intention-byway-faq/

A shorter description of the Byway: https://customercommons.org/a-new-way/

pAlgorithms -- personally-selected or -created algorithms running on your own data on your own server aka Intentron.

Buyers send messages of intent to sellers in a market. Within a community. Topic-based.

Example: wanting to buy an engine for a particular 1960's car engine

There are apps, and the byway (which is only the messaging system).
Format:
As a <ROLE>, I would like to <DO SOMETHING>, in order to accomplish <SOMETHING>.

Roles:

- Buyer / shopper
  - Chef in a restaurant
  - Car repair enthusiast
- Seller
- Delivery Driver

User stories:

(Vintage car repair)

1. As a shopper, I want to find a specific used engine for my vintage car that needs an engine replacement, so that I can get the car to work again.

(Restaurant)
MVP

2. As a chef in a restaurant, on Monday, I want to buy and have delivered all ingredients I need for 8 servings of Chicken Cacciatore, produced locally and organically, in order to serve my guests on Saturday night.
3. As a chef in a restaurant, I want to be certain that delivered produce is organic, fresh and produced locally, in order to keep quality high of my dinners.
4. As a chef in a restaurant, I want to be told when certain supplies become available that I had been looking for and failed to find, in order to make the dish with the original ingredients
5. As a chef in a restaurant, I want to be told when certain supplies become available that I didn't know of, but that will make my dishes better, in order to further improve the quality of my dishes.
6. As a chef in a restaurant, I want to know the reputation of the produce supplier before I select them to buy from
7. As a chef in a restaurant, I want to discover new suppliers by entering tags (Criteria?) so that I can learn about new supplier options?
8. As a chef in a restaurant, I want to see several purchasing alternatives that meet my criteria, and select the one I want, in order to further optimize my purchase.
9. As a farmer, I want the restaurant to advertise on their menu that their recipe contains ingredients from my farm, in order to increase visibility of my brand.
10. As a farmer, I want to advertise this week's surplus of produce, in order to sell my produce before it goes bad.
11. As a farmer, I want to advertise my goods such that it will be seen/categorized so that I can reach the widest possible range of buyers (e.g. restaurant chefs).
12. As a farmer, I want to see the open requests that I can meet, in order to make special offers for specific opportunities.
13. As a delivery driver, I want to be hired for delivering supplies within a local region, in order to earn some money.
14. As a delivery driver, I want to specify the parameters for trips I'm willing to accept (distance, tip, margin, ability to carry certain loads: hot/cold/weight/...) in order to earn enough money.

Extensions:

15. As a chef in a restaurant, I want to define the ingredients and respective amounts for my famous recipes, and a maximum cost of ingredients + delivery, in order to save time when ordering supplies for the next week.
16. As a chef in a restaurant, I want to keep the ingredient list of my famous recipes private, so people keep coming to my restaurant.

Question:

- Would this be in-scope:? As a chef I want to know that the person I selected as a supplier is the same business that I just sent the payment to.

An aside: I'm hearing three layers to the tech:

- Bottom layer: the byway - a message passing layer (including identity)
- Middle layer: common "commerce-related" layer: deals with payments, tags/matching, reputation. This middle layer will take a huge load off of the difficulty of building apps
- Top layer: ByWay-compatible apps

GS1 License Credentials for Global Trade Identification

Tuesday 3G

Convener: Paul Dietch, Phil Archer, and Todd Snyder
Notes-taker(s): Phil Archer and Todd Snyder

Tags for the session - technology discussed/ideas considered:

GS1 Identifiers, DID, Verifiable Credentials

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

Discuss prototype built by GS1, GS1 US and GS1 Germany to issue and verify credentials across multiple ecosystems: SVIP and Indy Hyperledger.

Paul talked through the slide deck. Slides are available.

Toddy Snyder (for GS1 US) and Sebastian Schmittner (for GS1 Germany) talked through some of the details of the toolchains they used. In the US, they made a lot of use of CHAPI for JSON-LD based VCs. In Germany the tool chain was based on Hyperledger Indy. GS1 Global had to implement *both* to be part of the PoC.

After the presentations, the group discussed where we can and should go next and how to achieve it. It's no one's job to solve all the problems but it is everyone's. So how is it funded? Governments are supporting, but we need industry and more. GS1 is committed to the journey and will provide time and developer time.

What's the easy way forward? Choose one method and go with that. But we, the tech community can't decide which route to take. It has to be industry. GS1 worked in the US and Germany. Both Those territories major on a different tech. So we can't "just choose one." Had there been a third participant, you can bet they'd have wanted the JSON-only version.

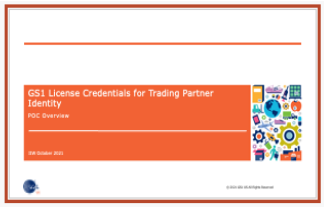
Running code, collaboration, openness and sharing. That's all we can do for now.

Session Chat Log
From Me to Everyone: 08:11 PM Sorry folks, we use the term 'keys' to mean identifiers, not crypto keys.
From Timothy Holborn to Everyone: 08:11 PM
From Artur.Philipp to Everyone: 08:11 PM ok thanks
From Timothy Holborn to Everyone: 08:12 PM so, multi-tenanted (perhaps multi-vendor related) identifier chains? ie:
https://docs.google.com/drawings/d/1oUsSlPEh8erOdkQJCLzFHBaqp7AYOJCqDw82YrCg9f4/edit?usp=sharing
(let me know if doc doesn't work)
From Drummond Reed to Everyone: 08:14 PM I like the assumption that the VC presentation is mutual/bidirectional
From Sebastian Schmittner to Everyone: 08:21 PM We tried the Hyper Ledger Stuff also on other ledgers, in particular the ID Union Test ledger
in essence, we re-invented credential chaining ;)
Actually twice, since we did something similar in the HL world

From Timothy Holborn to Everyone: 08:44 PM
q: any attempt to try interop with: https://docs.microsoft.com/en-us/azure/active-directory/verifiable-credentials/decentralized-identifier-overview ?
From SamSmith to Everyone: 08:45 PM
Suggest participating in the ACDC working group which is focused on layer 1 chaining vs layer 4 chaining
From Sebastian Schmittner to Everyone: 08:49 PM
thanks for the suggestion! Currently we are setting some hope into BBS+ VCs and aries interop profile/didcomm V2
Had some good discussion in this direction in session 1c already, looking forward to more
currently there is quite some funding in Germany going into SSI, raising some hope here ;)
From Heather Vescent to Everyone: 08:50 PM
(Yes I noticed your sponsorships)
From Sebastian Schmittner to Everyone: 08:51 PM
not meant to be advertising. ;)
From Heather Vescent to Everyone: 08:53 PM
I didn't take that as such, just as great participation in the community! :-)
So true Phil! And you are getting at the heart of my question!
From Timothy Holborn to Everyone: 08:56 PM
re: LD Serialisations nb: https://any23.apache.org/
From Sebastian Schmittner to Everyone: 08:59 PM
IP/SPX... good old days
From SamSmith to Everyone: 08:59 PM
I would be interested in your thought about interoperable security not merely interoperable semantics
From Timothy Holborn to Everyone: 09:00 PM
NB: i'd call the documentation level 'poor' https://www.w3.org/wiki/WebID yet imo, should be part of the future ecosystem overall. also, https://www.w3.org/WoT/
From Heather Vescent to Everyone: 09:00 PM
Timothy, +1, I completely agree. I find it very difficult to get funding for good documentation over there though.
Since W3C is all volunteer participation anyway
From Sebastian Schmittner to Everyone: 09:02 PM
so true! We invested time in learning and dev ops but it was all running on open source
From Judith Fleenor1 to Everyone: 09:02 PM
https://wiki.trustoverip.org/display/HOME/ACDC+%28Authentic+Chained+Data+Container%29+Task+Force

From Timothy Holborn to Everyone: 09:02 PM
nb also: old work (not so much me, but others in the W3C community linked to the WebPayments works: https://twitter.com/ProjectBitmark/status/513656134516088832

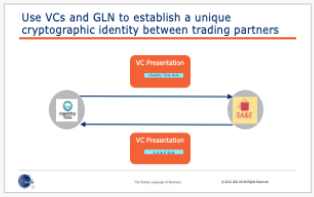
Slide Digest



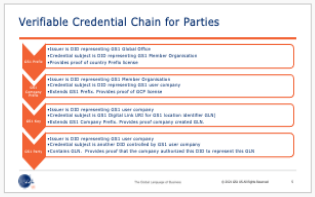
1

2

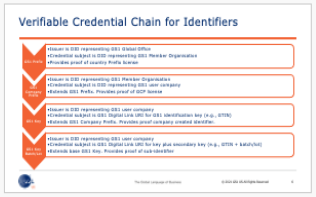
3



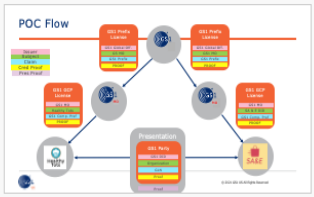
4



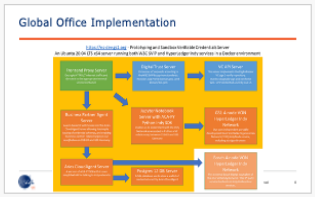
5



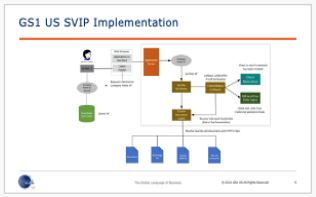
6



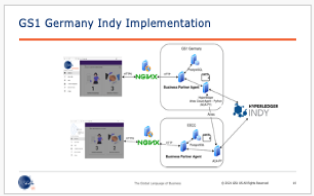
7



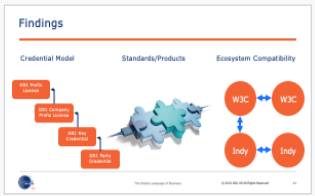
8



9

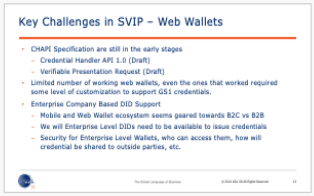


10



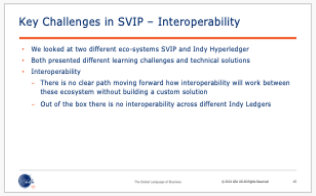
11

12



13

14



15

Microledger: Data Provenance Log for Authentic Data Economy

Tuesday 3H
Convener: Robert Mitwicki
Notes-taker(s): Robert Mitwicki

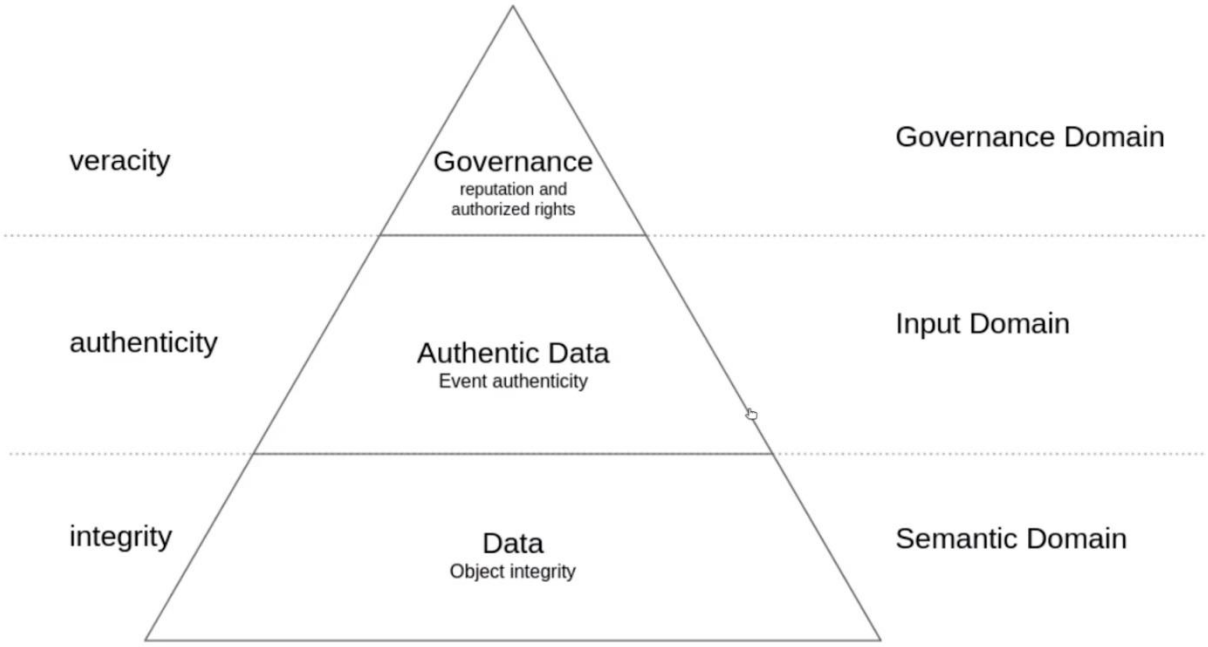
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Microledger is the concept extracted from great work which was done by KERI, ACDC, VC, Blockchain and more. The idea is to design a common framework for data provenance logs of authentic data. Focusing on integrity going through authenticity to enable veracity.

The specification is developed currently by Human Colossus Foundation, we are planning to join forces with DIF Applied Crypto group where similar work is already starting on data provenance log.

The specification can be accessed under:
https://github.com/the-human-colossus-foundation/microledger-spec/blob/main/README.md

All considered, relationships and mutual dependencies can be presented visually by authentic data pyramid:



Decentralized Identity and Self Sovereign Identity 101

Tuesday 4B
Convener: Chris Kelly (DIF) and Karyl Fowler (DIF, Transmute)
Notes-taker(s): Chris Kelly

Tags for the session - technology discussed/ideas considered:

Identity, IoT, Decentralized Identity, Self Sovereign Identity (SSI), Decentralize Identity Documents (DIDs), DID methods, Data Sovereignty, Governance, GDPR, Legally-ENabled Self-Sovereign Identity (LESS Identity), Trustless Identity, Toxic Data, DIF, Working Groups, Standards Track

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

Link to full PDF of presentation - Here Includes 3 Appendices w links to further resources and orgs

An Identity is information on an entity used by computer systems to represent an external agent. That agent may be a person, organization, application, or device, or even a digital artwork (eg NFTs)

1. SSI
    1. 2 components - tech and social/mental/infrastructure - 'movement'
    2. Movement - communities, orgs like DIF, but also end users, companies, legal frameworks, states and the general public
    3. Tech - the apps, services and platforms that are the mechanical parts of the system Infrastructure decisions, and commercial decisions can shape user expectations and behaviours, but legal requirements, customer demand and economic considerations also dictate the path of implementation
2. Current State
    1. 'Less identity'
    2. 'Trustless identity'
    3. Toxic data
    4. The concept of toxic data is any data on your systems, whether live or legacy systems, that you don't really need to conduct your business and that is potentially increasing your risk surface.
3. How it Works: The Tech
    1. Centralized ID - existing way
    2. Federated ID -existing way 2.0
        1. Still ends up consolidating data and power

Presents various problems

Potential solution: decentralized models, including blockchain

c. Tech basis for SSI

d. DIDs

e. Plurality of DID methods

f. VCs

g. Triangle of trust

h. Benefits of DIDs and VCs

i. Example applications

Overview of the communities, how and where to get involved

Explanation of ideation > incubation > refinement > standardization timeline

Q&A Session

Introduction to DIF Universal Resolver / Registrar

Tuesday 4D
Convener: Markus Sabadello, Bernhard Fuchs
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

DIDs, Universal Resolver, Universal Registrar

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

Universal Resolver application https://dev.uniresolver.io/
Github repo https://github.com/decentralized-identity/universal-resolver
Driver development https://github.com/decentralized-identity/universal-resolver/blob/main/docs/driver-development.md

Universal Registrar application https://uniregistrar.io/
Github repo https://github.com/decentralized-identity/universal-registrar
Driver development https://github.com/decentralized-identity/universal-registrar/blob/main/docs/driver-development.md

DID resolution is a fundamental part of every DID operation.
Around 100 DID methods are in the specification W3C did-methods list
Universal Resolver is an open source project to support many different did-methods
The Uni-Resolver runs as an external service

Semantic Interoperability with Layered Schemas and Semantic Pipelines

Tuesday 4E
Convener: Burak Serdar
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

Semantic interoperability, semantic harmonization, JSON-LD

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

Topics discussed:

- Layered schemas as a tool for semantic harmonization of data
- How to deal with variations of data coming from different sources
    - Example: One source represents date as unix timestamp, another uses yyyy/mm/dd, how to harmonize such data using layered schemas
    - Terms with functionality: examples on optionally validating data
- The key idea is to capture raw data with metadata and to interpret it layer based on context
- Semantic pipelines: ingest data, reshape data
- Semantic pipelines as a web service
- Problems with JSON-LD
    - JSON-LD is not namespace for JSON
    - JSON-LD cannot capture mappings of terms that mean one thing in one terminology but that means multiple things in another
    - JSON-LD is difficult to maintain because the meaning can be unrelated what can be inferred from the text

Links to layered schema resources:
http://layeredschemas.org/

Layered schema playground:
https://playground.layeredschemas.org/

Slide deck:
https://layeredschemas.org/docs/SemanticPipelinesWithLayeredSchemas.pdf

Session Chat:
From Timothy Holborn : https://www.w3.org/TR/shacl/
From Timothy Holborn : https://www.w3.org/community/cogai/ might be useful too
From Timothy Holborn : also: https://en.wikipedia.org/wiki/Semantic_Web_Rule_Language
From Timothy Holborn : FYI - some old work, that i'd say was instrumental to the development of this sort of stuff. http://dig.csail.mit.edu/2010/Papers/IAB-privacy/httpa.pdf
From Timothy Holborn : thesis is: https://dspace.mit.edu/bitstream/handle/1721.1/93833/900730390-MIT.pdf?sequence=2&isAllowed=y
From Timothy Holborn : https://any23.apache.org/
From Timothy Holborn : https://confluence.ihtsdotools.org/display/DOCOWL
From Dan Yamamoto : reminds me of Karma: https://github.com/usc-isi-i2/Web-Karma

From Timothy Holborn : https://www.w3.org/DesignIssues/N3Logic
From Timothy Holborn : https://prefix.cc/
From Timothy Holborn : https://lod-cloud.net/
From Timothy Holborn : an old email: https://lists.w3.org/Archives/Public/public-schema-gen/2017Feb/0006.html
From Timothy Holborn : FYI Also https://www.npmjs.com/package/did-io/v/0.4.1
From Timothy Holborn : https://github.com/mit-dig/httpa
From Timothy Holborn : a book library i made earlier. https://www.webizen.net.au/resource-library/book-library/
From Kyle Den Hartog : Thanks for sharing your project Burak. It's quite interesting. Can you make sure to add the links for that playground to the notes so I can comeback and take a look at it later
From Natan Sanson : Thank you Burak, interesting project

Identity and the Metaverse

Tuesday 4F
Convener: Johannes Ernst
Notes-taker(s): Charles Lehner

Tags for the session - technology discussed/ideas considered:

Metaverse, decentralization, social media

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

Johannes: Marc Zuckerberg gave interview in the Verge about how he will turn Facebook into a Metaverse company...
… five-year timeframe that Zuckerberg provided as an assumption. That in 5 years we would have some kind of pervasive Metaverse thing… some question about how/why it looks… If Facebook, expect it to be a walled garden…
Mike: can you define metaverse?
Amanda: who is speaking?
Brigitte: put recording on also.
Johannes: who is in favor of recording?
… Anyone against?
David.: That's the right question: is anyone opposed to it…. Silence is consent…
Johannes: okay, going to record… last chance to object.
…. Need host permission… how to claim host?
Kaliya: [...]
Johannes: okay, you are bring recorded… here is recording number 1.
… What is the metaverse? Definitions all over the place… no [standard]... first science fiction thing - Snowcrash by Stephenson.
… Another thing: the science fiction book and movie Ready Player One.
… Supposedly at Oculus you get a copy of Ready Player One on your first day…

… My definition: the collection of all information… a uniform user interface that exists on a variety of devices… from your mobile phone to smart goggles… including overlays (Augmented Reality - overlaid on the real world)
… To look at it from a perspective…. 3D Universe in which you can act and do stuff… We can talk about the edges…. That would be my definition.
… Facebook…. In order to catch up with friends and family… can see how it would [fit]... hang out in virtual space… something we don't really have in our 2D social universe.
… Is that good enough for a definition?
…
Vittorio: I just wanted to add… I've been doing that stuff since 1999… way before identity. I think that a good way of thinking about the metaverse is… it's an interaction model in which the computing is done by presence… the same vector as data… somewhat expressed via presence. Presence is best experienced…. But it's … necessary… If … you can reach it by a software agent… to me that's part of the metaverse. One other thing… projections in this kind of space are things that exist in reality. Things like artifacts you have in your life that have a digital aspect… the photocopier that says the paper is stuck here… if you have AR to show you that, that's also metaverse.
Dmitri: Hi everybody. One thing I highly recommend is the Open Metaverse Interoperability group at W3C, as well as the Twitter group… GitHub…
… One thing I was shocked to find is that there are a lot of Virtual Reality APIs built into our browsers… Chrome and Firefox have WebXR… I didn't realize that it runs pretty well in the browser. Then you can do things like plug into VR headsets… or do the Google cardboard, create a primitive headset with your mobile phone…
… A lot of interesting open metaverse servers… a lot of interesting implementations… The community has, fairly recently this year, discovered the decentralized identity community… Kaliya I understand you have engaged with their discord channel… There are a lot of needs / pain points in open metaverse projects, with portable identity and portable inventory… You have all these [implementations]... They are hoping to achieve that if you log into one server, create your 3D avatar… then log out and log into a completely different company, different implementation's virtual reality server, and be able to reuse your credentials… have my (IAMs?) come with me…
Johannes: … I tried to hack something in the browser… what would be a Indieweb homepage look like in the metaverse? Demo… this is about 2-3 hours of work… don't expect anything amazing… but interesting for me to see…

Dmitri Zagidulin1 To Everyone
4:22:39 PM
highly recommend https://twitter.com/open_metaverse?lang=en /
https://github.com/omigroup/omigroup
Chris Butler To Everyone
4:24:58 PM
This is pretty good too as an intro: https://www.matthewball.vc/the-metaverse-primer
A lot of overlap with "Web 3" as well
Johannes Ernst (Indie Computing) To Everyone
4:28:25 PM
I just did a prototype "metaverse homepage" at IndieWeb Create Day this weekend:
https://reb00ted.org/tech/20211011-personal-homepage-in-the-metaverse/

Johannes… In the web identity world, we think of [...]... I would like to not just bring my email address, but my avatar… I would like to define my avatar somewhere, not create a separate one for each site.

… A game… identity uses cases but not quite… Maybe if I define my own home - living room - can I bring it to someone elses world?
… I don't want to do too much speechifying… but want others to chime in with what their thoughts are.
George: how much do you think stuff you bring with you vs. stuff you create in that environment… people working on protocols to transfer information between protocols… I guess there is sortof potentially a transfer of attributes between the real world and the "matrix"... (dating myself, totally…). And those attributes are bound to some identity… I may want a couple identities, depending on the metaverse I'm interacting with… I suspect my gamer identity may be quite different from my [...] identity… Is there value that's created in the context of these metaverses? How do you transfer that value either out or in? Financial value… not just attribute value… badges, information… The identity piece doesn't seem overly complicated… but I'm probably missing nuances… Let's take the current scenario, I show up at the metaverse for the first time, I give them some verifiable credentials or signed attributes, the site validates those, and says okay, we'll assert your identity into the metaverse… then you have some linkage… I would assume the underlying attributes are different from what I would assert on entrance or registration.
Johannes: I'd like to carry a shopping bag… a single shopping cart… but 3D is more compelling… I could put something in and take something out…
Johannes Ebert: … bridges to other chains, protocols, transfers happening on-chain… the identity chain… I've spoken to a number of metaverse projects that have questions about identity… mostly about how do I know who are my users… There are these metaverse companies that have raised a lot of VC (venture capital)... just have blockchain addresses. How do I get crypto-native people to add real-world attributes to their blockchain address? And how to I get real-world people to get more into the metaverse? … Sounds similar to DIDs and Verifiable Credentials… a lot of things happening at the moment… I think this is where metaverse/decentralized-identity [can be] … a bridge to the real world…. Overlap… DeFi protocols… with my real-world identity… I think it's at this intersection of the real world with identity - not so much just about the assets that stay on the blockchain…

Dmitri Zagidulin1 To Everyone
4:33:26 PM
a lot of the work being done by OMI is exactly the ditch-digging kind of standardization of -- so what exactly are those VCs? what's the data model of a user profile?
Chris Butler To Everyone
4:33:32 PM
It feels like reputation is the key aspect here rather than stuff like a personal home page. E.g. gamer tags with your ranking or a hobbyist group with my previous posts.
Dmitri Zagidulin1 To Everyone
4:33:35 PM
like, each VC needs to be hammered out/standardized

Vitorrio… Interop… do we even know there is going to be a need for interop… I've been doing so for a few years… I've never used blockchain once for doing any of these… I had the ability to dress up my avatar anyway I wanted, without having to claim an avatar(?). Today, the metaverse in the Snowcrash sense, is there, is pretty primitive, but it's a set of purpose-built environments, in which the builder(?) builds an experience… to engage… I don't know how many times I've had to rebuild my avatar… Some support textures, or not, etc… If you have an iPhone, or Facebook, … if you want to use Emoji(?) in iMessage… If you're using Snapshot… yet another avatar…. The point is, what is the business case. Until those apps in the phone/metaverse is somewhere you go when someone wants to do business with you, vs. just walking down the street, until those are purpose-built, they need the … interoperability… the avatar… It might be an academic question… Let's think about it, if there would be a need for it… but let's not be under any illusion that any of this stuff will be necessary.

Johannes Ernst: I like the dose of realism you provide…. In a travel app, business case for building out apps… Before the apps occurred, we had a case for the web… I'm interested in personally, the equivalent of the Web use case for a Metaverse. One of the beautiful things about the Web is that I can start somewhere and start clicking… The web is a collection of millions of interlinked independent pieces… I would like to have a metaverse… similar to the 2D web… It's very possible that the commercial circumstances make that impossible - that the web dies off and we just have apps… But I would like to have an open metaverse… I would argue that the total value created is actually higher than in a set of purpose-built metaverse… but I can't prove that.
Rouven: I think if you build a social network with some form… different skins on top of us… connections and social graphs of different types… and can disclose attributes… we don't see the same interface… I think there are a lot of opportunities…. There will be certain assets that you can't just copy… so there is a scarcity effect (that might be blockchain-based), and there is …. Which can be disclosed in certain contexts…. You can see the space way more creative…
Vittorio: I like the vision you painted of the web, of following links… I agree it is fantastic… Now I see… just like your user-agent string is shared when you visit a website… but I think the part about a web app is misleading… To me it's not a smart delivery vehicle (app vs website), it's more about the curation. You can enter the app, or you can enter a local part… The level you achieve at Universal Studios will be at a different level… In the end, the part that makes it possible is financed by the existence of these big other people.... They do not necessarily interop with the local zoo. I completely buy (thanks for bringing it up) the idea of the web having a common base that you carry with you - but the level of experience you might want to have - when you think of Ready Player One - I think it's unlikely to see in the browser today… Curated experience… they have an interest in keeping you there… and not others (which Interoperabiliy would do)...
Johannes Ernst: Ready Player One is an interesting case… has a single organization operating it, with a benevalent dictator, who dies, and what happens after that. This is a book because it's a real problem… the users have no say… like in the case of Facebook… Personally I take the [...]
… However, if you go down the long tail, the ice cream shop and the [...] do interoperate, because they take the same credit cards. The amusement park may have its own currency… Even if you have curated spaces, I"d like to see you can get in and out, unlike the case where they are making it impossible…
David: Ready Player One is not Facebook, it's Second Life…. [...] was a long-time user of Second Life… I knew him… it's very much completely inspired by Second Life… he would disagree with you if he were here.
Johannes Ernst: I meant to say about the governance…
David: I was part of the governance
Chris: Interest in VR… walking around main street. Dark versions of AI… There is a video of someone that had a filter that would automatically make someone smiling… such a creepy experience, a yuck factor of world repugnance… but when it comes to VR, very popular to have the app experience. Cf. Ticktock vs. Facebook.
… I used to work for their identity labs…
… People want to have … experience…
… The "burning man experience"... it's odd to walk around, I'd rather just move between them.
… I don't want to have to walk across the entire playa to get that experience…
… Overlapping reputation experience…
... Gamer tag… a real issue like with Oculus… may be different from what you have on Facebook… A lot of overlap of pseudo-identities…
Johannes Ernst: I've made the assumption that of course we will have multiple personas… it's make very little sense otherwise…

Dmitri Zagidulin1 To Everyone
4:41:23 PM

@Rouven - Open Metaverse Interoperability Group https://github.com/omigroup/omigroup
gravatar is an excellent example
Rouven Heck To Everyone
4:44:19 PM
Thx!

Vittorio Bertocci To Everyone
Chris: bingo!
Chris Butler To Everyone
Hyper-Reality AR video I was talking about:
https://www.youtube.com/watch?v=YJg02ivYzSs&ab_channel=KeiichiMatsuda

Johannes Ernst: picking on Facebook because it has oversized influence.... Clearly [...] in many ways… If that is true, it will be more so - a business with a similar incentive structure - will have the same or worse effect - if all-encompassing… I'd like to not go there. I'd like to have the web back... I'd like to express myself with this competition that is possible… where not everybody has to fit into someone else's economic model… because ultimately… [Facebook as a corporation] optimizes for a lot of things but not the common good.
… What are some plausible scenario that by the time Facebook converts to a Metaverse company that there is a credible alternative governed in a more [...] way? Possible it can't be done, but I think we should have this conversation…
Chris: if you go into your Oculus, you can browse immersive experiences in the Web…
Johannes Ernst: but if I put it on, not necessarily all websites will be Metaverse…
Christ: … We have lots of ways to deliver immersive content on the web. I don't think most websites care… I still rail against the idea of the "immersive Wikipedia"...
Vittorio: Exactly… The point is affordances… when you are in an immersive environment, there are things you can do…. Turn around, what's behind you… But you need to have [...], otherwise you end up like a B movie…
Chris: …
Vitorrio: Mozilla has Mozilla Spaces… really nice. If you do have an Oculus, you just go there, and there are games, etc. But it's all proof of concepts… Invariably you find curated experiences… How Spider Type X (?) can achieve... how it works in reality, how to change the way it is interpreted… it really uses … you would have a hard time doing this… but I agree with Chris, Wikipedia is kindof okay the way it is… but until someone does investments…. The long tail… it will be hard to do… without the big people that pay for the main browsers… and create SDKs for curated experience… If you just have SDKs, you end up with GIMP.

Johannes Ernst: Is there an analogy to the early days of the web? … I feel like we're at the stage like where Bezos is thinking of selling something online… Here on the Metaverse… we have games, that sortof work as a business/value proposition… meeting spaces… might be sortof interesting… and things like exhibits that Vittorio pointed out…
… We managed to keep the web so that the little guys can do things…
… Do we have enough?
… You mentioned Mozilla… I'm blown away by how much investment Mozilla did in this stuff… I'm totally fascinated… nobody knows about it… so often… then they killed the product? Financial difficulties… I think we can do more, and need investment…
… I think I would build more stuff on my personal website if I could interact with user's avatar… but I don't know how to do that…

Dmitri Zagidulin1 To Everyone
4:55:56 PM

(several of the OMI contributors are ex-Mozilla-Spaces team)
Andy Morales To Everyone 4:58:19 PM
Just fyi, for everyone here, I am a principal product designer at Roblox, but I am here on an individual capacity, and have been talking often to OMI people.
Dmitri Zagidulin1 To Everyone
@Andy - oh, awesome!
what is missing? better person-level key management and recovery :)
Andy Morales To Everyone 4:59:59 PM
Centralized government funding? :) I recommend reading "How Not To Network a Nation" for information on how centralized efforts actually help with new techs
Controversial I know :)

Alan: … I would feel silly bringing a dragon into a business metaverse… but it might make sense to have a unified view…

Chris Butler To Everyone
Probably evolution of hardware. We need to build more immersive experiences for there to be more experiences that need VR.

Johannes Ernst: One thing I could do is have alternate rules of physics… but that is getting too geeky…
Alan: there is a web page where you can play with quantum scaling gravity…
… To me, whatever metaverse I'm in… In this room I have a picture - I don't see it in the other room - but would like to… that would require some form of [...]
Johannes Ernst: is this a conversation about metaverse identity that occurs somewhere? Dmitri pointed us to the OMI group…. Is this something people see happening more often going forward? Is there a logical place for it… should we have it at IIW? Maybe premature to have this conversation….

Vittorio Bertocci To Everyone well, you don;t see your furniture when you go at the restaurant or the post office :)
Chris Butler To Everyone Which are the weird physics you are talking about
Dmitri Zagidulin1 To Everyone 5:02:21 PM
join the w3c community group! :) and, of course, IIW!
Alan Karp To Everyone 5:02:43 PM
@Vittorio: Not that I see it all the time, but I can see it when I want to whichever met averse I'm in.

Andy: Hi, I work at Roblocks(?)... If we are to keep this from becoming walled gardens - which is what tends to happen when you have different economies… Different ways of incentivizing interoperability…. Because of the economic factors, I've been trying to think around how we can do "Ju jitsu" on the places that need interoperability… Children's privacy… how do we actually implement that across the metaverse… Not only could we incentive companies… but have government pressure… that could be a [...] force … to get some leverage… Interested in what other people think…

George: I'm still struggling(?) with the identity problem… I've heard about the KYC problem… some metaverses want to know that I'm a "real person" or not… there could be real reasons for that, or not… I was playing with a Facebook clone… I could get in, but if I wanted to do anything, they wanted to scan my driver licenses… Wait a minute, I'm not sure I'm ready for that.
… Moving attributes in and out… verification of data, users… don't seem to me like that different a problem…. At a bank there is some level of KYC to set up an account… Why is entering into the Metaverse that much different? People are working on making that easier so I could just do it once…

… A set of personas… Against that identity I have some set of claims… Noe we need specs for interop and how to transfer that data back and forth… I feel like these problems are governance and economic problems… especially when moving between metaverses…
Johannes Ernst: good questions…. In the browser world today, the vast majority of sites are anonymous… I haven't really logged in… I think in the Metaverse it will be the other way around. I have my avatar… and generally will be authenticated by default…
… If every relying party that I interact with… that will be different… privacy and correlation, etc.
George: sure, all sorts of interesting problems… collusions, or my data in a central hub, knowing everything about me and what metaverses I'm interacting with… the same problems we're facing today… Like just moving pieces on a chess board…
… Interoperability a huge issue… I think the login side… my phone as a collection of metaverses… the vast majority, I'm already logged in.. So on the web I may not explicitly log in, but that's because the sites could offer services to me in an anonymous way and still make money. That could change substantially… would not surprised if most sites start to require login…
… The web may become less "anonymous".... As people we are not anonymous… we walk around as a globally correlatable identifier…. But we forget… In the online world it's hard to forget, and we choose to monetize that… It's hard to change this.

Vittorio Bertocci To Everyone 5:04:04 PM
i think "metaverse" might be the trick thing to define in this context- for how things are implemented today, I thought that the point was exactly that you can't
Simon Nazarenko To Everyone
5:04:30 PM child privacy online is a big one
Vittorio Bertocci To Everyone
5:10:18 PM Johannes Ernst: appreciate that… Story about moving Netflix into the cloud… I didn't want to do that, but that happened inadvertetly…
… At some level there is a discontinuous change… on the same level as Cloud or Not Cloud..
… If we were to make the assumption that in the metaverse, in a decentralized web-like metaverse, where we will be authenticated all the time, we could build an infrastructure to do that, since we know it will happen, in a way that is privacy-preserving… It will be hard to retrofit it… I have goals that are not just money… If we build a package that involves protocols and technology, we could bend the metaverse as it is being built, to a direction that is more beneficial…
Andy: do you foresee something like… For example, Costa Rica gives you an ID when you are born… everyone uses it for everything… no one can steal it… not like social security numbers (bizarre…)... Kind of the opposite, making it extremely public, to get rid of the problem of someone stealing it… Even if that existed, why do you think that these companies with all these users will adopt it? I think that's the big question right now… do we want to get these companies to adopt it, or do we want to build something from the ground up?
Johannes Ernst: A good question, reform or revolution… In our socio-political system, it's unlikely we'll get more interop/optimization(?) for the benefits of the businesses over the users… that's the direction we generally go… We could say that's how it is…
Andy: Not being a party pooper, just wondering…
Johannes Ernst: how does the world look like, that is not centralized? If you can't explain it, nothing can ever possibly happen.
… How it functions, and competes for itself… then we can find reasons why someone with corporate strategy might want to participate…
… e.g. someone at CompuServer convinced them they would be better off connecting to the web…
Vittorio: sorry for being negative… my professional bias… even if we come up with a basic set of primitives that allow people to have privacy preserving [...], it feels like without incentives, it won't help… Web is

mostly anonymous (browser fingerprinting notwithstanding)... We've been going in the direction of not being able to afford that anymore… Companies just build something as a ticket… I have …. non-technical… some did not come close to a computer before Facebook came around…. But still, we started with decent privacy preserving stuff, but moved away… I applaud your attempt and want to participate… to create experiences in the metaverse, starting on the right foot, but under no illusion that [...] will not feel bound… nor will the users… they go for convenience.... Whatever is the value for convenience they will take… So let's not have illusions.

Johannes Ernst: Use of advertising as a primary business model… If we didn't have that, would probably get less fake news… One thing the web does not have is a payment layer… lots of people in the Crypto world working on that… If the Metaverse had something for payments (Crypto or not).... Would things shake out differently? I think it would.

Heather: Hey, it's fun to be in this conversation. I feel I have been repeating things about capitalism and stuff… But I think it's audacious to think we can challenge the business model that the Internet has always run on… that Google become Google on… maybe I'm just tired but I don't think we will win this... Corporations' incentive is for profit… Phil from GS1 said about SSI "does it work, and do I make more money with it" - the only reason companies are going to do anything is not because it's moralistically right… (Users are not demanding it)... We're just continuing on a path of Capitalistic destruction… I raalize you are trying to do the right thing, but I don't see the incentives changing… I don't know… is there any hope?

Johannes Ernst: Yes… everything pointing in the wrong direction…. But I would argue two things. It's a necessary requirement for anything to change is that some people who are "insane" (maybe us here…) are going to try to do something impossible…. We might fail, but the fact that we try is useful… Just like the IndieWeb built its own community… In this environment, this is how we function… The other thing is that for the first time in the last couple weeks, I've heard political voices say maybe we should ban surveillance capitalism, just like we banned child labored… Hearing this in the public discourse is new…. More [...] investments… Just like divesting from Apartheid, and Fossil Fuels, some will divest… Just like a 401K, one says "surveillance-capitalism-free", you might not put everything there, but may put some of your money there…
Brigitte: … Bitcoin just showed up, there was no real intention to derail the large financial players, just provide an alternative and this was picked up by early users and still grows today 10 years later … a parallel entity that over time has inspired new ways of getting things done…. I'm wondering if that is the same sort of thing here… Can we build a parallel [mechanism].... that might be so useful and effective that it takes on a life and growth of its own…

David: The laws are written in the context of the large powerful companies who benefit from Surveillance Capitalism… the people writing those laws run those companies… I have very little faith in Government fixing this…. But I like what Brigitte said… Bitcoin came out of no where, people like us… Bitcoin was probably Len… First versions used the last versions of Mixmaster… Satoshi was probably Len and Hal… doing something that had nothing to do with global finance, they just wanted to run anonymous remailers… Tor developers were also a part of this; they wanted to monetize running Tor nodes…. I wonder how big really is the crowd that cares. Is it just us? I might really just be us. If it is us, we should build something, and start setting up parallel systems…. My philosophy from the beginning... I'm on the cusp of building a wedge between Surveillance Capitalism and their Surveillance systems…. Once you have authentic data flowing through your self… if you move the code to that authentic data…. We are not giving up any information that feeds those models that Surveillance Capitalism models build… It's possible to … [do operations on authentic data].... The business process gets a one-bit answer (yes or no), proof of authenticity of inputs, proof of nonrevocation of inputs… allows e-commerce to happen without giving

private information…. It's all cryptography… So the answer going back to the business is trustable… The coolest part of this design is that I don't ever have to talk about privacy… It automates compliance …, reduces correlation(?), reduces fraud… and we can also do a cryptographic paper trail for 4th-Amendment purposes (for Americans…)
… Sorry to hijack conversation… we can do this…
Johannes Ernst: Yes, I think there are enough people with enough motivation to prototype something for their own purposes, and see where it can be… That's the kind of thing I'd like to see in the metaverse.
… We may reconvene this conversation at the next IIW… The world is moving fast… Would like to move faster than that… An inflection point… The things thrown at Facebook in recent weeks.. We can do better.

Session Chat transcript:

13:22:39 From Dmitri Zagidulin1 to Everyone: highly recommend https://twitter.com/open_metaverse?lang=en / https://github.com/omigroup/omigroup
13:24:59 From Chris Butler to Everyone: This is pretty good too as an intro: https://www.matthewball.vc/the-metaverse-primer
13:25:04 From Chris Butler to Everyone: A lot of overlap with "Web 3" as well
13:28:25 From Johannes Ernst (Indie Computing) to Everyone: I just did a prototype "metaverse homepage" at IndieWeb Create Day this weekend: https://reb00ted.org/tech/20211011-personal-homepage-in-the-metaverse/
13:30:09 From Charles E. Lehner to Everyone: https://docs.google.com/document/d/1mDy5Pi0b4rKlwKbvA1zTPPYsarXekuJ6jfSfZZPDKag/edit - Notes - could use some help
13:33:26 From Dmitri Zagidulin1 to Everyone: a lot of the work being done by OMI is exactly the ditch-digging kind of standardization of -- so what exactly are those VCs? what's the data model of a user profile?
13:33:32 From Chris Butler to Everyone: It feels like reputation is the key aspect here rather than stuff like a personal home page. E.g. gamer tags with your ranking or a hobbyist group with my previous posts.
13:33:35 From Dmitri Zagidulin1 to Everyone: like, each VC needs to be hammered out/standardized
13:34:23 From Charles E. Lehner to Everyone: I have a question
13:35:42 From George Fletcher to Everyone: KYC in the Metaverse :)
13:37:45 From Charles E. Lehner to Everyone: You're welcome
13:39:15 From Rouven Heck to Everyone: @Dmitri - what is OMI?
13:41:23 From Dmitri Zagidulin1 to Everyone: @Rouven - Open Metaverse Interoperability Group https://github.com/omigroup/omigroup
13:44:10 From Dmitri Zagidulin1 to Everyone: gravatar is an excellent example
13:44:19 From Rouven Heck to Everyone: thx!
13:46:10 From Chris Butler to Everyone: We should remember that in Ready Player One there was only one company that owned all of it: OASIS.
13:46:23 From Vittorio Bertocci to Everyone: Chris: bingo!
13:51:53 From Chris Butler to Everyone: Hyper-Reality AR video I was talking about: https://www.youtube.com/watch?v=YJg02ivYzSs&ab_channel=KeiichiMatsuda
13:55:56 From Dmitri Zagidulin1 to Everyone: (several of the OMI contributors are ex-Mozilla-Spaces team)
13:58:19 From Andy Morales to Everyone: Just fyi, for everyone here, I am a principal product designer at Roblox, but I am here on an individual capacity, and have been talking often to OMI people.
13:59:08 From Dmitri Zagidulin1 to Everyone: @Andy - oh, awesome!
13:59:47 From Dmitri Zagidulin1 to Everyone:what is missing? better person-level key management and recovery :)
13:59:59 From Andy Morales to Everyone: Centralized government funding? :) I recommend reading "How Not To Network a Nation" for information on how centralized efforts actually help with new techs

14:00:03 From Andy Morales to Everyone: Controversial I know :)
14:00:26 From Chris Butler to Everyone: Probably evolution of hardware. We need to build more immersive experiences for there to be more experiences that need VR.
14:01:37 From Chris Butler to Everyone: Games like Portal and Superliminal are going to be popular in VR (https://store.steampowered.com/app/1049410/Superliminal/)
14:01:40 From Chris Butler to Everyone: W
14:01:49 From Vittorio Bertocci to Everyone: well, you don;t see your furniture qhen you go at the restaurant or the post office :)
14:01:51 From Chris Butler to Everyone: Which are the weird physics you are talking about
14:02:21 From Dmitri Zagidulin1 to Everyone: join the w3c community group! :) and, of course, IIW!
14:02:43 From Alan Karp to Everyone: @Vittorio: Not that I see it all the time, but I can see it when I want to whichever met averse I'm in.
14:04:04 From Vittorio Bertocci to Everyone: i think "metaverse" might be the trick thing to define in this context- for how things are implemented today, I thought that the point was exactly that you can't
14:04:30 From Simon Nazarenko to Everyone: child privacy online is a big one
14:10:18 From Vittorio Bertocci to Everyone: the Dumbar number is king
14:11:04 From Chris Butler to Everyone: Vittorio: which one? ;-)
14:11:31 From Vittorio Bertocci to Everyone: 150!! :P
14:11:34 From Chris Butler to Everyone: https://en.wikipedia.org/wiki/Dunbar%27s_number#/media/File:DunbarsNumber.png
14:11:59 From Vittorio Bertocci to Everyone: yep, that one:)
14:12:11 From Chris Butler to Everyone: 1500 people you can recognize… but they have different representations in each meta verse.
14:12:23 From Andy Morales to Everyone: But the companies that are guiding the "meta verses" right now won't do it without substantial motivation
14:12:26 From Rouven Heck to Everyone: Single reputation score sounds dystopian
14:12:27 From Vittorio Bertocci to Everyone one order of magniture down
14:12:31 From Andy Morales to Everyone: Won't adopt it, I mean
14:13:11 From Chris Butler to Everyone: Whuffle from Cory Doctorow's Down and Out in the Magic Kingdom
14:14:22 From Andy Morales to Everyone: Sorry for not raising my hand, Vittorio! Just saw we have to do that
14:14:42 From Vittorio Bertocci to Everyone: dpn't worry Andy, I am Italian, I do it all the time :)
14:15:09 From Nader Helmy to Everyone: Agreed @Rouven ☺
14:15:43 From Nader Helmy to Everyone: Thought that's why we built this decentralized infrastructure to begin with
14:16:00 From Alan Karp to Everyone: @Rouven: You can have multiple personas.
14:16:03 From Nader Helmy to Everyone: Consent-driven portable reputation sharing can be incentivized in thoughtful ways
14:16:32 From Nader Helmy to Everyone: I think the issue now is the concept of portability in that respect is completely non existent
14:16:41 From Nader Helmy to Everyone: So we almost have to cross that hurdle first
14:17:39 From Rouven Heck to Everyone: Even with different persona's - I think a general score is tricky, reputation is so contextual.
14:18:17 From Rouven Heck to Everyone: I assume that 'a Metaverse is too diverse to have one score'
14:18:32 From Heather Vescent to Everyone: Ding Ding DIng!!!!
14:18:40 From Alan Karp to Everyone: The idea is that I control what I do with my different personas, so in a sense I control their reputations.
14:18:41 From Heather Vescent to Everyone: +100

14:18:47 From Nader Helmy to Everyone: Agreed, you don't need a single general score but you need some kind of common framework that allows reputation to cross boundaries and still be understood. Not as a universal metric but contextually
14:18:49 From Chris Butler to Everyone: Agreed!
14:18:59 From Andy Morales to Everyone: I like how this is slowly becoming "how do we solve capitalism?"
14:19:09 From Dmitri Zagidulin1 to Everyone: lol
14:19:11 From George Fletcher to Everyone: lol
14:19:17 From Nader Helmy to Everyone: @Andy the best kind of IIW session haha
14:19:18 From Alan Karp to Everyone: If I have a good reputation in one MV, I would like to use that to bootstrap my reputation in another.
14:19:19 From Vittorio Bertocci to Everyone: Andy that's exactly where all this stuff usually goes
14:19:23 From Chris Butler to Everyone: The times you want to transfer reputation is usually to get some benefit in the cold start moment… like changing mileage programs.
14:19:38 From Kerri Lemoie to Everyone: @Andy - hah! Yep
14:20:20 From Vittorio Bertocci to Everyone: Preach, Heather!! +++
14:20:21 From Rouven Heck to Everyone: I fully disagree - we have a great opportunity with Web3/Protocols using as inventives
14:20:39 From Michael Shea to Everyone: I think this is where the absence of policy makers over the past 10+ years have to step up.
14:20:52 From Nader Helmy to Everyone: It's not a zero sum game lol
14:21:06 From Andy Morales to Everyone: I think we need to both have an optimistic final scenario, AND work on Trojan horses to introduce our vision to these companies
14:21:15 From Andy Morales to Everyone: That's why I'm like "policy, PR, compliance"
14:21:15 From Nader Helmy to Everyone: There is a massive decentralized web movement happening and the mega corps are barely aware of it or understand it
14:21:51 From Andy Morales to Everyone: To be fair, I worked in ConsenSys on Web3, and a big part of Web3 becoming big has been speculation due to HODL TO THE MOON
14:22:01 From Andy Morales to Everyone: They just got money and people jump on ships with money
14:22:17 From Heather Vescent to Everyone: Yes, yes I agree. But maybe I am le tired now. And I don't feel like I/we have been successful with my past endeavors, so why continue?!
14:22:48 From Heather Vescent to Everyone: RE: regulation is one way to address it. Intriguing.
14:22:53 From Rouven Heck to Everyone: I think DeFi & NFTs show the first signs on how the decentralized web could operate
14:22:54 From Andy Morales to Everyone: One of my Strengths Finder strengths is "motivation" so I say NEVER SURRENDER
14:23:00 From Andy Morales to Everyone: haha
14:23:25 From Simon Nazarenko to Everyone: we won't win the fight unless the worldwide identity crisis strikes, where people will open their eyes and realize that there is another approach... imo
14:23:30 From Nader Helmy to Everyone: @Andy I agree with the Trojan horse approach. They barely know what's going on, they wouldn't understand it even if we tried. By the time they realize what's happening it will be too late for them
14:23:56 From Andy Morales to Everyone: @Simon suggesting some Mr.Robot tactics here? haha
14:24:07 From Nader Helmy to Everyone: @Rouven exactly. I see this happening on a daily basis and see the way that people with power dismiss it and it does nothing to take the wind out of the momentum behind web3/defi/nfts
14:24:10 From Simon Nazarenko to Everyone: ^ this
14:24:11 From Nader Helmy to Everyone: Try as they may
14:24:33 From Kaliya Identity Woman to Everyone: I think we could if we worked hard and ran fast answer the "does it work" and "can it make me more money problem"

14:24:51 From Andy Morales to Everyone: Ya BUT “the children!” Is a good place to start imho
14:24:56 From Andy Morales to Everyone: “Think of the children!"
14:25:06 From treycarl to Everyone: “One must imagine Sisyphus happy.” :)
14:26:11 From Heather Vescent to Everyone: Back to monetization!
14:26:18 From Andy Morales to Everyone: Hold on, I don’t remember vividly, but didn’t the Bitcoin white paper mention finance?
14:26:24 From Andy Morales to Everyone: Gotta go get my copy
14:26:25 From George Fletcher to Everyone: @andy I agree that "protecting our children" is an interesting place to look at introducing new models
14:27:22 From Rouven Heck to Everyone: Big tech & finance is slowly realizing the risk / opportunities with web3, and it will fight the movement … - but I think the movement is pretty strong already…
14:27:36 From Vittorio Bertocci to Everyone: eeeexactly. Whomever flaunts "94% of people opted out of tracking in iOS15" is disingenuous. When the price to pay is clicking a button vs another people care, ask them to give up Amazon Prime and see how much they care about privacy
14:28:11 From Vittorio Bertocci to Everyone: (in resposne to "who cares besides us here")
14:28:32 From Kaliya Identity Woman to Everyone: that is a naive way to think about how businesses will do business.
14:28:38 From Heather Vescent to Everyone: Sounds like what is envisioned in this video (disclaimer, I made this based on work done at SWIFT in 2011 & 2012) https://vimeo.com/52354667
14:28:53 From Heather Vescent to Everyone: Just showing that you can buy a motorcycle, but not how much money is in your bank account.
14:29:08 From Andy Morales to Everyone: Yo just checked and the white paper mentions “peer to peer cash” and “e-gold” and I know economics =! Finance but in the modern day world they are
14:29:17 From Andy Morales to Everyone:
So I’d argue that Satoshi DID think of finance and economics from the beginning
14:29:36 From Nader Helmy to Everyone: @Vittorio which only proves that people don’t want to give up their services if they’re never given a realistic alternative. When it gets built there will be an alternative economy with a different set of tradeoffs and it will be a real choice.
14:30:13 From Nader Helmy to Everyone: Thats what’s happening with web3/defi and what can happen with identity-based services
14:30:24 From Heather Vescent to Everyone: Yes I am interested! Hold session #2
14:30:33 From Heather Vescent to Everyone: Please and thank you!
14:30:34 From Kerri Lemoie to Everyone: I’m interested
14:30:34 From Nader Helmy to Everyone: Yes please
14:30:35 From Brigitte Piniewski to Everyone: Yes I am interested
14:30:37 From Simon Nazarenko to Everyone: thank you!
14:30:40 From Vittorio Bertocci to Everyone: @nader agree in theory- I just suspect we have different views on the prospect of those techs to be a realistic alternative
14:30:41 From Sebastian Posth to Everyone: Interested
14:30:43 From Rouven Heck to Everyone: Interested!
14:30:45 From Kaliya Identity Woman to Everyone: yes lets do this
14:30:49 From Vittorio Bertocci to Everyone: interested!
14:31:04 From treycarl to Everyone: Interested!
14:31:08 From Charles E. Lehner to Everyone: Charles Lehner <[...]@spruceid.com>
14:31:28 From Charles E. Lehner to Everyone: Thank you... Audio not working currentyl...
14:31:31 From Kerri Lemoie to Everyone: Thank you!

Picos, DIDComm, and Decentralized SSI Agencies

Tuesday 4G
Convener: Phil Windley
Notes-taker(s): Phil Windley

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

Picos (persistent compute objects) are an actor-model programming system with long-term persistent state. Each pico also has persistent identity and availability for a cloud-native developer experience. Picos are DIDComm-enabled agents supporting SSI. Consequently, picos are capable of running specialized application protocols for any given workflow in a secure, cryptographic environment. The architecture of picos makes them independent of the runtime they executed on, holding out hope of a decentralized SSI agency. This talk introduces picos, demonstrates their DIDComm capabilities, and presents a roadmap for building a decentralized SSI agency, independent of any particular organization.

Session Slides here:
https://www.dropbox.com/s/d70smrnh8ii79vx/Picos%20and%20Decentralized%20Agency.pdf?dl=0

What is ToIP ACDC (Authentic Chained Data Containers)

Tuesday 4K
Convener: Sam Smith
Notes-taker(s): Sam Smith

Tags for the session - technology discussed/ideas considered: Authentic Chained Data Containers. Verifiable Credentials. SAIDs. Self-addressing IDentifiers. Secure Attribution.

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

Session Slides
Here: https://github.com/SmithSamuelM/Papers/blob/master/presentations/ACDC_IIW2021B.web.pdf

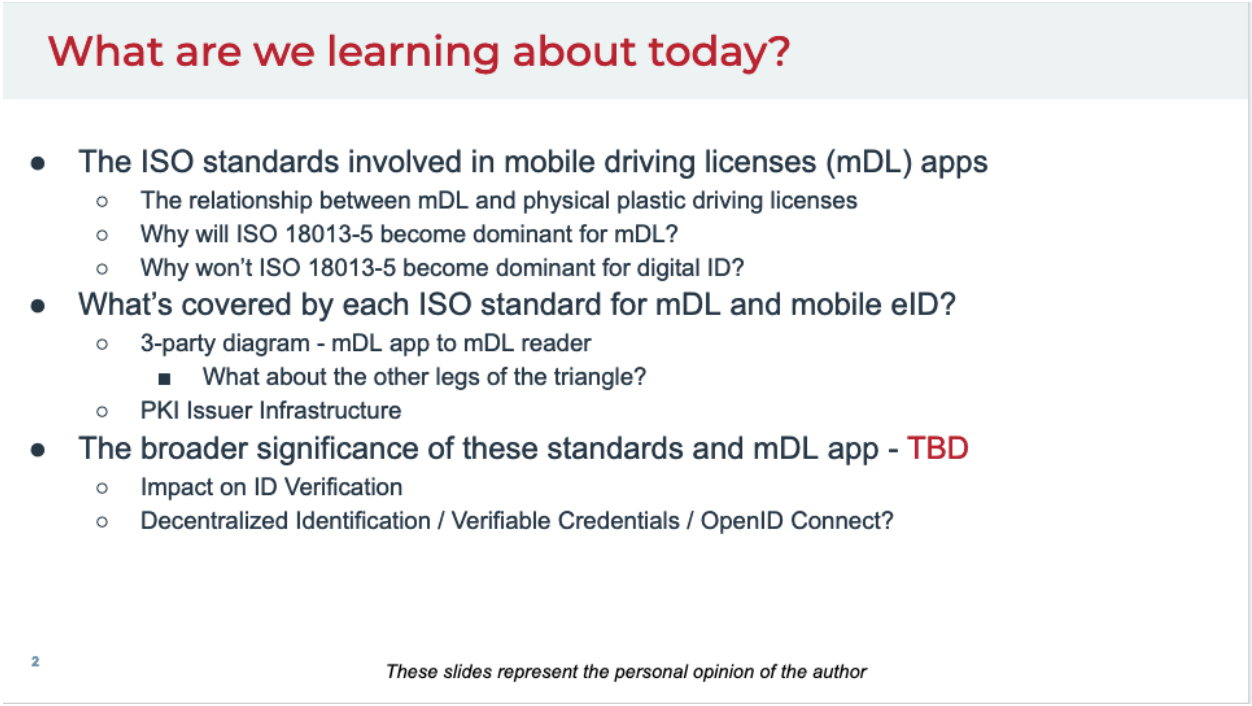
Notes Day 2 Thursday October 13, 2021 (Sessions 6 - 15)

ISO 18013-5 Mobile Driving License AND Verifiable Credentials - Better Together

Wednesday 9A
Convener: Andrew Hughes
Notes-taker(s): Andrew Hughes

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

- The session became about the ISO 18013-5 standard - what's in scope, what is out
- ISO 18013-5 is designed to primarily specify a driving license
- Additional/secondary uses can exist, but those are not covered in ISO 18013-5
- We discussed the idea of credentials derived from 18013-5 mDL for use as more general-purpose eID credentials
- << I have to review the session recording for more detailed notes >>



Click to add text

OVERVIEW OF MOBILE DL

3

Which ISO standards support Mobile Driving License?

- Published September 2021 https://www.iso.org/standard/69084.html
  - ISO 18013-5 (part 5) — ISO-compliant driving license — Mobile Driving License application
    - Defines how mDL App and mDL Reader connect, exchange, verify data over radio or optical transport protocols (QR, NFC, BLE, WiFi aware)
- Drafts at ISO committee stage
  - ISO 23220 parts 1 through 5 – "Building blocks" for Mobile eID applications
    - Defines broader eID functions, of which mDL is a specialization of one part
    - E.g. General architecture options, data elements, issuance, engagement/transmission/presentation, security/trust model & elements
  - ISO 18013-6 mDL test methods
  - ISO 18013-7 "Day 2" mDL topics - 2nd priority mDL topics
    - "Day 2" includes holder/prover authentication/verification not involving the Verifier; "over the internet" engagement and transfer

4

These slides represent the personal opinion of the author

ISO 18013-5 mDL app scope

Scope

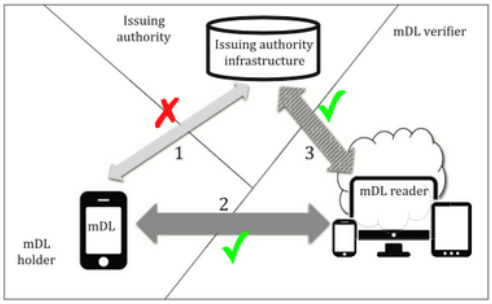
This document establishes interface specifications for the implementation of a driving licence in association with a mobile device. This document specifies the interface between the mDL and mDL reader and the interface between the mDL reader and the issuing authority infrastructure. This document also enables parties other than the issuing authority to:

— use a machine to obtain the mDL data;

— tie the mDL to the mDL holder;

— authenticate the origin of the mDL data;

— verify the integrity of the mDL data.



https://www.iso.org/obp/ui/#iso:std:iso-iec:18013:-5:ed-1:v1:en

5

These slides represent the personal opinion of the author

Who created ISO 18013-5?

- ISO SubCommittee 17/Working Group 10 (SC 17/WG 10)
  - Vendors: driving license systems, backend DMV systems, 'State Printing Houses'
  - Government issuers (DE, NL, AT, others)
  - US (AAMVA), EU (E-Reg), Australia (AUSROADS), Japan motor vehicle administrators (issuers)
  - National Standards Body experts
  - Large platform providers
  - UL & others (there will be a market for their testing and certification services)

Note: ISO Members are National Standards Bodies (NB).
Subcommittees and Working Groups are comprised of NB-accredited Experts in each topic. Accreditation rules vary by NB.
ISO publications are widely used, but not free or freely available.

6

These slides represent the personal opinion of the author

ISO WG Motivations for mDL (my opinion!)

1) To define a mobile DL version of ISO-Compliant DL / International Driving License
   a) The primary motivation at the beginning of the project
   b) 18013-5 is written for Issuers to ensure that mDL and mDL Readers 'do the right thing' to secure and use mDL
   c) Security (integrity, availability) and privacy (selective release) concerns are top of mind
   d) General intention is to augment plastic DL with mDL
   NOTE: mDL App & mDL Reader must work when no network available! "Offline Mode"
2) Following that, to define a general purpose identification document for presentation on mobile devices
   a) Secondary motivations - acknowledgement of the dual nature of driving licenses as entitlement and as Government-issued Photo ID
   b) As time progressed, the general-purpose aspects were split off into ISO 23220 series (Mobile eID Building Blocks)

7

These slides represent the personal opinion of the author

mDL as a dominant digital credential solution?

Yes.

- Embraced by MVA issuers internationally, big vendors, Android/iOS/Microsoft support, UL testing/certification
- WTO Agreement on Technical Barriers to Trade
  - In essence vendors conforming to standards from Standardizing Bodies like ISO can expect a more predictable trading environment. Meaning that conformant products and services cannot be rejected by a country's government for technical reasons. Removes significant obstacles to trade.
  - https://tbtcode.iso.org/sites/wto-tbt/home.html

No.

- mDL is Issuer controlled - and the Issuers are Governments
- mDL is not really 'web native' in current specification - 18013-5 is oriented towards closed/authorized domains where the Issuer and Verifier are known to each other

Maybe.

- This is the most significant bridge into the "Government-issued credentials" domain so far
- If Issuers/Governments can treat mDL like they do DL, then secondary and derived use cases will be possible

8

These slides represent the personal opinion of the author

Click to add text

INSIDE ISO 18013-5

9

ISO 18013-5 mDL app scope

Scope

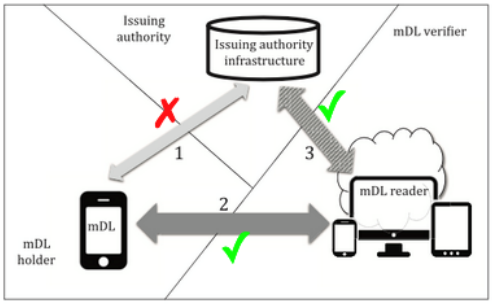
This document establishes interface specifications for the implementation of a driving licence in association with a mobile device. This document specifies the interface between the mDL and mDL reader and the interface between the mDL reader and the issuing authority infrastructure. This document also enables parties other than the issuing authority to:

— use a machine to obtain the mDL data;

— tie the mDL to the mDL holder;

— authenticate the origin of the mDL data;

— verify the integrity of the mDL data.



https://www.iso.org/obp/ui/#iso:std:iso-iec:18013:-5:ed-1:v1:en

10

These slides represent the personal opinion of the author

Terms and Definitions of note from ISO 18013-5

- **mdoc**: document or application that resides on a mobile device (3.1) or requires a mobile device as part of the process to gain access to the document or application
- **mdoc reader**: device that can retrieve mdoc (3.2) data for verification purposes
- **mdoc holder**: individual to whom an mdoc (3.2) is issued
- **mdoc verifier**: person or organization using and/or controlling an mdoc reader (3.3) to verify an mdoc (3.2)
- **mDL**: driving licence that fulfils at least the same function as an IDL but, instead of being paper or plastic based, is an mdoc (3.2)
- **mDL reader**: mdoc reader (3.3) that can retrieve mDL (3.6) data
- **mDL holder**: individual to whom an mDL (3.6) is issued, i.e. legitimate holder of the driving privileges reflected on an mDL
- **mDL verifier**: person or organization using and/or controlling an mDL reader (3.7) to verify an mDL (3.6)

11

These slides represent the personal opinion of the author

Terms and Definitions 2

- **device retrieval**: method of data retrieval exclusively using the interface between the mdoc (3.2) and the mdoc reader (3.3)
- **server retrieval**: method of data retrieval using the interface between the mdoc reader (3.3) and the issuing authority infrastructure (3.13)
- **MSO**: mobile security object
- **IA**: issuing authority
- **IACA**: issuing authority certificate authority
- **IDL**: ISO-compliant driving license
- **VICAL**: verified issuer certificate authority list (a.k.a. PKD)

12

These slides represent the personal opinion of the author

Functional requirements

The functional requirements include

a) An RP can request, receive and verify the integrity and authenticity of an mDL whether online connectivity is present or not for either the mDL or mDL reader.

b) An mDL verifier not associated with the issuing authority can verify the integrity and authenticity of an mDL.

c) An mDL verifier can confirm that the person presenting the mDL is the mDL holder.

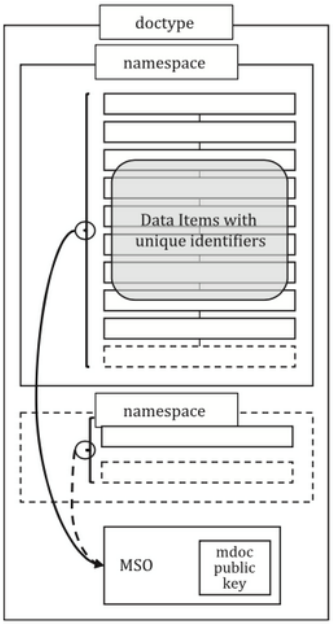
d) The mDL to mDL reader interface supports the selective release of mDL data

13

These slides represent the personal opinion of the author

Data structure sketch

- Note that for each 'doctype', multiple 'namespaces' are possible
  - i.e. a doctype=mDL can have namespaces from 18013-5 plus domestic jurisdiction, plus whatever. This causes issues when attempting to 'flatten' the data structure. E.g. which 'first name' is the authoritative one?
- MSO includes
  - Hashes for each data element
  - The public key associated with the mDL
  - Signed by Issuer's key



14

These slides represent the personal opinion of the author *Image excerpt from ISO 18013-5*

Data exchange steps

- Device engagement:
  - to authenticate parties as required; set up ephemeral keys; signal to switch to data transmission channel
  - QR or NFC
  - Day 2/18013-7: 'over the internet'
- Data retrieval:
  - from the mDL app (online or offline) or from the issuer infrastructure (online only)
  - NFC, BLE, WiFi Aware
  - OIDC, WebAPI (possible, but not preferred)
  - Day 2/18013-7: websocket, REST, OIDC SIOP
- Note that the mDL presents engagement data and the mDL Reader uses that to set up the connection. 'Reverse engagement' will be drafted so mDL app reads engagement data from the Reader side.

15

These slides represent the personal opinion of the author

mDL Transaction Flow

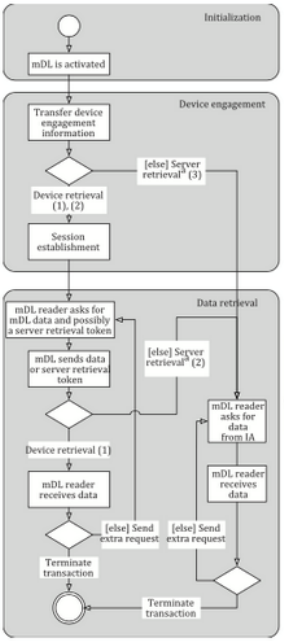
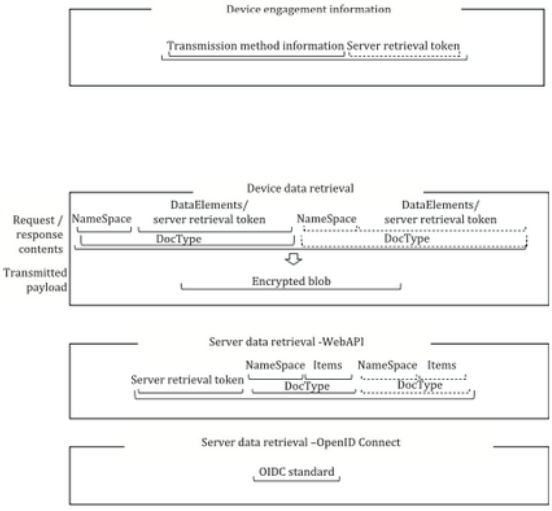


Image excerpt from ISO 18013-5



16

These slides represent the personal opinion of the author

Security goals

Table 4 — Security goals and mechanisms

Security goal	Functionality	Device retrieval	Server retrieval
Protection against forgery	Authenticate the origin of mDL data	Issuer data authentication	JWS
	Verify mDL data has not changed from issuing authority	Issuer data authentication	JWS
	Verify how up to date the mDL data is	Issuer data authentication	JWS
Protection against cloning	Protect against cloning of mDL/ binding mDL data to a specific device	mdoc authentication	mdoc authentication[a]
Protection against eaves-dropping	Preserve confidentiality of mDL data	Session encryption	TLS
	Prevent unnoticed alteration of communication	Session encryption mdoc authentication	TLS
Protection against unauthorized access	Prevent unauthorized access of mDL data	Close-range device engagement with session encryption	Close-range device engagement (with session encryption)[a]
	Prevent unauthorized access of mDL data	mdoc reader authentication[b]	TLS client authentication[b]

[a] Only applicable if the server retrieval token is transferred using device retrieval.
[b] This is an optional method.

Image excerpt from ISO 18013-5

17

These slides represent the personal opinion of the author

Data elements

- mDL doctype+namespace has all the data elements you would expect in a driving license
- Must include subject Portrait photo from the issuer
- Optionally includes elements to support age-related selective release
  - Age_in_years; age_birth_year; age_over_NN
- Verifier is responsible for confirming that Presenter is the Holder (the intended Subject) - currently this means compare Portrait to person's face
- Supports 'domestic data elements' - public/semi-public/ private namespaces

Data integrity features

- See Clause 9 of ISO 18013-5

Issuer certificates and keys infrastructure

- VICAL - master lists of authorized certificates similar ICAO PKD
- Unclear how unregistered mDL Verify apps can exist (like person to person ID Verification apps)

cheqd: Payment Rails, Customisable Commercial Models and Decentralised Governance for SSI (pressie & AMA)

Wednesday 10A
Convener: Fraser Edwards, Alex Tweeddale
Notes-taker(s): Ross Power & Alex Tweeddale

Tags for the session - technology discussed/ideas considered:

1. What are the problems with existing SSI in terms of business and economic incentive models?
2. Why does Self-Sovereign Identity need more sophisticated payment systems?
3. How does the cheqd Network bridge this divide, in a way which is standards interoperable and ledger-agnostic?
4. The importance of performance, scalability and decentralisation for Layer 1.

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

Link to Session Slides:
https://www.dropbox.com/scl/fi/m6n94inenmgnpo8mo3qc1/IIW-presentation.pptx?dl=0&rlkey=hzagsgr1rkd28m3j9dmp0gr7u

Session Summary:

1. Fraser Edwards presented cheqd's vision of becoming the de facto leader in payments in exchange for Verifiable Credentials.
2. The presentation began with the commercial challenges that many SSI projects have faced, in terms of lacking a tangible business model.
3. The presentation demonstrated how a token, built on a decentralised public-permissioned Network, cheqd, could lower KYC costs for ecosystem participants as well as create new recurring revenue streams for Credential issuers.
4. The Network also utilises a decentralised governance model, to avoid a single point of friction or failure in the Network which can generally be seen from centralised governance authorities.

Questions:

1. Fraser was questioned on the privacy preserving nature of monetising credentials, specifically, whether cheqd can considered that payments could be correlated if Credentials were set at unique price points. The answer to this question was that payments will likely not take place atomically on cheqd, but in aggregate - removing the risk vector for price and identity correlation.
2. Fraser was questioned on how the revocation registry was going to be implemented to meter the payment of Verifiable Credentials in a privacy-preserving way. This is a work item that will need to be followed up and worked on with the community.

COVID Credentials: How To Meet The Market Where It Is

Wednesday 10B
Convener: Lucy Yang, Kaliya Young, John Walker
Notes-taker(s): Lucy Yang

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

The community leaders of the COVID Credentials Initiative (CCI) share how CCI is working to meeting the market where it is by address three questions:

- What is CCI and how has CCI evolved to meet the market?
- What have we learnt from the GHP Interoperability Blueprint work?
- Where is the market today and what are our opportunities?

Session Slides:
https://docs.google.com/presentation/d/1n6OirMXMJN43PM7VpvypHMecV0J0ILvf0hAZSrPzBDE/edit?usp=sharing

Fantastic DIDComm Protocols and How to Write Them

Wednesday 10D

Convener: Sam Curren
Notes-taker(s): Sam Curren

Tags for the session - technology discussed/ideas considered: DIDComm, Protocols

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

Session Slides: https://hackmd.io/rwOOObn4RzaITcC217lGpw
(more links in slides)

Q&A

- Sandboxing? (see links)
- DIDComm protocols <> Aries RFC relationship?
    - From TimoGlastra to Everyone: So all Aries protocols are DIDComm protocols, but not all DIDComm protocols are Aries protocols if that makes sense; DIDComm is extracted from Aries in V2. You can use DIDComm without Aries, but can't use Aries without DIDComm. Aries is focused on creating, transmitting and storing verifiable digital credentials, while the application of DIDComm is much broader
- Alex from Spherity: FInal version when? Feature freeze? How/when to buidl?

- Geo Fletcher “v2 is almost done but v3 is already starting” sounds really scary, this sends up red flags about timeline and life expectancy
- Vic C: does an ecosystem sprout from this? An app store?
    - Sam: I can see lots of systems (and the web) integrating this as a protocol (the way everything does email), or bootstrapping it
    - Sam: This would’ve been easier to build as a product/platform, but building it as a protocol strives for the goal of being like email
    - Vic: How could people “invest” in the protocol beyond just donating code/review/etc? Is a “token” out of the question?
    - Sam: I’m nervous about binding the DIDComm protocols to a long-term risk; a token could crash, be a net negative, etc;
        - Protocols could go this route, but not the DIDComm framework around it; protocols could be proprietary, support a tokenized network, etc
    - David: Why did SMIME fail?
        - [from chat, Sebastian]: SMIME certs cost money-- let’s encrypt for DMIME is missing
        - Sam: I mean, DIDs and DIDComm are, debatably, PGP with more steps!
        - [from chat, Bart]: PGP failed because it was too technical, I worry DIDComm could too… or put differently: people use apps/services, not technology/protocols
        - Sam: i can’t really answer this…
        - [Natgeo]: Especially in light of our tendency for creating so many “V1 layer” alternatives —> if you have more than one key server (or key ledger/chain/etc) you ain’t got any. Key management philosophy matters, and we still have a lot of work to do there
        - Sam; I tried doing TLS with DIDDoc keys, which is allowed by the DID spec… but `openSSL` and all the commodity TLS tooling assumes lots of things, and would have to be reimplemented all the way down…
            - Partic for mobile-friendliness and async routing :/

Links from the Zoom Chat:

- Sandboxing? Anything like the eth community’s Ganache?
    - Sam C: Aries toolbox is a little out of date (cert issue), but it works!
    - (from audience) Don’t know If this helps but we release a Typescript open sourced npm package based on Aries Cloud Agent Python which tends to track DIDComm developments

Exclusive Self-Ownership

Wednesday 10E

Convener: Paul Trevithick
Notes-taker(s): Markus Sabadello

Tags for the session - technology discussed/ideas considered: Personal Data, Self-Ownership

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

What if all your personal data lives on a device you own?

There is data about you but not owned by you. Fragments and shards of your digital self. From a technical point of view you own it, but you may not "really" own it.

Data is bought and sold, we are subservient, there is power distortion.

New idea: Data sits in your hands, it's yours, we don't allow copies of it! Can be enforced through technical and legal mechanisms.

An Extended LDP-BBS 2020 and ZKP-LD Playground

Wednesday 10F
Convener: Dan Yamamoto and Kazue Sako
Notes-taker(s): ***

Tags for the session - technology discussed/ideas considered: BBS+, ZKP, Cryptography, JSON-LD

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

Session Slides: https://drive.google.com/file/d/1xKjXbzwMdZC5azPuRy-mtWuyfEuqsb8T/view?usp=sharing

Playground link: https://playground.zkp-ld.org/

Github Code links:
https://github.com/yamdan/zkp-ld-playground
https://github.com/yamdan/jsonld-signatures-bbs
https://github.com/yamdan/bbs-signatures
https://github.com/yamdan/bls12381-key-pair

The Mattr's BBS+ LD implementations were forked and improved upon. Instead of signing each whole N-Quad, each term of each N-Quad is signed. Multiple credentials can be aggregated.

Demo of ZKP-LD playground showed multiple issued credentials with different credential subjects being aggregated into a single presentation

There is an intention to use these changes as the start for a new signature suite (perhaps BbsBlsSignature2021)

There is interest in future work: recipient binding, range proofs, ...

The id URLs can be anonymized for each presentation, but the same id's are the same within a single presentation.

It may also be possible to use k-times anonymous presentations

Currently use an informal URN: urn:anon:xxxxxxxxxxxxxx for anonymized URIs. Standardizing it should be one of the future works.

Finding alternatives for LD Canonicalization (if any) is one of possible ways to improve efficiency.

Current version of ZKP-LD Playground and three libraries possibly contains bugs; any feedback is welcome to make them better.

Discussion of using this extension with DIF presentation exchange

Zoom Chat:
Brent Zundel: +1 to defining a new signature suite

Brent Zundel: exactly what I was getting at

Kyle Den Hartog: Second follow up question

Kyle Den Hartog: Have you considered other canonicalisation mechanisms to reduce the proof size?

Nuttawut (Finema): May I ask if "urn:anon" a standardized URN?

Nuttawut (Finema): thank you

David Huseby1: So you're going to keep a cache of ZKP presentations to try to detect people falsely presenting somebody else's proof?

Hakan Yildiz: Absolutely, great work!

aj-finema: Is it possible to share the presentation?

aj-finema: Thank you :)

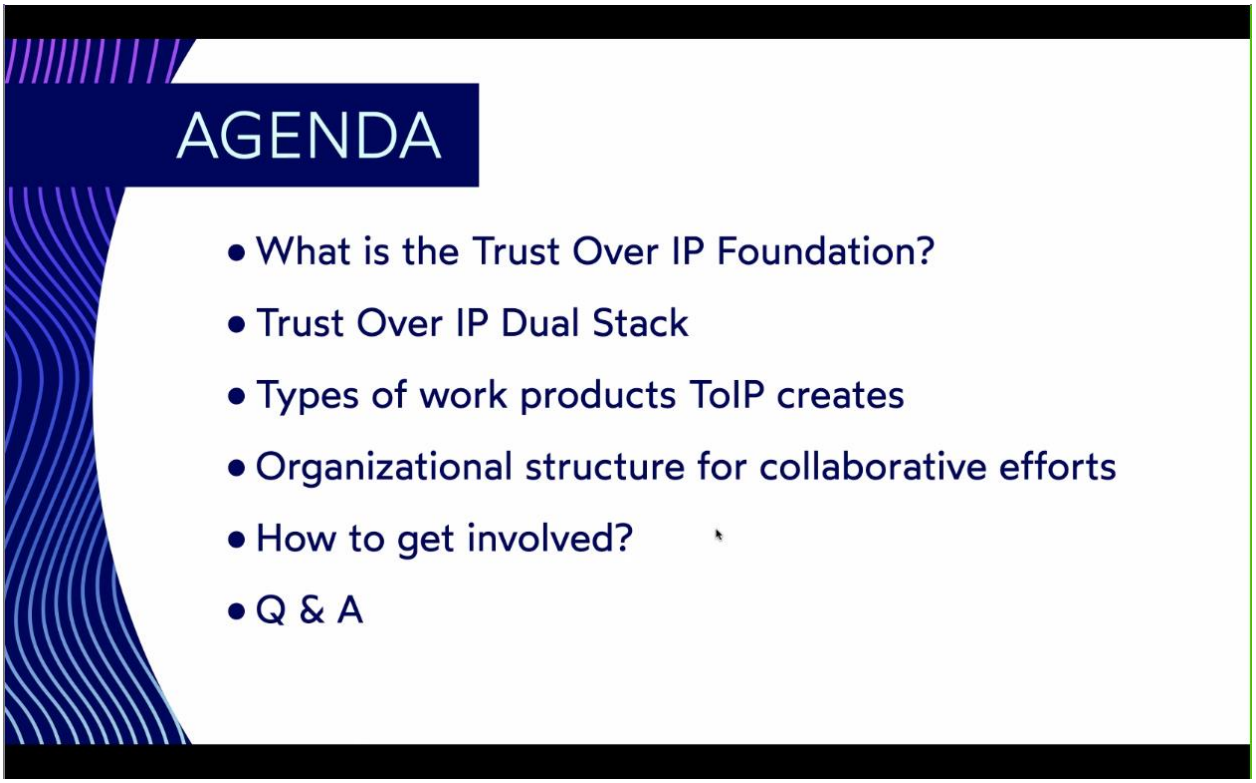
Introduction to Trust Over IP

Wednesday 10H

Convener: Judith Fleenor
Notes-taker(s): Charles Lehner

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

Join Trust Over IP
https://trustoverip.org/get-involved/membership/



How does the Trust Over IP foundation fit in? What kinds of work products do we create? What is the organizational structure? How do you get involved? Support us financially?

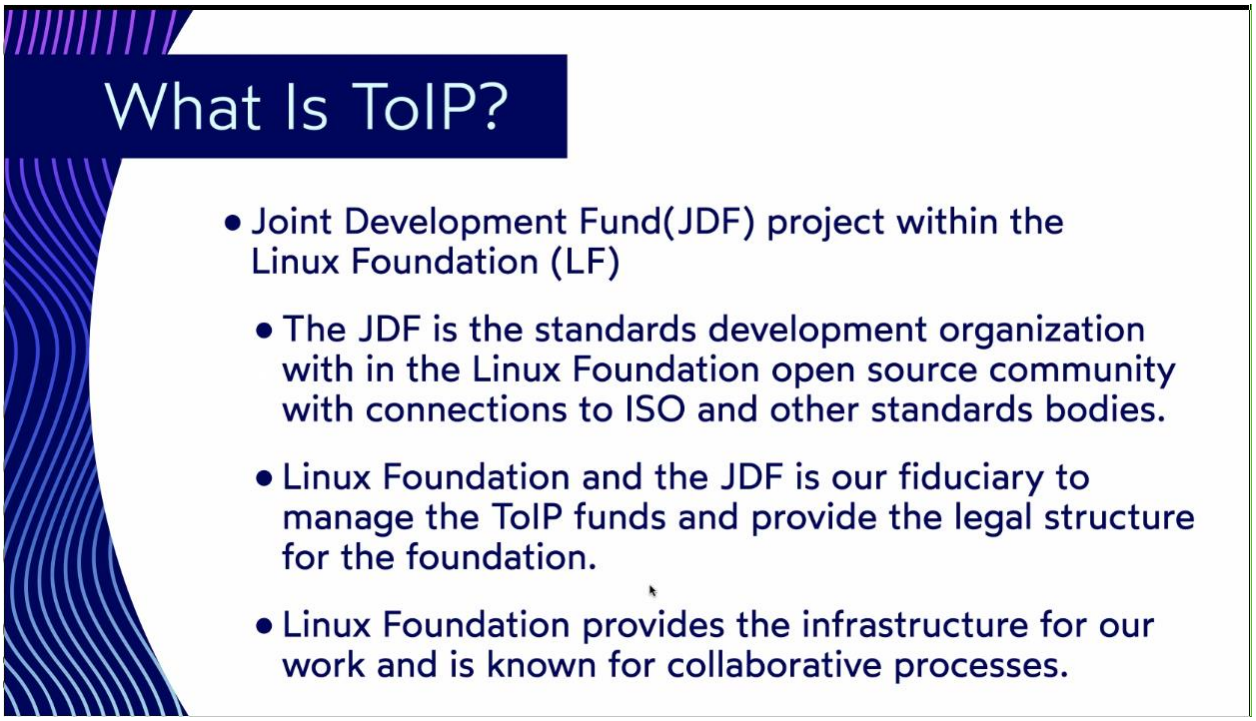
Difference from other organizations: we focus on both cryptographic interoperability at the machine layer, but also on the human accountability on the legal, business and social impact layers. We do both.

ToIP is a collaborative community.

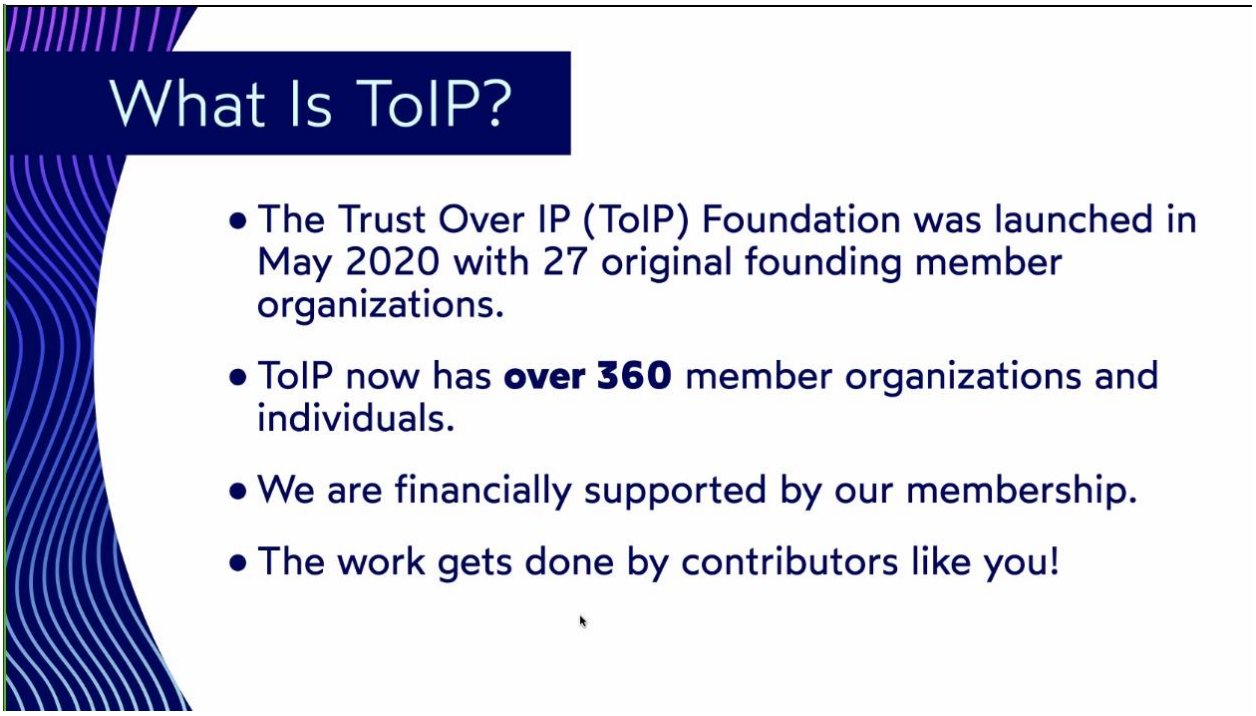
We get together, discuss things, hash them out, argue about it. A JDF project within the Linux Foundation. Financially supported by membership. Contributors can join for free.

Collaborative community. Uses Zoom. Also uses asynchronous collaboration via Google Docs, GitHub and Slack.
Who is involved? Industry experts, and people new to Decentralized Identity.

JDF is a proto-standards development foundation within the Linux Foundation. JDF has special tracks to take something out of the JDF, for standardization - a “fast track”.

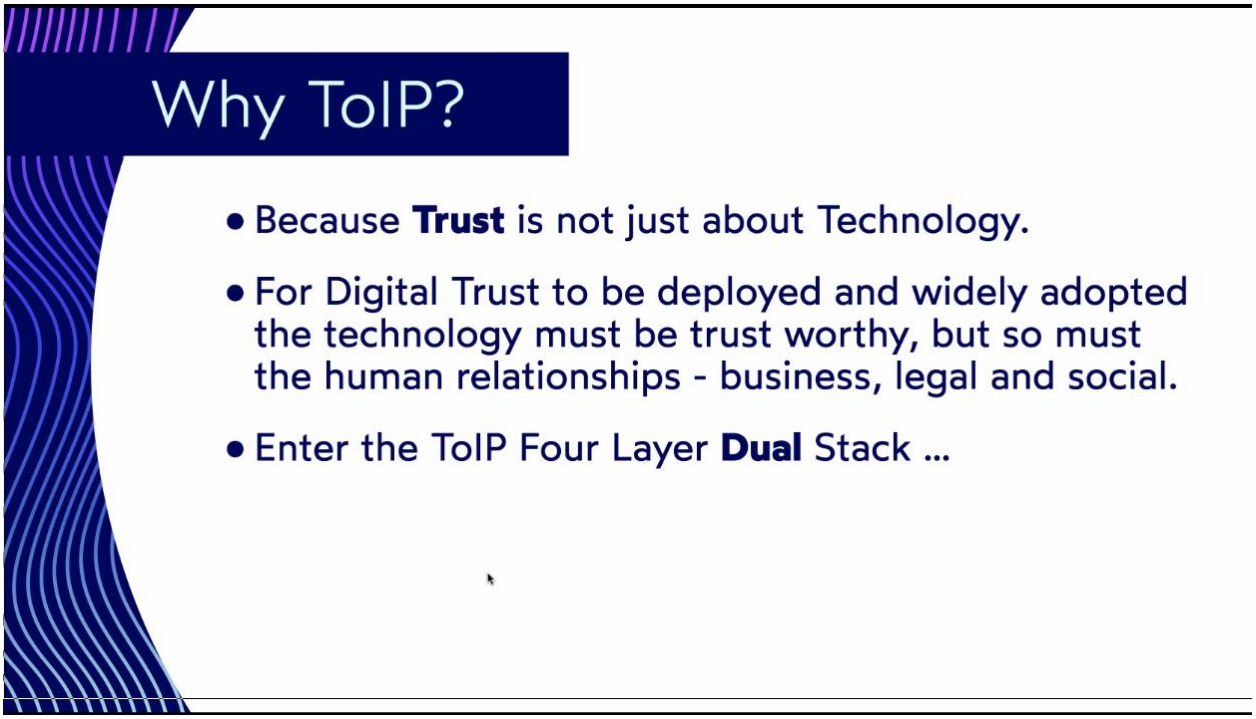


… Linux foundation provides infrastructure also…

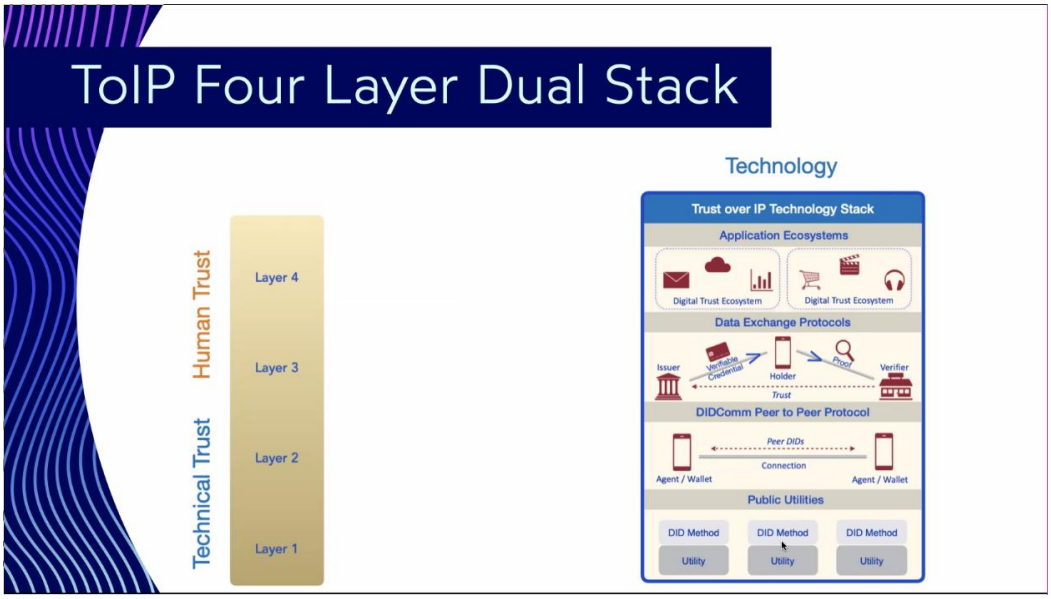


ToIP foundation started just over a year ago - 27 founding members - but the need came way before that. See the whitepaper on the website for more history. Now has over 360 member organizations and individuals. You can join as an individual or for your member organization.

We are financially supported by our members.
When we have enough money…. We can hire… otherwise work is done by [volunteers].

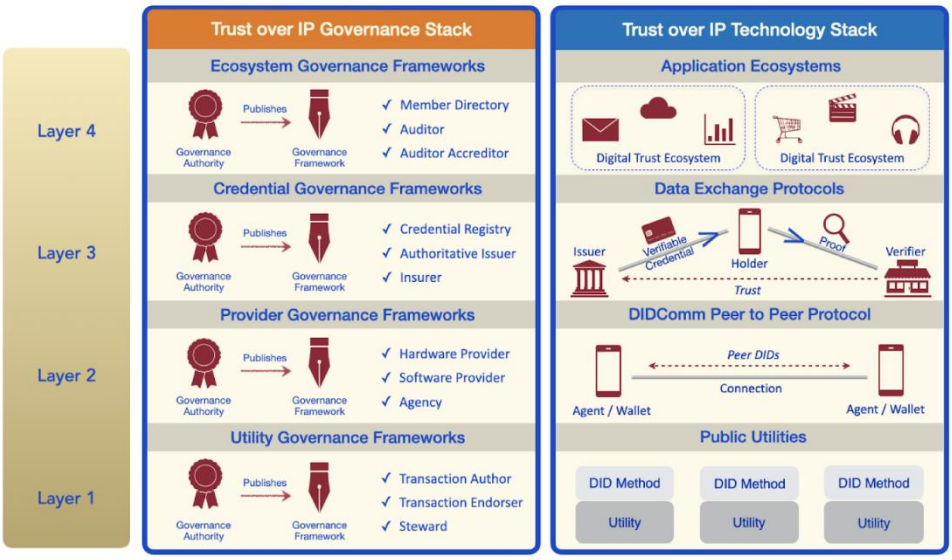


Trust is not just about technology.
We're not just the Technology over IP foundation… The tech must be trustworthy, but also the social, legal and business relationships… The ToIP Dual Stack.



We collaborate with DIF… whether at the public utility layer, exchange protocols…. This work is getting pretty solid in the world. From our point of view, so much is not done yet… but compared to a few years ago, we've come a long way.

We've noticed that even though the technology layer is starting to come together, there is a missing piece to make it all work - that's the governance - the legal, business, social impacts that must happen - because this technology exists. We've realized that these things cannot be separate: you cannot design the tech without the governance… In fact, the governance leads the tech decisions.



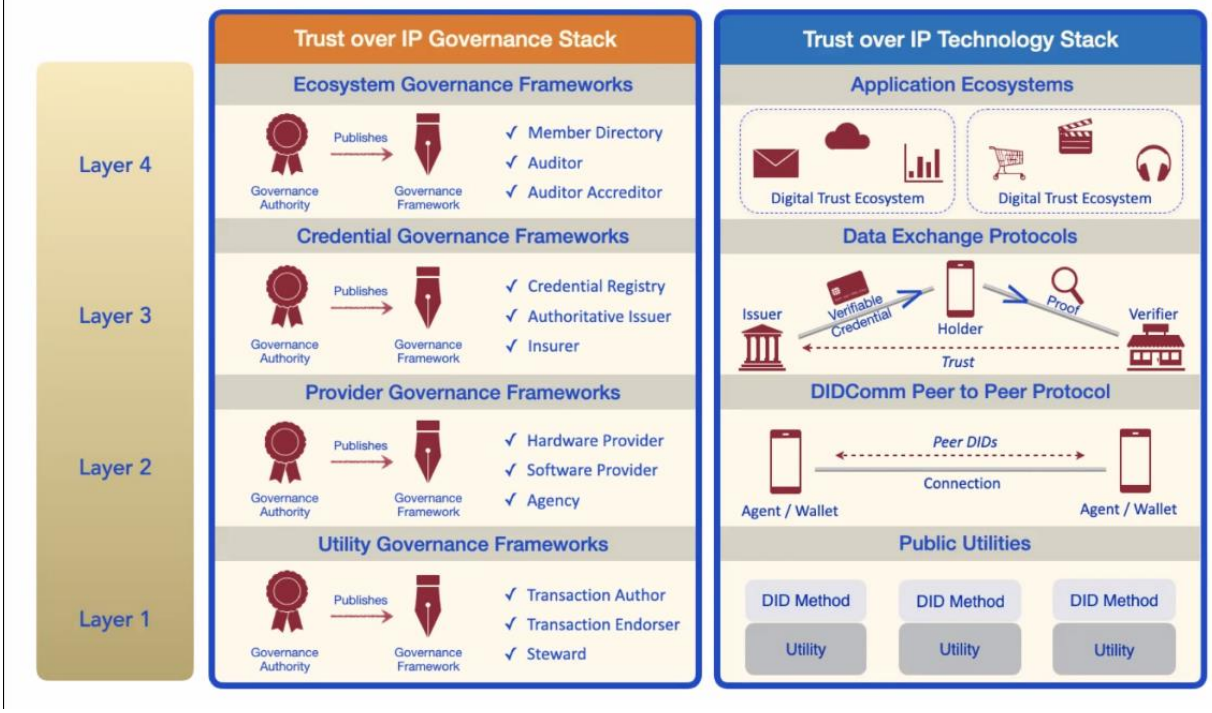
The four layers of ToIP infrastructure are analogous to the four layers of our ground transportation infrastructure

I'm a "muggle"... want to make it simple… Stole this from Drummond…. Four layers like ground transportation…. Layer 1: Roads, highways, public utilities that have to be there in order for anyone to do transportation. Above that….
Layer 2..., Layer 3..., Layer 4...

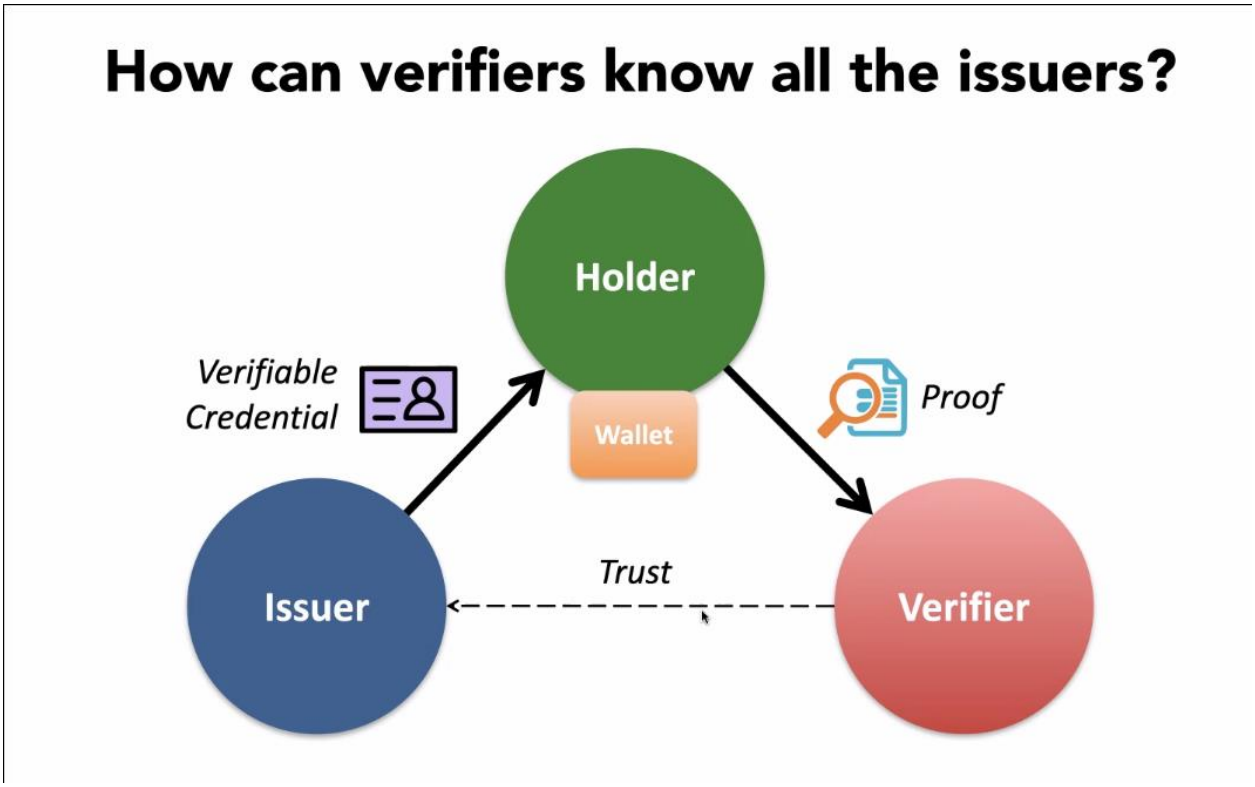
Layer	Purpose	Tooling Required at each Layer
4	Transportation Industry (Market Applications)	
3	Signage & Traffic Controls (Rules of the Road)	
2	Cars & Trucks (Private Equipment)	
1	Roads & Highways (Public Utilities)	

Compare to Trust over IP…

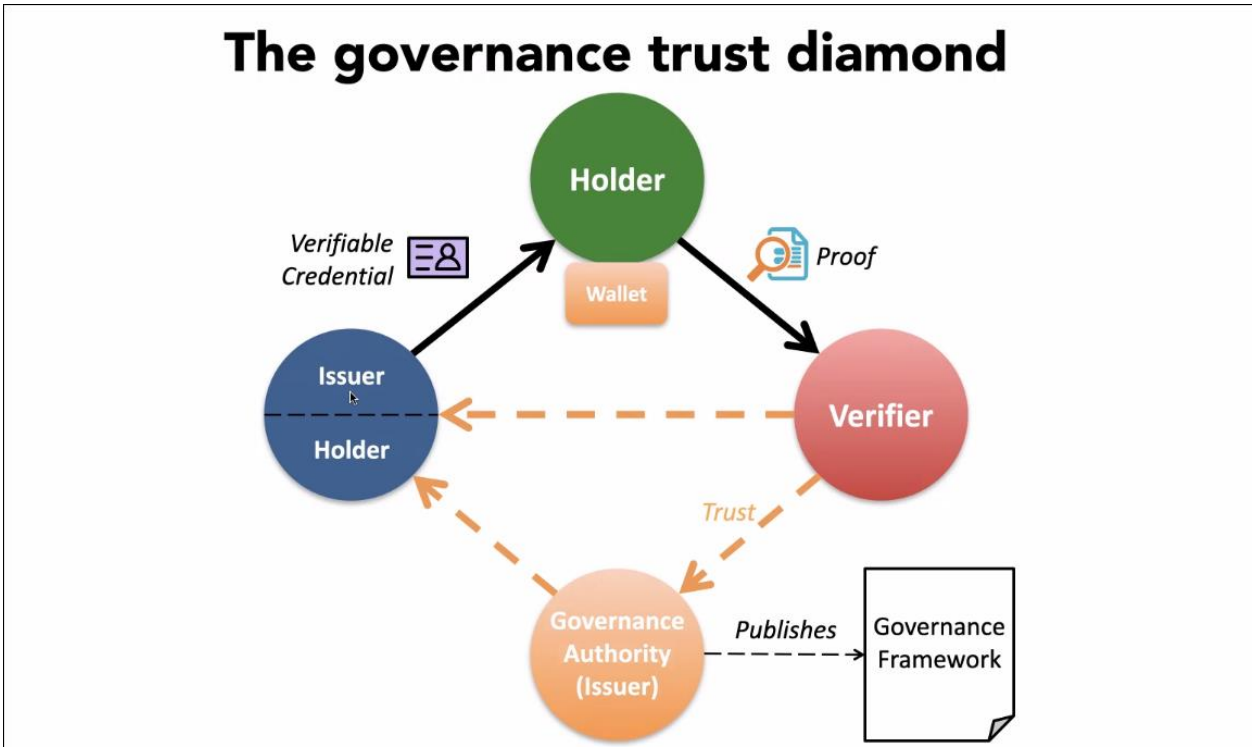
(layer 1) Sovereign network governance framework most fully formed at, but other networks like ID Union and Check'd are working on theirs and I think Check'd is giving a presentation on theirs later today.
Above that, peer to peer protocols (layer 2)
Above that, …
(layer 4) Some examples of governance frameworks at layer 4 being worked on at ToIP and elsewhere are YOMA, GLIEIF, IATA… etc.



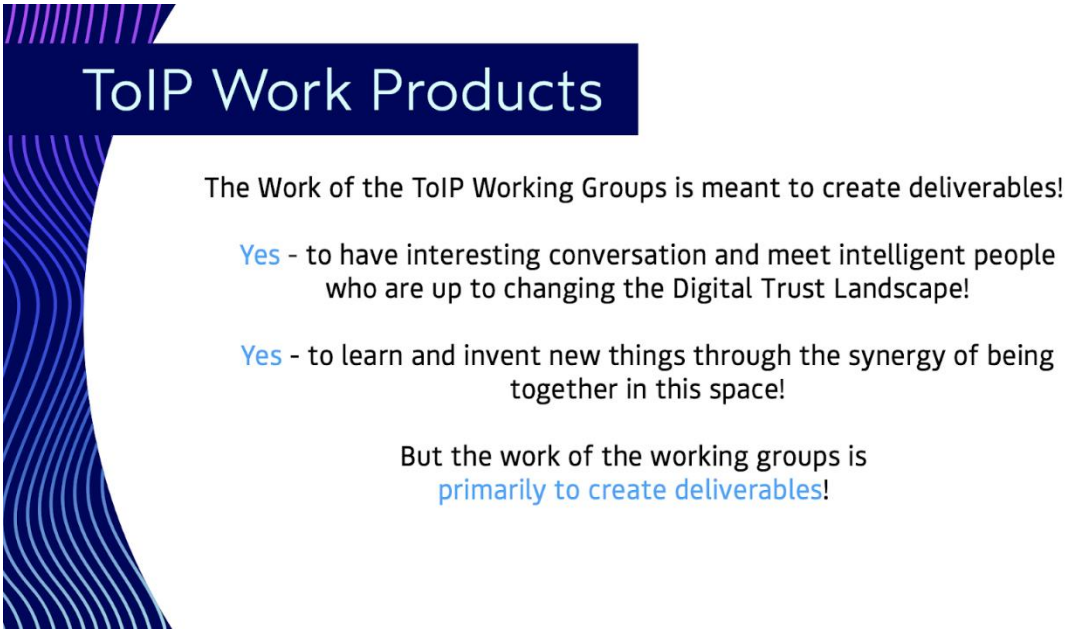
Yoma - organization working with UNICEF for jobs for youth - their governance framework sits in conjunction with the technology choices.



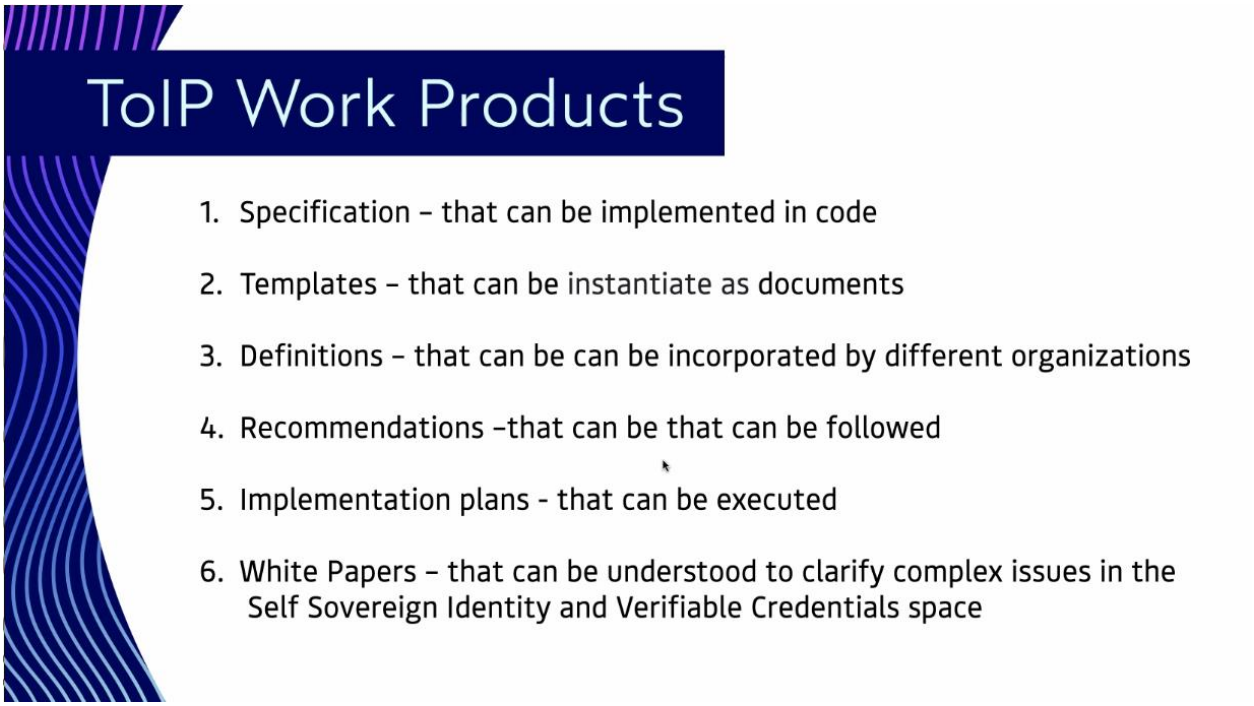
The Trust Triangle… Issuer issues certificate, puts it in the Holder's wallet… Then some Verifier asks for some sort of proof to verify whatever it is… Think of the driver license… trying to get beer, they ask for it so you can't get it [when you are too young]... That's okay, in the old world, because you don't remember everything you see on it - unless you're Rain Man. Now you just want to give the proof "are they old enough" to the verifier. In the old model, you have to go back to the issuer to ensure trust - in the new model, you don't have to do that.



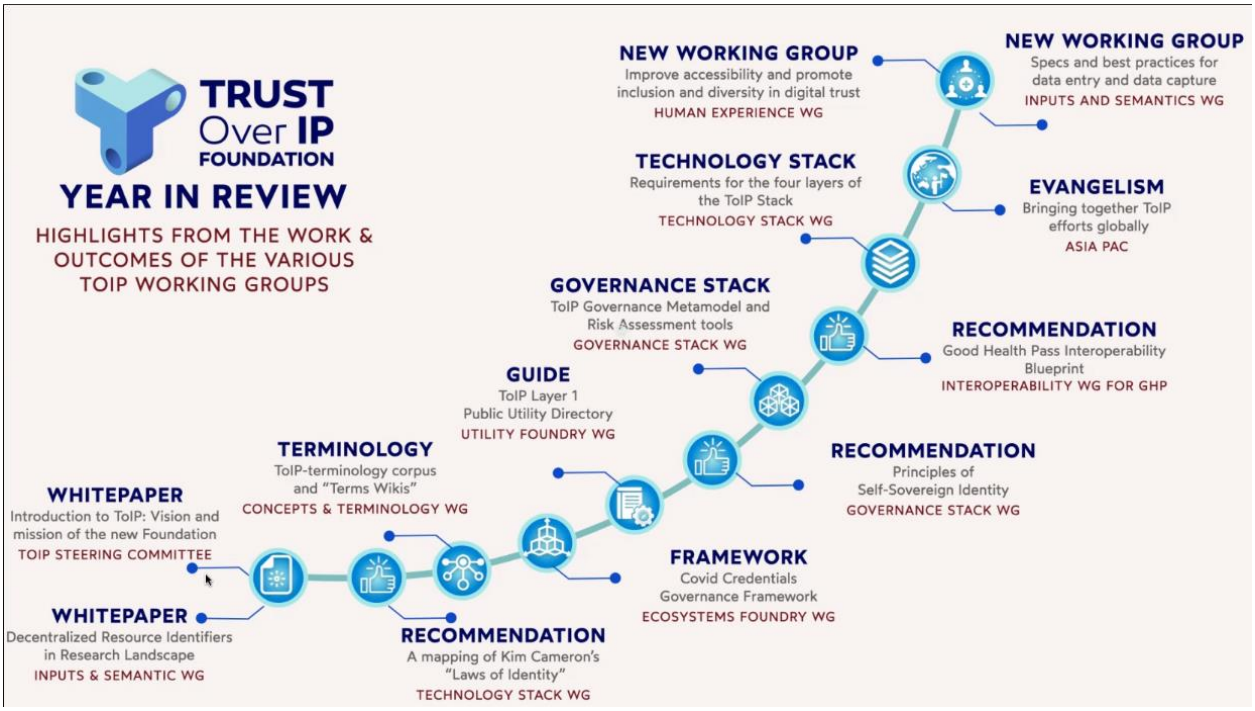
In a governance framework, you don't want to have to go back to every verifier to make sure it is okay… the verifier can just look at it and say yes this is a valid credential… like in the real world a credit/debit/bank card… they issued it because they are part of a governance framework. This bank gives it…. To the holder…. Then the verifier knows it is part of the governance framework and knows they can trust it… This is why governance
No integration(?) needed between the issuer and verifier.



Work products done in Working Groups… meant to create deliverables… We make things and have synergy… that's the fun… but the work is to create deliverables.



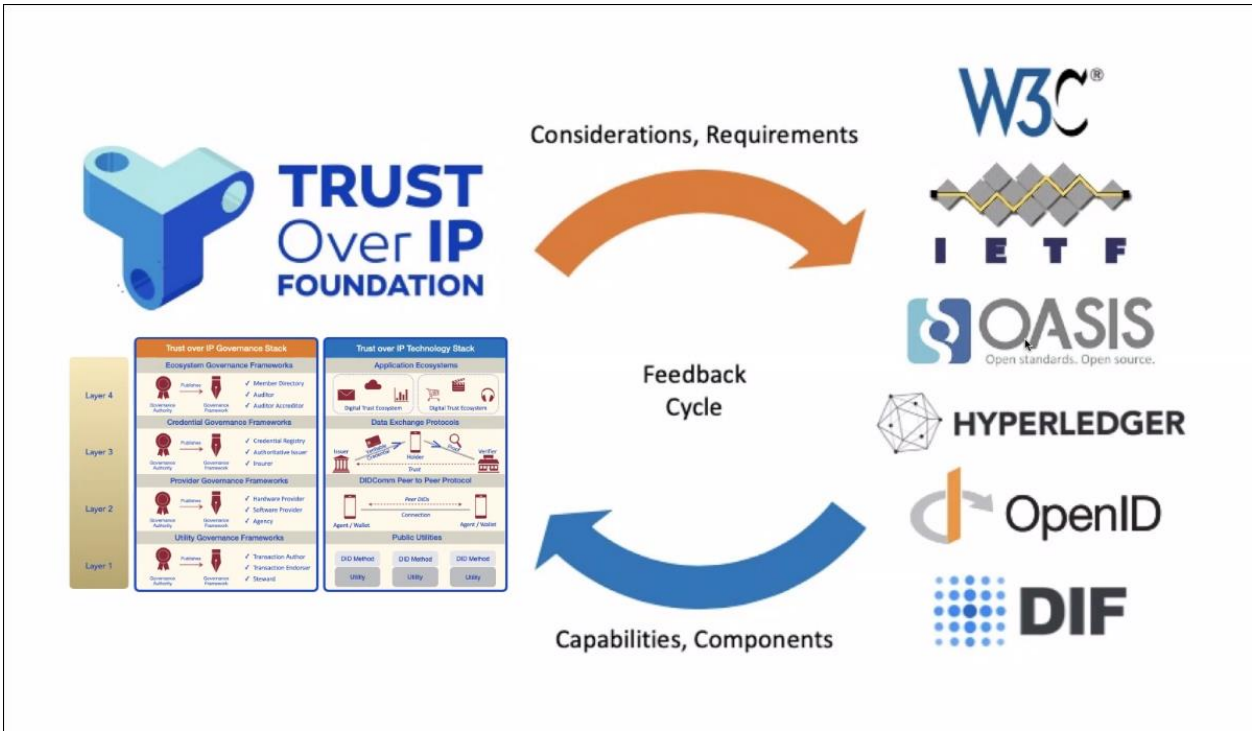
1. Specifications
2. Templates
3. Definitions
4. Recommendations
5. Implementation plans
6. White paper



Example: first year…. Introductory white paper being rewritten… in a collaborative process, since August… hopefully the new ones will come out soon…
Larger project: Good Health Pass Interoperability Blueprint… shows the collaborative effort… started in 2020… Good Health Pass Collaborative… realized they didn't have the infrastructure to get it written… task forces, working groups…. So we spun off a working group, the Interoperability for Good Health Pass Working Group to help develop this - that became a 180-page paper. But governments didn't pick it up? Doesn't mean it wasn't very important work…. The 120 collaborators were able to think of issues they might not have thought of otherwise.... The work, even if not immediately adopted, is making movement toward the eventual future.

Human experience group… on its third meeting… Europe-friendly time… join that.

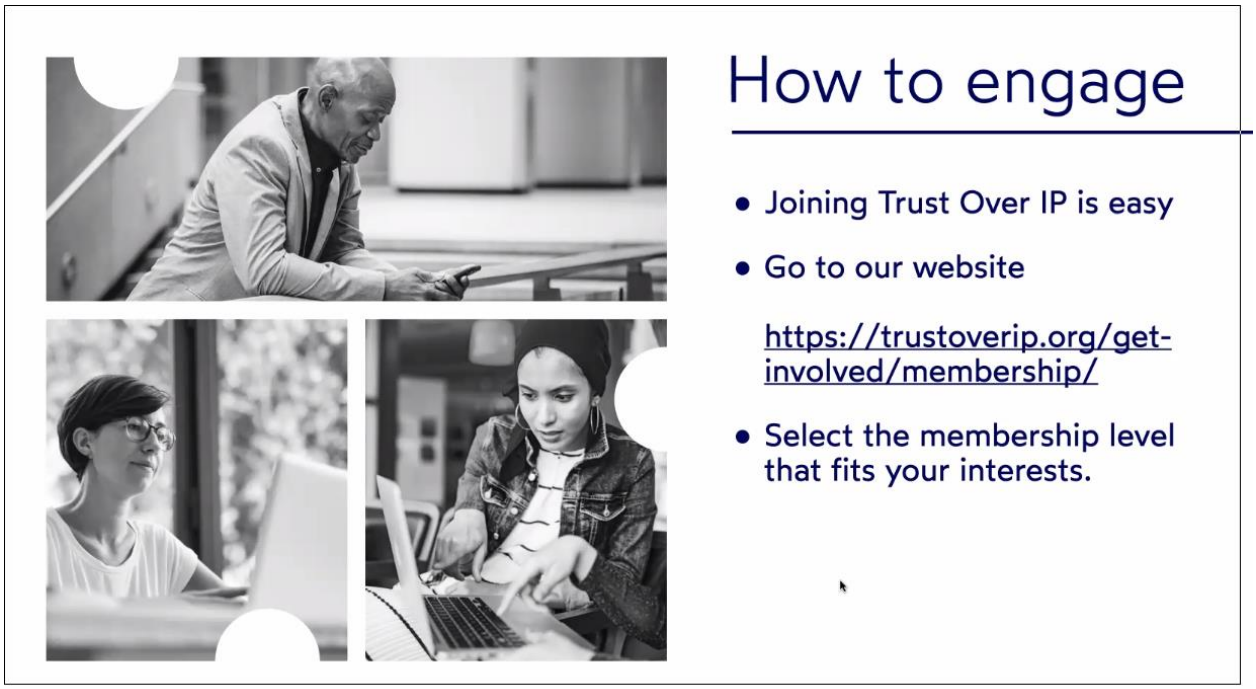
ToIP isn't trying to replace any of the other organizations, standards bodies, development organizations… but we are constantly collaborating with them….



Hyperledger…. Aries…. DIF… doesn't mean we're all about that, but we collaborate with them… If you know someone..., they can become a member as well.

Working groups…. They work across with each other…. Governance Stack and Technology Stack are not working completely separately…. Inputs and Semantics goes deep talking technical details all day…. Concepts and Terminology - creating a terms wiki - for use by any organization… to render a glossary… so

two projects could list wording conflicts in the directory, when different ecosystems have different meanings for words… available for any organizations, not just ToIP WGs.



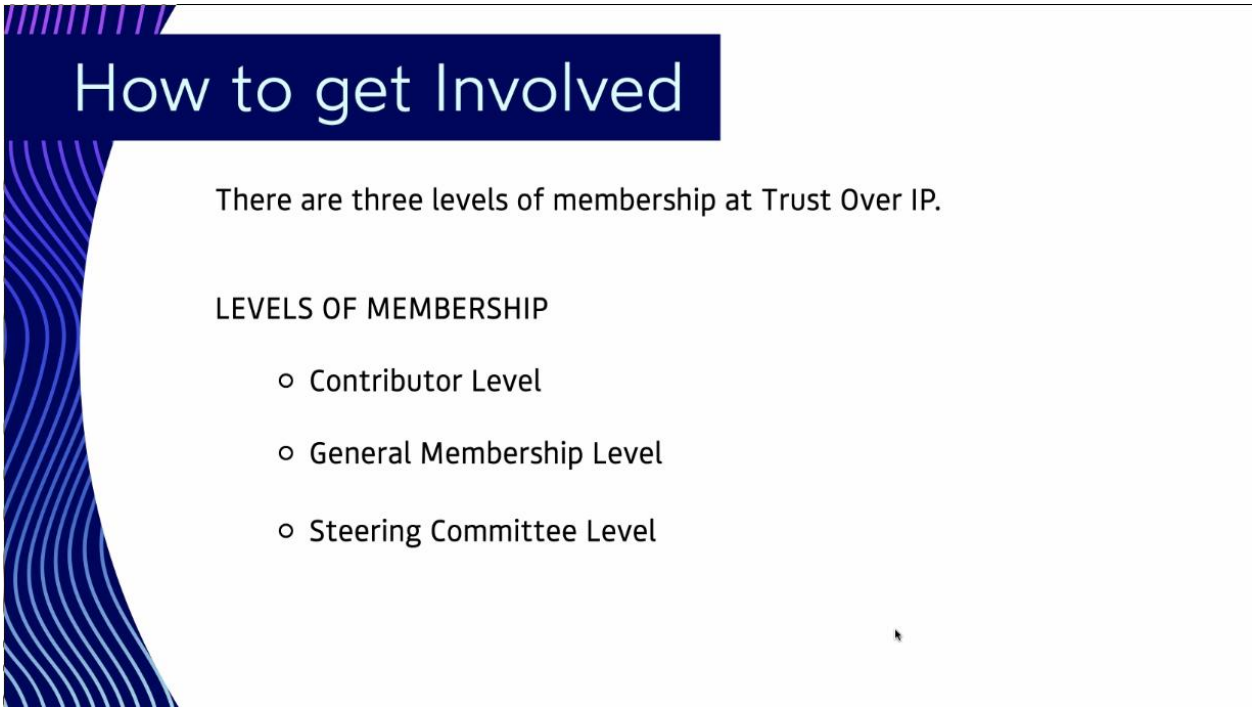
How to Join? Go to website, select membership that fits with you.

Question from Jeff O - what is frustratingly exciting about this work for you right now?
Any edge-space stuff that you are reaching towards but maybe don't know the people…?

Judith: There is so much work to be done in all these areas… Sometimes we can get sideways on little details… then people get frustrated they don't have time to work on it, because it's too complex, and they are overstretched on multiple projects and tasks… People may get frustrated it's not moving fast enough…. But at the same time too overwhelmed to do it all… Baby steps are better than no steps… We didn't start walking by running a marathon, we stand up and fall down, stand up and fall down, then eventually can run the marathon.

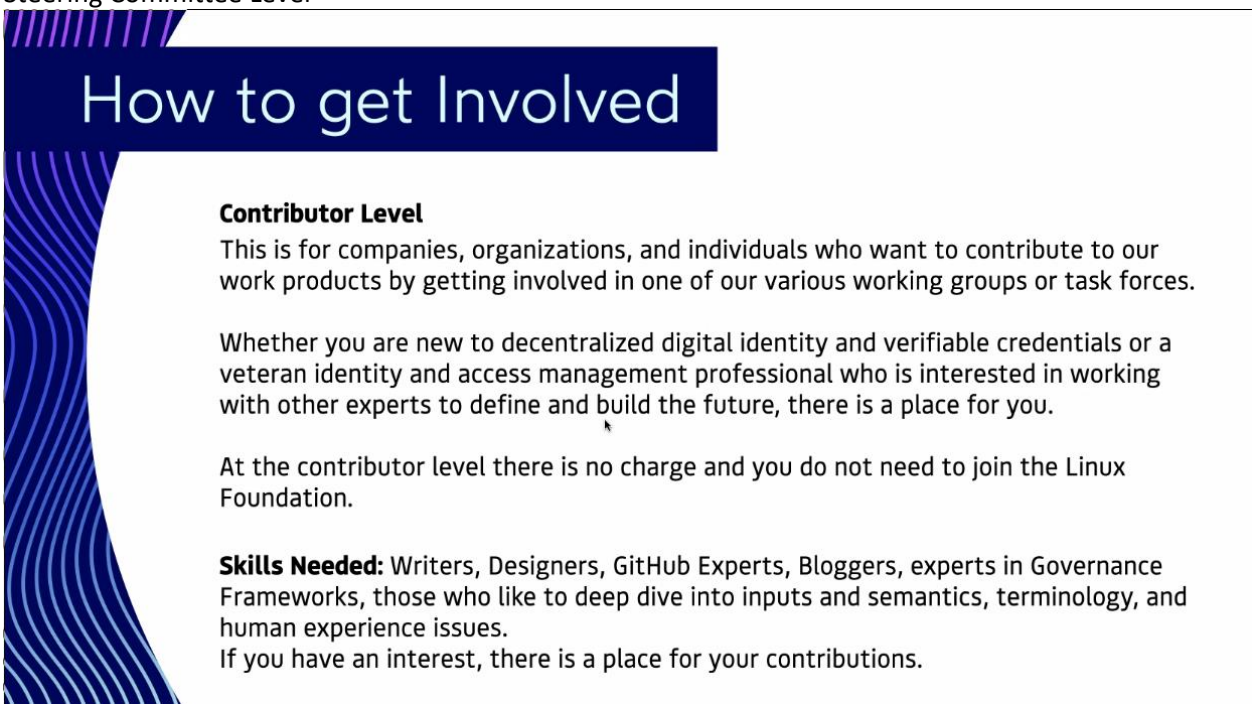
Jeff O: Thank you.

Judith continues the presentation...



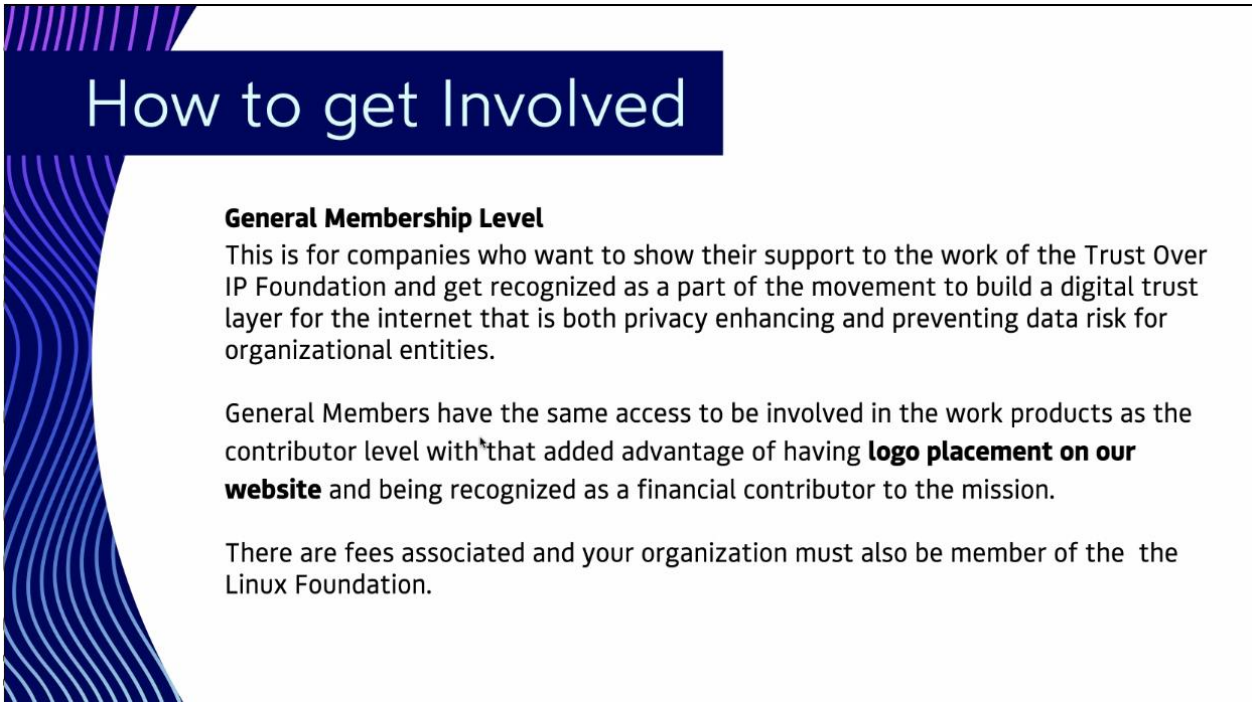
Levels of membership…

Contributor Level
General Membership Level
Steering Committee Level



You don't have to know everything about Decentralized Identity to contribute…. We need writers, designers, GitHub experts, bloggers… [you can learn about decentralized identity through this]…. We also need experts in governance frameworks.
… If you like to get into terminology, mental models, there is a working group for that.
… Human experience… may have several task forces coming up…

… For people who want to join, meet people, and enjoy collaborating.



General Membership Level - if you want to show support, get recognized for building the movement, financially. Logo placement. Fees based on size of organization. Must be a member of the Linux foundation.

Steering Committee…. For organizations that want to be a part of the strategic direction… they have the ability to become voting members of the Trust Over IP Foundation…. If you are interested in this, reach out to me judith@trustoverip.org and we can discuss it further.

Jeff O: What's the stickiest stuff… if you were to tell someone in a minute the "cool factor"... what would you say?.... Great technological concepts in play and underway…. If they are technologically inclined… what's your best one or two lines for someone interested?

Judith: One ecosystem is called Yoma(?). They are working on a marketplace for youth in Africa… The big problem is that they can go to school, get education, but they when going to get a job, they're asked "where is your experience?" - So this marketplace… people could put things on it like "I need a designer to do XYZ…" then youth can apply do the work and they get credits that show they have this experience in the marketplace… An example of a good use for Verifiable Credentials solving a need in the world.

… Another project…out of Luxemburg… Product Circularity Data Sheet(PCDS)… What's actually in various goods… so when it comes time to recycle… the recycler would know how to process it… Our General Member GS1 might be able to assist them.... The more they start to look at their PCDS module they are seeing… we need to be able to do it in a decentralized way. They came to collaborate with with our industry experts.

Darrell is the chair of our Technology Stack…. Led a session yesterday… Interoperability not really there yet…. The sticking point…

Phil: The reason I came to this session is I'm still trying to figure out where I need to be… I have at least 2000 unread emails from Heather's group in the CCG… many from ToIP… please don't take it personally… I know that GS1 collectively… my colleagues… we know we need to engage more… but we can't be everywhere at once, and we need to work out where we need to be… Heather has good lines about why I should be in the CCG…. You mentioned the Circular Economy…. Yeah, and hundreds of others…. How does anyone navigate this space? Come to IIW... I don't know the answer.

Judith: ToIP isn't trying to displace other organizations… we want to be a collaborator that pulls other organizations in, and works across silos…. I think we have to bring ourselves back down a bit and work across silos at the thinking level… Let's get a call in the next couple weeks… I think the PCDS people… would be good for you to know about…

Heather: I came here because… there are lots of different groups… My attitude and personality… my role in CCG… I'm in the CCG world, but I got the role because I was annoyed by the way things were being done, and decided to be the change I wanted to see… so please don't think I'm some W3C tool… I don't think I'm particularly well-liked there… But my goal is to increase diversity and inclusion there…. I tend to be blunt, please don't be offended… There are a lot of groups…. DIF said they would do protocols(?).... Now there's the European ones…. Ah! And we can't seem to work together. On an individual perspective… On logistics… I hang out with the supply chain folks, because I'm interested in supply chain tracking stuff, and have done research… no wonder the community is confused… Then there's IETF… and ISO - mobile driver license. Ah! What I've learned in my time as a co-chair is that there will be drama… that's just part-and-parcel with it, because of business… Honestly I don't understand what ToIP does… I'm super fine with collaborative stuff… I've invited… I just don't know what the solution is… My role is … I limit my hour engagement…. Another thing is that organizations don't want to fund this connector work…. But they will fund a startup that's going to go bust in 2 years… I'd love to be part of the solution… I'm a co-chair at W3C CCG now, not forever… for some very specific things.

Judith: I'm sorry, I was just about to tell you to watch the recording that says where ToIP fits in, but for some reason it wasn't recording… Maybe I will do it a second time… Let's see how good I did explaining it… Can someone on the call repeat what I said on where ToIP fits in with regards to all these organizations?

Timothy: Is there a document with links?
… Question about provenance… What people do in the artificial world of companies… legal groups of people… corporation as a group of persons… global(?) infrastructure… made by mankind… a whole bunch of people who work on things for different reasons - not all necessarily paid… Open standards… How does ToIP support provenance? History of this work... With standards bodies… patent protection…. Intellectual property… permission to use others' prior art… The combination of those two things… what's the position of ToIP… what are the issues?

Judith: I don't know if this really answers your question, but going back to this slide about the organizational structure of ToIP… It's a JDF project… You sign membership agreements… You can join as a collaborator for free… but you still have to join the ToIP Foundation…. By joining it, you are then signing the legal documents with regards to IPR. Everything done at ToIP currently picked Apache(2.0)? And Creative Commons 4.0... So you are working in an open standards, open software environment… The other piece is that you are not just giving things away, it protects you… Anything you contribute… who picks it up is picking it up at their own risk… They can't come back to you and say this piece of software doesn't work and sue you… This is part of why ToIP went to the Linux Foundation / JDF… It provides the legal structure for the foundation… You can join for free, sign the member agreement…

Timothy: In the literature about the history of verifiable claims, I've just posted about the history that predates the IIW of 2020, so people can evaluate ToIP as a trustworthy infrastructure…. Rule of law… How is the provenance of what you are bringing together… Integrity?

Judith: I don't think we've had a chance to read those links yet…

Phil: You're right, Timothy, whatever tech you lay out someone will say "I did it before you".... That's the space we're in… Tim Lee Barnes has been held up in court… all the time… The number of people who think they invented the internet, you would not believe. There are patents on the most numskull stuff you would not believe…. What any SDO has to navigate… Judith is right to highlight… Usually you have a separate IPR agreement for each WG… But when you join you are subject to some rules… It's designed so that at the end the standard is the best possible - either IP-free, or specific terms you want. People outside the group have no control of that.
… That's not saying anything about GS1…

Zoom Chat:
I'm in https://www.visitportdouglasdaintree.com/ Australia ;)
Drummond Reed To Everyone
10:56:08 AM There's going to be a session on the Future of Governance today that will cover the Cheqd governance framework
Jeff O To Everyone
11:04:38 AM Opportunity to Assist: The Human Experience Workshop @ ToIP
Judith Fleenor (Trust Over IP) To Everyone
11:07:00 AM https://trustoverip.org/get-involved/membership/
Drummond Reed To Everyone
11:17:19 AM You need to be here Phil!!
Heather Vescent To Everyone

11:17:21 AM Hah! Same! There are too many groups.
Phil Archer (GS1 Global) To Everyone
11:20:15 AM ?? I've only heard respect, heather
Heather Vescent To Everyone
11:23:49 AM Judith, IDK, maybe we can have you also present at the CCG sometime.
Me To Everyone
11:24:41 AM Phil Archer (GS1 Global) To Everyone
11:32:37 AMhttps://www.gs1.org/docs/Digital-Link/HowAndWhy_GS1_Digital_Link.pdf

TCH Links
One of my old links: Sep 2014
https://docs.google.com/drawings/d/1oUsSlPEh8erOdkQJCLzFHBaqp7AYOJCqDw82YrCg9f4/edit

May/June 2015:
https://docs.google.com/document/d/1pRtTu9EssjhyyK3qkQymZepIUkqCwvMo6imnr4fqsrg/edit

Jan 2016: https://docs.google.com/document/d/1pzZJ-pb-luy0jNryY2lrfJUNntjDGNm4-2wXKt72C6k/edit
Some of Manu's Old Credentials Docs Links
AUG 2014: https://docs.google.com/drawings/d/17mfHu4EqsnZQ2eFI115qC8FUuLOX-ZSnWpCjo7q1Vlc/edit
October 2015: https://docs.google.com/presentation/d/1644G7jJZbUTpyEGALWj6t4m5kJc-bt90QCfRmW5IRuk/edit#slide=id.p
https://docs.google.com/presentation/d/1ithW3t-ahelw_0jsAbVmhXi5NyRl_-BAW6hMnJmoixc/edit#slide=id.p
March 2016:
https://docs.google.com/document/d/1dYup3KC2nak3LVTzyapr996TKxDj1w5Eyp4g13rQQBA/edit
June 2016: https://docs.google.com/presentation/d/1mL0MsPpdxdKiYFWVIyGVOFzypBsjylxepACN2MYw-yg/edit
Sep 2016:
https://docs.google.com/presentation/d/1pFGC1G7CbizUuvbmjECfnNRL4fZk9QLxG8d3nehgwNU/edit
OCT 2016 IIW (IIW 23)
https://docs.google.com/presentation/d/1pY6TGsCBzmui_KVM5Q71t1LbHgdv10vRPov7SoISjqU/edit
https://docs.google.com/presentation/d/1BsGY6YOlkfTQQyxm0jJadxBhJwBCE3QLDoyRENzhS0k/edit
April 2017:
https://docs.google.com/presentation/d/13ztihmZSl7nIBW2TuJxgkNmwFcOjOFvxSDAQ0ACiyYg/edit
Nov 2017:
https://docs.google.com/presentation/d/1woq0pZD872NvhBIu90GIZMf8MQLWCtXM1NCx8n6s0VM/edit

Bridging Digital and Physical to Make Identifiers Identify (a terrible gab in web standards…)

Wednesday 11A
Convener: Liam McCarty (Unum ID)
Notes-taker(s): David Chadwick (additional info)

Tags for the session - technology discussed/ideas considered: identifiers, keys, W3C, WebAuthn, WebCrypto, DIDs, wallets, VCs

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

SESSION INFO:
tl;dr:
Do identifiers identify? Only if they're *associated* with a person or thing consistently over time. For human identity, this is easy with a mobile app but impossible with a web app, due to a terrible gap in web standards. We need community action to advocate for general, hardware backed cryptographic signatures on the web! This would make it possible to build decentralized identity wallet web apps, not just mobile ones, dramatically improving the odds of adoption.

Short Summary:
Decentralized identity efforts have typically relied on mobile app wallets, since mobile operating systems offer crucial functionality, especially hardware backed cryptography and device biometrics. But mobile app wallets face enormous barriers to adoption because people are unlikely to install new apps they don't yet know the value of. Mobile SDKs only partly address this problem because they must be embedded in host apps that many people may not yet have installed, and they must work largely behind the scenes, complicating the "sovereignty" of users over their identities.

Imagine if a web app could do the cryptography and biometrics a mobile app can. This would enable web app wallets, which have almost zero barriers to adoption, as users can access them from a URL rather than through an installation process. The result would be a dramatic increase in the usability of decentralized identity tech and therefore the odds of its adoption.

The problem is, current web standards don't support what's necessary! WebCrypto enables general cryptographic signatures but not tied to device hardware. WebAuthn enables hardware backed cryptographic signatures but only for the very narrow use case of authentication. I've made proposals to each of these groups to effectively combine the two functionalities to achieve general, hardware backed cryptographic signatures on the web, but each group is in a bind. WebCrypto committed awhile back not to focus on hardware, and WebAuthn in its very name has a mandate only for authentication.

So, at this point, we need to rally the community to support expansion/combination of these specs! It would be a true game changer for decentralized identity tech.

Additional material
Verifiable Credentials Ltd has integrated WebAuthn (FIDO2) with the Verifiable Credentials Data Model to provide the bridge this talk is looking for. A presentation about this is available here
https://verifiablecredentials.info/presentations
And a description of our first prototype (based on FIDO UAF) is published here

David W Chadwick, Romain Laborde, Arnaud Oglaza, Remi Venant, Samer Wazan, Manreet Nijjar "Improved Identity Management with Verifiable Credentials and FIDO". IEEE Communications Standards Magazine. Vol 3, Issue 4, Dec 2019, Pages 14-20

Links:
My presentation to the DIF Identifiers & Discovery WG on this topics (September 13): https://github.com/decentralized-identity/identifiers-discovery/blob/main/agenda.md#meeting---13-september-2021---1400-et-recording
WebAuthn W3C spec: https://www.w3.org/TR/webauthn-2/
WebCrypto W3C spec: https://www.w3.org/TR/WebCryptoAPI/
My proposal on WebAuthn GitHub issues: https://github.com/w3c/webauthn/issues/1608
My proposal on WebCrypto GitHub issues: https://github.com/w3c/webcrypto/issues/263
(Abandoned) Hardware Based Secure Services W3C group: https://www.w3.org/community/hb-secure-services/
(Abandoned) Hardware Based Secure Services W3C spec: https://rawgit.com/w3c/websec/gh-pages/hbss.html

Session Slides:
https://drive.google.com/file/d/1o7VuanEdJqnqVZGvzfgHmGp1eO17ETWd/view?usp=sharing

Is the Smart Home a Dictatorship, Co-op or Homesteading?

Wednesday 11C
Convener: Chris Butler - LinkedIn, Twitter
Notes-taker(s): Chris Butler

Tags for the session - technology discussed/ideas considered:

Identity, pseudo-identity, communal computing, IoT, smart homes

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

Session Slides:
https://docs.google.com/presentation/d/e/2PACX-1vQrfwD6AOisVpNmMlHAy-4ysCkp7UTEFcmGAdjQIu359yF4Y-TepHbtCVJVElQDUFKFL1enETkdbQ92/pub?start=false&loop=false&delayms=3000

Background materials:

- Articles
  - Communal Computing
  - Communal Computing's Many Problems
  - A Way Forward with Communal Computing

- Other talks:
    - AIxDesign Communal Computing workshop with animistic design mapping
    - Solving multi-user Alexa and Google Assistant use cases

ZOOM Chat Log:

Jeff O: Great graphical explainers Chris!
Jeff O: Thx Tim!
fundthmcalculus: Chris, will you post the slide deck, especially the trust relationships venn diagram?
Timothy Holborn: 2016: https://docs.google.com/presentation/d/1ud8Jm4oHvR-YFIylqPoPJgv9TljQCydiR9HXAHrHwTs/edit
Chris Butler: https://miro.com/app/board/o9J_lqh1FGs=/
Jeff O: Wonder if homesteading may = "in touch"
Timothy Holborn: https://www.w3.org/WoT/
fundthmcalculus: @Chris, since we're talking governance:
Dictatorship, Democracy, and Colony?
Timothy Holborn: https://www.hbbtv.org/wp-content/uploads/2020/10/HbbTV-SPEC-00525-HbbTV-SPEC-00515-008-hbbtv203_2020_10_14.pdf
Jeff O: The phrase "Public Privacy" come to mind and was brought up @ IIW a few years ago - per Justin R\
Timothy Holborn: (linked to the HbbTV spec above) https://github.com/MPAT-eu/MPAT-core
Jeff O: The kitchen being a public space w/aspects of delegated (maybe privacy based), parents get the re=supply info as well as the what's to eat, but the kids may just get the what's to eat. To Alan's point I think.
Jeff O: "....delegated info... re:above
Jeff O: Re: Zones in a home, etc. People (consumers in particular) often don't understand bandwidth loads and QoS prioritization concepts. A PC one foot from a ethernet connection does not need to lean on WiFi. So much low fruit that is foundational.
Jeff O: "Why is my WiFii slow?" Everyone streaming Netflix after school, Sonos everywhere, updating in the background. Becomes "mayhemic" at a point in my experience.
johannes: Alan: where would you manage those permissions?
Jeff O: Set any expiry time?
Jeff O: Don't want to get that expiry wrong, eh!? :(
George Fletcher: OAuth supports explicitly revokable tokens
Alan Karp: Didn't use to, right?
Jeff O: Ever driven away from your FOB? I have : ((((((Lesson: Never turn off your car to avoid this problem. We blew it...
George Fletcher: The /revocation endpoint has been valid for many years... but it was added after 6749 and 6750
Alan Karp: Clearly I haven't been keeping up.
Fundthmcalculus: pro tip: get a car with a physical key, can't lose it. Also, most have a feature where they flash a "key not detected" error.
Timothy Holborn: Thankyou all.
Joyce Searls: Picos help with things having their own identity.
Jeff O: @fund: tru dat. we heard the alarm beep upon reviewing our circumstance. My daughter even said...gulp, "It said Key not in range" and didn't share that out. I heard too on replay but it didn't jostle me as it was so unfamiliar an alert... Physical hide-a-key - YES!
fundthmcalculus: That's a software defined network.
Jeff O: modular repurposing
Jeff O: like an ISP modem on a new circuit

windley: http://worrydream.com/refs/Smith%20-%20Croquet%20-%20A%20Collaboration%20System%20Architecture.pdf
windley: That's Reed's paper on Croquet
Alan Karp: We worked with the Croquet team while they were at HP Labs.
fundthmcalculus: Lamp says: I'm sorry Chris, I can't do that.
Joyce Searls: Gotta leave. Thanks so much.
windley: Yeah @alan, the Acknowledgements mentions HP.
Jeff O: Can you drive away from your home's FOB?!

Controlling Your Medical Data via DIDComm - discussion and feedback on our system architecture

Wednesday 11E
Convener: Elias Strehle (elias@circulartree.com)
Notes-taker(s): Elias Strehle

Tags for the session - technology discussed/ideas considered: DIDComm, Hyperledger Aries, Hyperledger Indy, Medical Data

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

Link to the slide deck

Some edge cases to think of when considering patient control over medical data:

- Some psychiatric patients are not allowed to see their own diagnosis
- Some infectious diseases MUST be reported to public health authorities, even against the patient's will
- Physicians might want/need to see medical data that the patient is unwilling to share

We want to send files (possibly images or even videos) across DIDComm. Does that make sense?

- It's already possible to send attachments via DIDComm
- Becomes impractical for large files on phones, unsurprisingly
- Possible alternative: Just pass File URL + Access token + Hash via DIDComm

Interoperability:

- How to make sure the recipient understands what they get and gets what they expect?
- This is very hard, medical data is extremely diverse and there are a lot of competing standards
- Our project does not have a great answer to this yet, but we hope to get communication out of the way quickly so we can work on (semantic) interoperability as soon as possible

Do we use VCs?

- Currently not, authentication relies on personal contact during peer-to-peer registration
- It is already clear, though, that this is not feasible or trustworthy enough for all use cases
- VCs for authentication will have to become part of the solution
- VCs for file hashes might also be interesting to establish trust on data
- The Hashlink standard might be useful for this
- Is Hashlink already part of DIDComm? So far only as attribute of a credential

Idea: One advantage of the system is that you can discover the medical data that exists via DIDComm:

- Connecting with medical provider and then seeing a list of available data is a great alternative to filling out annoying paper forms
- A search functionality would be really cool ("Does anyone have an x-ray of my arm?")
- But as soon as we need semantic interoperability this gets extremely complex

As a patient, how can I trust the medical provider?

- Malicious software/faked QR codes could be a problem
- This is where VCs come in from an identity perspective

Have you tried embedded versions for medical devices?

- No, the project hasn't explored that
- Can we make pacemakers communicate directly with physicians instead of manufacturers? How would we integrate that use case?
- Very complex as there are a lot of different devices and many of them have strong constraints on computation/memory/storage/availability

Use case to consider: How can emergency responders get access to critical medical data?

From a medical provider's perspective: Who should have the DID - the institution or its employees?

- Both are possible, depends on strength of relationship (e.g., employee DID might make a lot of sense for psychotherapist) and use case requirements
- Legal framework and requirements likely vary a lot from country to country

Who in the system should have a public DID?

- Usually unproblematic for institutions, i.e., medical providers
- Peer DIDs for private persons can make a lot of sense
- Indeed, it would be very problematic to have a "super-ID" for a patient, this might not be GDPR compliant
- However, this makes it harder to link VCs for authentication (subject binding)
- "Subject binding"
- If a patient's phone is stolen, using peer DIDs only would still allow them to block access to medical data from that phone: This requires a secure backup to cancel the keys on the stolen device

What are potential business models for mediators/ledger operators?

- No big amount of trust towards mediators required, they see only encrypted data
- Often, the app provider could also provides the mediator
- Mediators for medical institutions or practitioners could probably cost money, or might be provided by professional associations/schools/government
- Note: There are open source standards for the relationship between mobile app and mediator, but it's also possible to do something on your own without losing interoperability with the rest of the system

GoDiddy.com - Create, Resolve, Search DIDs

Wednesday 11F

Convener: Markus Sabadello
Notes-taker(s): Trent Larson

Tags for the session - technology discussed/ideas considered: DID, DID Resolution, DID Doc, tool, UI

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

Showed godiddy.com
- To Resolve DIDs, enter one or choose from examples with the button on the right.
- To Create or Search, log in by entering email and you'll get an API key & login link.

docs.godiddy.com - Includes examples for the API.

api.godiddy.com

Resolve
- Can return only the DID doc vs all doc & metadata
- Can return in different formats, eg CBOR
- Can return selections of the DID doc if you use a # fragment
- Can use query parameters, eg transformKeys, eg from Ed25519VerificationKey2018 to JsonWebKey2020 or jwks

Search
- Note that the front page shows most-recently-created DIDs on multiple networks.
- Allows searching by substrings of DIDs or values in a path

"Authentic" Auditing & L:ogging - Microledger lite?

Wednesday 11G
Convener: Neil Thomson, QueryVision
Notes-taker(s): Neil Thomson

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

Slides - link to the slides presented in the session

Concern that upgrading existing text streaming logging or auditing implies additional overhead (which may be perceived as not adding value).

Response: Processing and bandwidth are constantly increasing. Key is pushing processing of raw data capture to the edge. Bias towards fast, secure, authentic raw data capture. Push processing overhead into extraction and use of the captured data.

There was an interest in data

The Future of Governance

Wednesday 11J
Convener: Alex Tweeddale, Drummond Reed, Nicky Hickman
Notes-taker(s): Ross Power, Chris Matichuk

Tags for the session - technology discussed/ideas considered:

1. What is machine readable governance? Is this desirable or does it run counter to flexible and agile governance? Discussion about how YOMA has developed a lean governance model to be maximally flexible

2. Do we need centralised governance authorities? Or is there a better way of managing decisions in a more decentralised way. How does cheqd decentralise governance?

3. What are lessons we have learnt from our time in governance, and where do we see the future going?

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

Aspects of governance

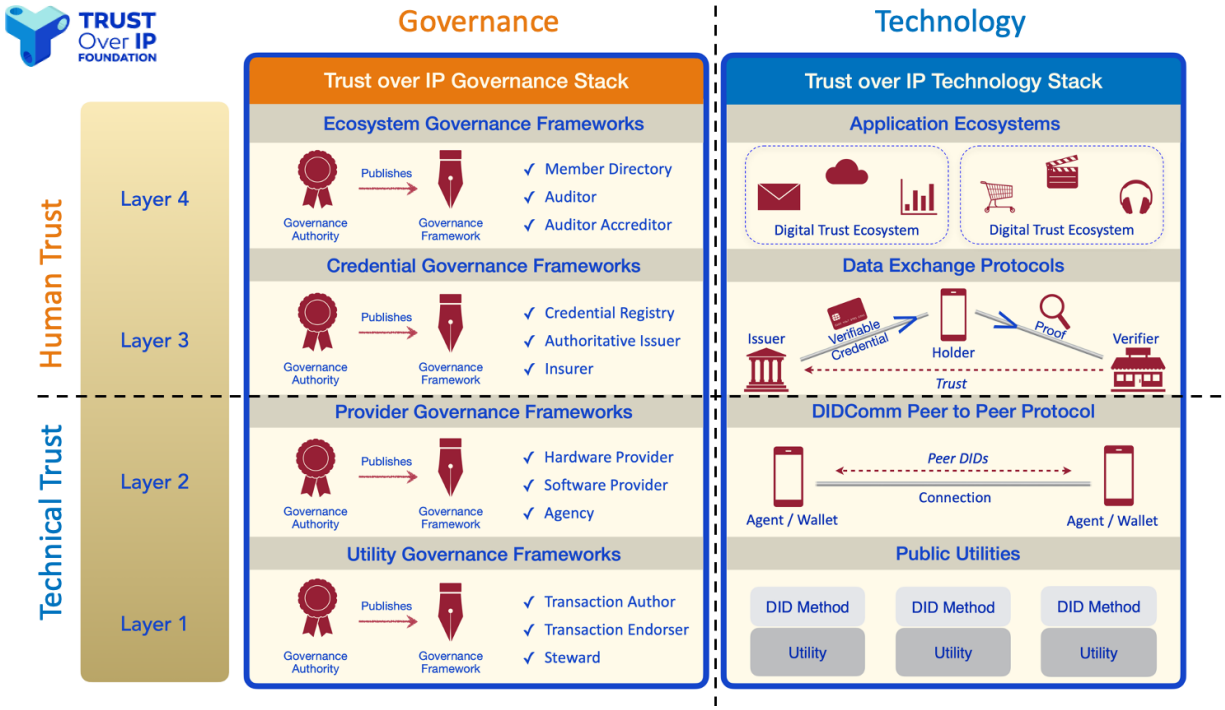
- Laws - enforced by the use of force
    - Speed limits
- Norms - enforced by social otriaton
    - Don't sing on the elevator
- Structures - fundamental limitations
    - Wall and gate, far easter to go through the open gate then the wall.

Links shared in chat:

- https://wiki.trustoverip.org/display/HOME/ToIP+Trust+Registry+Protocol+Specification
- https://wiki.trustoverip.org/display/HOME/ToIP+Governance+Metamodel+Specification
- Yoma Rules
    - https://docs.google.com/document/d/1UGUq6wuTrJH-TCkL7Fzw8cHqcFXMoQwK/edit
    - https://docs.google.com/presentation/d/1aaPvAlgJUnAzxhN8e3-7sb_3K1gdRyU5/edit#slide=id.p1
- Micro board - https://miro.com/app/board/o9J_lGpCxU0=/?invite_link_id=532208146676
- Frameworks for ethical decision-making:
    - Brown https://www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions
    - Markkula Center for Applied Ethics https://www.scu.edu/ethics/ethics-resources/ethical-decision-making//
- Trust Registries - https://docs.google.com/document/d/1ZGXUB0oODHO66PQkO66-fbAu6f7sVVToOz3Q8RNG0fs/edit#heading=h.z9eu4otrys70
- ACDC task force - https://wiki.trustoverip.org/display/HOME/ACDC+%28Authentic+Chained+Data+Container%29+Task+Force
- Cheqd governance work - https://docs.cheqd.io/governance/principles/foundational-principles
- Here are some other governance tokens and blockchains that use tokens for governance voting, for comparison
    - https://cryptotop10.org/top-10-governance-tokens/

- Polkadot: https://wiki.polkadot.network/docs/learn-governance
- http://humanfirst.tech/

A picture of how governance frameworks fit at each of the four layers of the ToIP stack:



ZOOM CHAT DOWNLOAD

18:06:02 From Scott David to Everyone:
The King of Governance!
18:06:02 From Aaron Goldman to Everyone:
King?
18:06:34 From Scott David to Everyone:
The governance of Kings?
18:07:26 From Aaron Goldman to Everyone:
How to add Filibuster to your distributed system 🤔
18:07:31 From Scott David to Everyone:
Layers allow structured externalities for governance.
18:07:34 From Bart Suichies to Everyone:
Good morning Dennis jr :)
18:07:35 From TimoGlastra to NickyHickman(Direct Message):
Hey Nicky, I work with DIDx on the technical stack of the Yoma project. Didn't knew you worked on the YOMA project. Very cool :)
18:08:02 From NickyHickman to TimoGlastra(Direct Message):
likewise - would love to connect 1:1
18:08:07 From Dennis Mittmann to Everyone:
good evening it is ^^
18:08:48 From TimoGlastra to NickyHickman(Direct Message):
Great! I'll reach out to you on Linkedin to meet up after IIW. Look forward to it

18:08:55 From Kent Bull to Everyone:
How do I create or extend a governance framework for my given use case such as with the Trusted Registry idea from Trinsic? I want to set apart a set of issuers for a given credential type as the governing body for that credential type. What is a good way to do so?
18:09:15 From Scott David to Everyone:
Governance is the attribute of any system that has rulemaking, operation under the rules and enforcement of the rules (legislative, executive and judicial functions in the nation state constitution context). Can have "own" versions of all three in house, and./or can normatively cross reference any one of the three.
18:09:33 From TimoGlastra to NickyHickman(Direct Message):
Or we can meet up in the unsession hour. Let me know what works best for you
18:10:05 From Joe Hsy to Everyone:
@Drummond, great to see you again. Do you know of any governance work in the online fraud prevention area, especially in standards for verified credentials?
18:10:05 From windley to Everyone:
+1 Scott
18:10:26 From Drummond Reed to Everyone:
@kent Check out the ToIP Trust Registry Protocol Specification: https://wiki.trustoverip.org/display/HOME/ToIP+Trust+Registry+Protocol+Specification
18:10:50 From Scott David to Everyone:
Governance systems are "constituted" (hence 'constitutions') via arrangements that constrain the new governance thing so constituted. That encourages the self-binding of the components to the thing so constituted. (Compare US federal system, compare standards setting, etc.)
18:11:06 From Drummond Reed to Everyone:
For folks wondering what the "ToIP Governance Metamodel" is: https://wiki.trustoverip.org/display/HOME/ToIP+Governance+Metamodel+Specification
18:11:36 From Scott David to Everyone:
Syntheses of aspirations and needs of stakeholders as starting point. Beautiful indeed.
18:12:51 From Simon Nazarenko to Everyone:
is this doc publicly available?
18:15:14 From Scott David to Everyone:
Can start with existing practices in existing community as raw material for new governance (compare Christopher Alexander in architecture), with risk of perpetuating biases of earlier governance. In the alternative, can start with "anomalies" and harms that threaten vulnerable and precarious populations under existing governance regimes, under the idea that the anomalies and suffering are the ways that a system "speaks" to its stakeholders about its edges and inadequacies.
18:15:35 From Scott David to Everyone:
Risk based is great. Not need beneficence for adoption. Based on self interest of de-risking.
18:17:09 From Drummond Reed to Everyone:
I'd like to bring up a particular governance topic that has become quite relevant for COVID-19 credentials: trust registries.
18:17:19 From Scott David to Everyone:
Embodiment of affordances of prior decisions into code (and also material culture, language, etc.) is source of lag AND measurable reliability. Expectations are bound up in system performance, implicit and explicit.
18:17:38 From NickyHickman to Everyone:
Yoma Rules - is in a review cycle - you are all welcome to review https://docs.google.com/document/d/1UGUq6wuTrJH-TCkL7Fzw8cHqcFXMoQwK/edit?usp=sharing&ouid=103576046431467753337&rtpof=true&sd=true

18:17:59 From NickyHickman to Everyone:
Miro board https://miro.com/app/board/o9J_lGpCxU0=/?invite_link_id=532208146676
18:19:14 From Shannon Wells to Everyone:
https://www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions
18:19:33 From Darrell O'Donnell to Everyone:
“machine readable governance” - great concept, dangerous to take too far - not that much is truly “machine readable”
18:19:47 From Judith Fleenor(Trust Over IP) to NickyHickman(Direct Message):
I told Shannon about the HXWG, you might want to reach out an personally invite her… I think she would be interested it HXWG
18:19:55 From Darrell O'Donnell to Everyone:
+1 Shannon
18:19:57 From NickyHickman to Everyone:
yes @scott - in the lean governance method, metrics are embedded in the process - look at the miro board top piece on lean governance
18:20:01 From Mike Ebert to Everyone:
I won't hijack this session, but we definitely have some cool things to talk about when it comes to machine readable governance and how it can help without crippling the ethics or the humans.
18:20:33 From Scott David to Everyone:
Yoma looks great. Compare nice article by Porter and Ronit called the “5 stages of private rulemaking” (or something like that). The review phase creates a feedback loop helping to sculpt governance for a given situation (compare product localization, compare theatrical adaptation, etc.)
18:20:54 From Alex Tweeddale to Everyone:
Would love it if you could give an overview after the raised hangs
18:20:56 From Darrell O'Donnell to Everyone:
@Mike - I am hoping I can make it to your session. Looking forward to hearing about what you have.
18:20:57 From Alex Tweeddale to Everyone:
hands*
18:21:15 From Alex Tweeddale to Everyone:
And then you can plug your session :D
18:21:30 From Shannon Wells to Everyone:
The ethical framework can also help with making decisions about how to write the machine governance. E.g. you could conceivably figure out a way to detect dilemmas and halt a process until human input is added (just a last minute thought)
18:21:44 From ChrisKelly to Everyone:
+1
18:21:49 From Mike Ebert to Everyone:
Ok, I'd be happy to chat a little about what we'll present.
18:21:51 From Darrell O'Donnell to Everyone:
@Shannon - agreed
18:21:58 From ChrisKelly to Everyone:
human oversight, appeals and review process is important
18:22:01 From Alex Tweeddale to Everyone:
Absolutely Shannon!
18:22:01 From NickyHickman to Everyone:
+1 @Darrell - important to consider dangers of MRG human readable and machine readable need to work together
18:22:36 From Kerri Lemoie to Everyone:

Can someone please share the link to this doc again?
18:22:40 From Scott David to Everyone:
+1 to Shannon. Brown article notes Santa Clara work on ethics which nicely emphasizes “processes” of ethics. Perhaps governance is best viewed as a “process” not a destination?
18:22:40 From Darrell O'Donnell to Everyone:
One of my favourite sayings from some very savvy governance and policy people was “sometimes, friction is a feature”
18:22:45 From @PrivacyCDN to Everyone:
How do you address possible issues of “Tech saviourism” so that structural inequities are addressed proactively?
18:22:46 From Marc Davis to Everyone:
+1 @Shannon
18:23:07 From Aaron Goldman to Everyone:
You may want to put links in the notes doc https://docs.google.com/document/d/1fVcnLZJW-SeDWLgKuJAXbbdlCCD0-6qDUOJL40dkl0Y/edit
18:23:10 From Shannon Wells to Everyone:
We are working with the Markkula Center for Applied Ethics and Georgetown U
18:23:16 From Darrell O'Donnell to Everyone:
@PrivacyCDN - especially when a system has been running for a while with embedded flaws/bias.
18:23:18 From NickyHickman to Everyone:
crucial question @PrivacyCDN -
18:23:20 From Shannon Wells to Everyone:
@Aaron will do
18:23:26 From @PrivacyCDN to Everyone:
By definition, for example, international travel is for the privileged.
18:23:38 From NickyHickman to Everyone:
I am studying ethics this quarter - looking for answers
18:23:51 From NickyHickman to Everyone:
We should treat MRG the same way as AI
18:23:53 From Darrell O'Donnell to Everyone:
@Nicky - I think that work drives more questions than find answers.
18:23:59 From Chris Matichuk to Everyone:
Is the BC Gov orgbook a type of trust registry?
18:24:19 From NickyHickman to Everyone:
finding the right questions is the start of a brilliant solution
18:24:19 From Scott David to Everyone:
Big clarification: Parse concepts of “ethics” from those of “equity” - Lots of additional solutions space opens up.
18:24:20 From Darrell O'Donnell to Everyone:
@Chris - yes, it lists bona fide corporations
18:24:22 From @PrivacyCDN to Everyone:
@NickyHartman see IEEE P7000 series of standards and the IEEE ethics in design documents
18:24:33 From Mike Ebert to Everyone:
We have a demo that is slightly different for the same use case.
18:24:38 From Kevin Griffin1 to Everyone:
I’m seeing trust registry is that synonymous with verifiable data registry?
18:24:58 From @PrivacyCDN to Everyone:
+1 @ScottDavid on parsing
18:24:59 From Chris Matichuk to Everyone:

Might be interesting to list out all the existing trust registries and the scope of each.
18:25:03 From Kevin Griffin1 to Everyone:
Or would a vdr be an implementation of a trust registry
18:25:10 From Darrell O'Donnell to Everyone:
@kevin - sort of - but not as a replacement of a ledger/chain/database - it's a list of things you need to answer trust decisions
18:25:20 From Kevin Griffin1 to Everyone:
thanks
18:25:27 From Mike Ebert to Everyone:
For example, our demo will work without needing to query the trust registry with every issuance/verification
18:25:53 From NickyHickman to Everyone:
yes we need both of these and also a requirement for MRG
18:26:06 From Chris Matichuk to Everyone:
The issue of trust registry has come up a few times in the DIACC.ca discussions.
18:26:23 From Darrell O'Donnell to Everyone:
@Kevin - yes - a list of Issuers that are considered authoritative would be a good example
18:26:24 From Fraser Edwards to Everyone:
Got to drop, awesome session Alex, Nicky & Drummond
18:26:45 From Scott David to Everyone:
Technically "equity" under law is the correction of rules of general application (from rule of law)(check Aristotle)). Ethics is normative in a different way. Note that trolly car problem has different answers in different cultures. Equity is different - it is a process of correcting general rules at the edges. Precarious populations are typically under measured and under-served at the edges of bell curves. Equity processes can help governance to pause and correct. Technical requirements are the new "rules of law" that need "adjustment" at the edges.
18:27:18 From @PrivacyCDN to Everyone:
Also need to be clear on parsing 'choice', 'forcing', and 'coerce'. You may not be forced to an action (i.e. gun to head) but social circumstances can add up to coercion. Coercion is a big issue in medical research ethics for example.
18:27:21 From Drummond Reed to Everyone:
ToIP Trust Registry Protocol Specification:
https://docs.google.com/document/d/1ZGXUB0oODHO66PQkO66-fbAu6f7sVVToOz3Q8RNG0fs/edit?usp=sharing
18:27:31 From Scott David to Everyone:
Great discussion folks. I need to drop. See you all in a later session.
18:27:39 From Drummond Reed to Everyone:
Thanks Scott!
18:27:48 From Todd Gehrke1 to Everyone:
+1 on not decentralizing everything
18:27:56 From NickyHickman to Everyone:
Also could trust registries be a transitional Web 2.0 - Web 3.0 staging post
18:27:59 From NickyHickman to Everyone:
??
18:28:25 From windley to Everyone:
Wrote a bit about decentralizing centralized things this week:
https://www.windley.com/archives/2021/10/nfts_verifiable_credentials_and_picos.shtml
18:29:48 From John Court to Everyone:

An issuer should never have control over what verifiers can see their credentials….that seems to be a complete perversion of SSI and the Holders Sovereignty !
18:30:15 From James Ebert to Everyone:
+1 Ad Hoc interactions are important to ensure we keep in mind when building out governance frameworks
18:30:17 From Darrell O'Donnell to Everyone:
@John - it is the governance authority that MAY want to limit authorized verifiers
18:30:22 From Darrell O'Donnell to Everyone:
Not the Issuers per se.
18:30:31 From Drummond Reed to Everyone:
@John Court: totally agree
18:30:36 From Paul Bastian to Everyone:
John, that could also be very indirect, e.g. you must be in the trust registry to query that crednetial
18:30:47 From Paul Bastian to Everyone:
but it gets dangerous
18:31:24 From Alex Tweeddale to Everyone:
Do people think KERI and ACDC could provide the answer to the centralised trust registry question?
18:31:28 From NickyHickman to Everyone:
For those that want a deeper dive on Yoma Rules! and Lean Governance here is a link to a presentation we gave to the DIF Africa Group, I think a recording of that meeting is also available from DIF
https://docs.google.com/presentation/d/1aaPvAlgJUnAzxhN8e3-7sb_3K1gdRyU5/edit?usp=sharing&ouid=103576046431467753337&rtpof=true&sd=true
18:31:28 From Darrell O'Donnell to Everyone:
Trivial example - a liquor establishment accessing a driver license for age of majority - where that is considered “normal and privacy respecting” but if they asked for ALL of the data in my driver license, it would be odd.
18:31:43 From Margo Johnson1 to Everyone:
When is a Trust Registry the right tool for the job, versus more ad-hoc presentation of authorizing information (i.e. My business is accredited by (trusted party) - here is a VC that proves that) where governance may be managed today in other ways not using this tech. Are we over-reaching here given the maturity of this tech relative to existing governance structures? (playing devils advocate a bit :))
18:31:53 From Shannon Wells to Everyone:
It’s a milieu-based framework - what is the milieu? the culture, the nation-state, the neighborhood, the city, the subculture? that tells you what the needs are. De-centralization will not always serve the needs of that environment. Looking at a problem with a dogmatic attachment to a specific technical solution will result in a failure to meet needs, IMO
18:31:56 From John Court to Everyone:
Ok I can see certain verifiers being blackballed, not sure how that would be enforced other than the mentioned Verifiers credentials being checked by the holder …. Always beleived holders would also have to effectively be verifiers of businesses
18:32:22 From Darrell O'Donnell to Everyone:
@Margot - great Q - classic, useless answer - “it depends”
18:32:40 From @PrivacyCDN to Everyone:
Non-trivial example from Canada: Who issues a credential that verifies that an individual is a member of a First Nation?
18:32:45 From Darrell O'Donnell to Everyone:
@Margot - I’ll add than in many real world scenarios we already know the rough rules of the road.
18:33:01 From Drummond Reed to Everyone:

@Margot - I was going to say the same thing. I'll get on the queue to talk about ACDC (Authentic Chained Data Container) credentials.
18:33:12 From Drummond Reed to Everyone:
https://wiki.trustoverip.org/display/HOME/ACDC+%28Authentic+Chained+Data+Container%29+Task+Force
18:33:29 From Chris Matichuk to Everyone:
Anyone with notes...remember to add to the session notes:
https://docs.google.com/document/d/1fVcnLZJW-SeDWLgKuJAXbbdlCCD0-6qDUOJL40dkl0Y/edit
18:33:44 From Drummond Reed to Everyone:
Thanks for the reminder Chris!
18:34:21 From @PrivacyCDN to Everyone:
About 15 years ago there was a paper that showed that trustmarks on websites increased the likelihood that the site hosted malware because of the ease by which websites could get a particular trustmark.
18:34:44 From Shannon Wells to Everyone:
Fact
18:34:44 From Marc Davis to Everyone:
Transitive trust is the foundation of society.
18:34:48 From NickyHickman to Everyone:
We will ask the students to transcribe and summarise for us!
18:34:52 From windley to Everyone:
But there's not one. Right?
18:34:56 From Tim-from-IAMX to Everyone:
🐾 holder should neither depend on 1) issuer to convert to digital verifiable credential (takes too Long, Violation of SSI principle to be so slow) and not to depend on 2) White-listing. Why? The Verifier decides on which credential is accepted. The holder needs a [→] Gateway from real world to the chain, that he decides on, lowest barrier, highest convenience, alsmost no costs
18:34:57 From windley to Everyone:
*just one
18:35:03 From Darrell O'Donnell to Everyone:
Having an SSL cert used to mean something - that there was a real company behind the website - it is now useless for that trust decision and has devolved to "my comms are encrypted"
18:35:23 From windley to Everyone:
+1 Darrell
18:36:21 From John Court to Everyone:
+1 Darrell
18:37:09 From Paul Bastian to Everyone:
thats true for DV certs only
18:37:20 From NickyHickman to Everyone:
As everyone is talking I am thinking of some cool ways of applying the local-first principle AND having local trust registries for yoma ecosystems
18:37:26 From John Court to Everyone:
CA cert = DIDComm connection semantics, needs VCs to become trusted at human level
18:37:27 From Paul Bastian to Everyone:
EV certs and QWAC SSL certs verify the real organisation in the back
18:37:47 From windley to Everyone:
+1 John
18:38:26 From NickyHickman to Everyone:
thinking of how https://www.grassrootseconomics.org/ works with local currencies. Trust is the 'currency of social interaction'

18:38:42 From David Waite to Everyone:
Browsers don't surface that you use an EV cert anymore.
18:38:47 From David Waite to Everyone:
We used to think that all certificates were EV - no, the CAs just had processes that were really frustrating ;-)
18:38:48 From Darrell O'Donnell to Everyone:
@Paul - what percentage of folks know that to be the case? I'll argue very low.
18:38:52 From Paul Bastian to Everyone:
no but your SSI Wallet could
18:38:53 From Marc Davis to Everyone:
+1 John
18:39:14 From Darrell O'Donnell to Everyone:
@paul - and my browser used to...
18:39:19 From Paul Bastian to Everyone:
the mechanisms exist to enable strong trusted Verifiers with given TLS infrastructure
18:39:35 From Darrell O'Donnell to Everyone:
agreed though - my Wallet and/or Agents will do this work for me.
18:39:45 From Darrell O'Donnell to Everyone:
And learn from your wallet/agents too
18:39:45 From Paul Bastian to Everyone:
Google tries to kill EV certificates though
18:40:07 From Charles Lanahan to Everyone:
what is an EV cert?
18:40:16 From Paul Bastian to Everyone:
but EU pushes QWAC which is the eIDAS-enabled equivalent to be mandatory for browsers
18:40:53 From Paul Bastian to Everyone:
https://en.wikipedia.org/wiki/Extended_Validation_Certificate
18:40:59 From Charles Lanahan to Everyone:
ahh thanks
18:41:45 From Paul Bastian to Everyone:
I'd love to make a session on it but I don't have the time for preparation :/
18:43:41 From Chris Matichuk to Everyone:
This is a great point...we don't need another Facebook controlling the rules for everything.
18:43:47 From John Court to Everyone:
Promising but you have to solve the fraudulent vote and 1 vote per REAL identity problem.
18:43:48 From NickyHickman to Everyone:
we have no governance authority in Yoma, just an administering authority
18:43:49 From Drummond Reed to Everyone:
+++1
18:44:09 From Drummond Reed to Everyone:
that's an innovation in itself, Nicky!
18:44:21 From Andy Morales to Everyone:
Why do we, since Web3 and blockchain came over , equate democracy = economy (i.e. token-motivated systems)
18:44:37 From Darrell O'Donnell to Everyone:
@nicky - "administering authority" sounds a lot like a body that governs?
18:44:46 From NickyHickman to Everyone:
it was a reflection of reality and the way the yoma community comes together
18:44:57 From windley to Everyone:

Yes, what are they administering?
18:44:58 From NickyHickman to Everyone:
It has no governance control
18:45:06 From NickyHickman to Everyone:
or rights
18:45:28 From NickyHickman to Everyone:
the processes for revising the GA
18:45:41 From windley to Everyone:
Who created the processes?
18:46:07 From NickyHickman to Everyone:
a ToIP TF based on the functionality and existing 'contracts'
18:46:22 From NickyHickman to Everyone:
there are many holes - e.g. no dispute resolution mechanism
18:46:57 From Darrell O'Donnell to Everyone:
perhaps “no formal and permanent governance authority” is a more correct phrase?
18:47:18 From Darrell O'Donnell to Everyone:
“we swarm when needed and let the system run otherwise”?
18:47:50 From NickyHickman to Everyone:
great description - looking forward to your feedback on Yoma Rules! :-)
18:48:10 From Kevin Griffin1 to Everyone:
@Alex with regard to could KERI and ACDC - can they provide one possible implementation fir trust registries - yes, I think they could, If by the usage of KERI you mean establishing a root of trust with an accompanying eco system governance framework, and the usage of ACDC to provide chained verifiable credentials (sorry for the slow response)
18:48:16 From Marc Davis to Everyone:
Is there a link for Alex’s deck about cheqd.io?
18:48:36 From Alex Tweeddale to Everyone:
https://docs.cheqd.io/governance/principles/foundational-principles
18:48:39 From Richard Esplin to Everyone:
> Why do we, since Web3 and blockchain came over , equate democracy = economy (i.e. token-motivated systems)
The token can align incentives between participants. Other governance models I've participated in have a division between those who prefer to talk about governance, and those who are actually building the network.
18:49:00 From Bryan Pon to Everyone:
+1 Andy ….. “Truly democratic” governance implies representative governance, but if you look at the socioeconomic and demographic composition of those with voting power in any of these networks, I think you’d be hard-pressed to argue that those making the decisions reflect any large-scale population.
18:49:29 From Shannon Wells to Everyone:
There is other Proof of Stake, token-based governance on other blockchains btw (to audience, I’m sure @Alex knows this already), for comparison, Polkadot is one.
18:49:54 From NickyHickman to Everyone:
Don't forget cheqd is layer 1 and an incentivised n/w so the pre-requisite is economic motivation
18:51:44 From Kaliya Identity Woman to Everyone:
How can you add another payments thing onto the already very hard problem of just getting VCs to interoperate.
18:52:28 From Shannon Wells to Everyone:
@Bryan PoS chains inevitably privilege wealth, the only way I know of around that is to form staking pools that represent interest groups.

18:52:45 From Shannon Wells to Everyone:
so the staking governance works more like a republic
18:54:23 From Rouven Heck to Everyone:
I think tokens are a great way to build governance systems, but I don't think it will be easy/possible to build a token that achieves the all objectives with the same token - stable payment solution, security of a network and non-network governance....
18:54:23 From Chris Matichuk to Everyone:
If the idea is staking for decentralized governance, would there be staking pools, and what about the risk of 1 big staking pool making it centralized?
18:54:53 From Bryan Pon to Everyone:
@shannon Agreed… if a network only impacts the population of wealthy, educated Global North technoptimists that are involved in staking etc, then great, we can say that governance might be representative or "democratic." But if it impacts other segments of the population….
18:54:54 From Shannon Wells to Everyone:
that's already happening. Tezos is utterly dominated by Binance staking.
18:55:26 From Rouven Heck to Everyone:
with high rewards on staking it's a centralization
18:55:40 From Richard Esplin to Everyone:
> I think tokens are a great way to build governance systems, but I don't think it will be easy/possible to build a token that achieves the all objectives with the same token - stable payment solution, security of a network and non-network governance....
I agree with this.
18:55:50 From Rouven Heck to Everyone:
token distribution is core
18:55:51 From Shannon Wells to Everyone:
by "staking pool for interest group" I mean potentially individuals who have certain interests joining together to form a staking pool run by someone perhaps elected to make voting decisions.
18:56:05 From Richard Esplin to Everyone:
cheqd supports staking pools, BTW.
18:56:53 From John Court to Everyone:
@Drummond - Chat takes off because it is a decentralized forum not requiring the centralised restriction of single speaker :-)
18:56:54 From Rouven Heck to Everyone:
What is the cheqd token distribution? Team, Outlier + Evernym?
18:57:15 From Darrell O'Donnell to Everyone:
You need a network to start building - adding incentives (tokens) for developers and users will increase dispersion of the token - that's my hope/thesis.
18:57:24 From Rouven Heck to Everyone:
You might need a 'fair launch' of a token to have a better start
18:57:57 From NickyHickman to Everyone:
ooh I like that 'genesis governance' I have been describing it as starter-yeast for the yoma sourdough
18:57:57 From Darrell O'Donnell to Everyone:
@Rouven - I imagine dozens of Master's and PhD theses being granted for defining "fair launch"
18:58:36 From Shannon Wells to Everyone:
yes definitely
18:59:06 From Rouven Heck to Everyone:
It's happening in various projects since years
18:59:08 From Alex Tweeddale to Everyone:
https://blog.cheqd.io/entropy-in-decentralised-governance-part-one-b6dc2dab0085

18:59:15 From Alex Tweeddale to Everyone:
3 parts of goodness
18:59:23 From Richard Esplin to Everyone:
To the point of "fairness" for different populations, such as global south, emerging economies, etc, I expect that there will be different networks that tailor to those various needs.
18:59:45 From David Waite to Everyone:
@John more that speaking is a consensus driven ordering while chat is an asynchronous system :-)
18:59:57 From Shannon Wells to Everyone:
“turtles all the way up"
19:00:19 From John Court to Everyone:
@David I like that the speaking is the spark and chat is the fire :-)
19:00:52 From NickyHickman to Everyone:
ON a system of justice that is based on Fairness - see https://plato.stanford.edu/entries/rawls/
19:03:04 From Shannon Wells to Everyone:
yes definitely
19:03:10 From Chris Matichuk to Everyone:
And what happens if the system indicates not enough randomness....
19:03:19 From Shannon Wells to Everyone:
that’s the follow up Q
19:03:28 From Rabble to Everyone:
Gosh, if you had a decentralized system like scuttlebutt there's no need to measure centralization because we have no centralized single ledger like blockchain projects.
19:04:01 From Chris Matichuk to Everyone:
That is kind of why I suggested a governance for the governance (whatever that might mean)
19:04:14 From John Court to Everyone:
Thoroughly impressed with the volume of work on this at docs.cheqd.io deserves a lot more time to digest for me.
19:04:31 From Margo Johnson1 to NickyHickman(Direct Message):
Hey Nicky! Would love to say hello and share ethics resources at some point. I taught an ethics course for graduate design students and when we reviewed frameworks through case studies in the SSI space we almost always feel towards consequentialist frame. Curious to hear what you are finding.
19:04:43 From Aaron Goldman to Everyone:
For scuttlebutt the bottle neck would be the number of source repos that implement the protocal
19:04:50 From NickyHickman to Everyone:
You can also Measure hierarchy in networks https://arxiv.org/abs/1202.0191
Level of influence (there is a clever mathematical formula that enables you to measure levels of influence in networks, and a good deal of research in this domain eg http://dss.in.tum.de/files/bichler-research/2008_kiss_identification_of_influencers.pdf . to identify a participant or node that has disproportionate influence
19:04:53 From Shannon Wells to Everyone:
@rabble: https://medium.com/certik/the-blockchain-trilemma-decentralized-scalable-and-secure-e9d8c41a87b3
19:05:26 From Judith Fleenor(Trust Over IP) to Everyone:
Helpful, thanks for explaining Alex
19:05:53 From NickyHickman to Margo Johnson1(Direct Message):
would love to catch up sounds as if you can really help me!!! I am studying now. Also feels as if we should meet. https://calendly.com/nicky_hickman/
19:06:03 From Darrell O'Donnell to Everyone:

type of problem - how about one where the PoS folks won't vote for the changes needed to shift the entropy where things improve?
19:06:20 From Shannon Wells to Everyone:
good Q
19:06:29 From Mike Ebert to Everyone:
Have to run, see you all later (hopefully at my session tomorrow)
19:06:52 From Joe Hsy to Everyone:
Not sure you can ever get around the risk of collusion off-network.
19:07:05 From Rabble to Everyone:
@chris yes, you could measure decentralization based on the number of distinct implementations and user facing applications. Few blockchain projects have multiple implementation with zero code reuse or sharing.
19:07:17 From Margo Johnson1 to NickyHickman(Direct Message):
Agreed - will find a time :)
19:07:31 From Mark Drummond to Everyone:
@Joe it's hard to stop people from being people!
19:07:39 From Marc Davis to Everyone:
@Darrell, you mean like in the USA today?
19:07:47 From Joe Hsy to Everyone: Need, ultimately it is still people...
19:07:47 From mary104 to NickyHickman(Direct Message): Hi Nicky!
19:08:05 From Darrell O'Donnell to Everyone:
@Marc - that was more of a governance in general thing but take it as you like!
19:08:07 From NickyHickman to mary104(Direct Message): hi mary
19:08:13 From mary104 to NickyHickman(Direct Message): nice to see you here
19:08:19 From NickyHickman to mary104(Direct Message): likewise
19:08:22 From mary104 to NickyHickman(Direct Message):
and hear you ;P
19:08:36 From Phil Wolff to Everyone:
Mediators that settle cross-governance disputes.
19:08:46 From Darrell O'Donnell to Everyone:
is the King subject to governance?
19:08:53 From NickyHickman to Everyone:
my hope for the future of governance - local first & cooperative
19:09:23 From Marc Davis to Everyone:
@Darrell it is a key problem of how self-governing systems operate in which money can be used to convince stakeholders to vote against their own long terns interests.
19:10:00 From Tim-from-IAMX to Everyone:
Trust Triangle. The Verifier trusts the authenticaton Agent.
19:10:01 From NickyHickman to Everyone:
my fear for governance - it exacerbates existing power imbalances and inequities because we automate too quickly without thinking human first
19:10:12 From Marc Davis to Everyone: +1 Nicky
19:10:17 From Darrell O'Donnell to Everyone @Tim "authentication agent"?
19:10:21 From Joe Hsy to Everyone: +1 Nicky
19:10:23 From Margo Johnson1 to Everyone: +1 Nicky
19:10:25 From Catherine Nabbala to Everyone: +1 Nicky
19:10:36 From Shannon Wells to Everyone:
Jumping on the +1 Nicky bandwagon
19:10:46 From Apichet (shake) Finema to Everyone:

We're talking about country's regulations, norms, and cultures..
19:10:52 From Darrell O'Donnell to Everyone:
@Nicky - that's my terror of "machine readable governance" - but I like terror - it means there is something there of value IMO
19:10:54 From Tim-from-IAMX to Everyone: Gateway to OnBoard credentials. Convert plastic and paper attributes by authentication agent: Hardware, Software, Biometrics on state level
19:11:24 From NickyHickman to Everyone:
If you are interested in joining Yoma Ecosystem TaskForce @ToIP you are welcome!!!! https://wiki.trustoverip.org/display/HOME/YOMA+Ecosystem+Task+Force
19:11:28 From Apichet (shake) Finema to Everyone:
True to what nick said…norms, regulations, and cultures…even if do right..may go against human first
19:11:44 From Kaliya Identity Woman to Everyone: http://www.humanfirst.tech
19:11:47 From Aaron Goldman to Everyone:
Hope: we get better at building ad-hoc just in time communities to solve problems
19:12:07 From Apichet (shake) Finema to Everyone: Kaliya! nice
19:12:08 From Kaliya Identity Woman to Everyone:
who is in the room and dealing with people being people as opposed to techno-utopianism
19:12:12 From Alex Tweeddale to Everyone:
Side note, we're looking for Node Operators at cheqd - if there's any SSI providers in the chat who are interested in learning more and joining our community!
19:12:14 From Aaron Goldman to Everyone: Fear: that we tie all our identities to political affiliations
19:12:52 From Kaliya Identity Woman to Everyone:
if folks want to engage with Humanfirst.tech please reach out to me.
19:12:55 From John Court to Everyone: My main hope for governance is that at the very least Holders will all require VCs from Verifiers of some sort before they will hand over any VC data themselves, or it is a ladder of trust approach on both sides of the Holder, Verifier interaction.
19:12:59 From Marc Davis to Everyone: +1 @Kaliya
19:13:04 From Kaliya Identity Woman to Everyone: kaliya@identitywoman.net
19:13:04 From Gillian Delaunay to Everyone: @kaliya One in the room over here! (Hand wave)
19:13:20 From Kevin Griffin1 to Everyone: @Alex @Nicky fantastic session - thank you
19:13:52 From Richard Astley to Everyone: Really great session, thanks!
19:14:07 From Chris Matichuk to Everyone:
Lots of good stuff....notes please - https://docs.google.com/document/d/1fVcnLZJW-SeDWLgKuJAXbbdlCCD0-6qDUOJL40dkl0Y/edit
19:14:23 From Shannon Wells to Everyone: Thanks all speakers, lots of food for thought
19:14:25 From Kimberly Linson to Everyone: Great session! Thank you!
19:14:26 From Judith Fleenor(Trust Over IP) to Everyone:
If you want to get involved with Governance Frameworks being discussed at ToIP… https://trustoverip.org/get-involved/membership/
19:14:27 From Marc Davis to Everyone:
Amazingly informative and provocative session, congrats!
19:14:36 From NickyHickman to Everyone: Thanks all for joining
19:14:42 From Darrell O'Donnell to Everyone: keep being awesome folks!
19:14:44 From Mike Varley to Everyone: Thanks everyone
19:14:48 From ChrisKelly to Everyone: Thanks all for some great discussion

Sign-In With Ethereum (AuthN)

Wednesday 11K

Convener: Wayne Chang, Spruce Systems (NYC)
Notes-taker(s): Juan Caballero, Spruce

Tags for the session - technology discussed/ideas considered:

- Authentication (maybe Authorization)
- Security and Privacy Engineering
- UX, Wallets, Web3

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

Important links

- Dedicated website for the project (includes research, notes, and recordings for community calls)
- Draft Spec

Spruce Links

- Company Website, Discord server, and Developer Portal
- Demo for Kepler, our ZCap-based "EDV" storage solution (Q&A at demo table)
- Demo of Rebase Protocol, our self-serve identity assurance engine - (also available in more verbose version) (Q&A at demo table)

Notes:

- Wayne - Screenshare
    - RFP
        - Metamask - 10mil MUA
        - Context: AuthN, "accounts" in Web3 zone
        - Context: example of OpenSea
    - Spec overview
    - Site overview (links to community calls)
    - Screenshare of Supporters section - User research
    - Spec in more detail
        - EOA/SC addresses - no questions
        - ENS -

Questions

- AGropp: metamask = only wallet?
    - WYC: yes, altho Oliver and I are working on other
- Nader: high-level, what are advantages of SIWE over manual consent to specific actions?
    - WYC: 2 categories of ethN signatures - TXNs sent to nodes, and arbitrary data signing
        - We all agree arbitrary data signing is not great, partic if not standardized
        - Oliver: Caveat- Wallets implement a set of JSON RPC interfaces, not only for onchain use cases-- 191 is one of them
- Malla: SIWE can be used with OAuth, you said; what are the use-cases for OAuth that you're imagining?
    - WYC: Use cases: degen first

        - WYC: OAuth for web2 (one more button for OAuth companies)
    - AGropp: OAuth and uncorrelated stable identifiers?
        - WYC: That's out of scope of this spec; you would use an HD wallet-derived keys for this, and what you're describing is higher level
    - Oliver: is it a requirement that wallet vendors don't change implementation?
        - WYC: Depends what you mean by "use this"
        - Oliver: this uses the dumb signature API; it's "dangerous" because it *looks like* it works for the RP, without actually having any security
        - WYC: Let me finish this your and i'll come back to domain binding normative requirements and other security issues
        - Oliver: why not ask more of implementers?
        - WYC: We're interviewing them… the further we push, the less likely they are to commit and implement in the short-term.
    - Kyle: False rendering attacks?
        - %s - cross-site Scripting attacks (XSS_?
        - WYC: frontendSPA
    - Oliver: Is this ABNF extensible?
        - WYC: URI list is only extensibility
        - Oliver: RPs need to validate response against a versioned ABNF; version 1 RPs won't be able to parse version 2 messages (WYC: SemVer)
    - Kyle: Augur's prediction market
        - Kyle: They put a bunch of files on IPS accessed through an IPFS gateway - how would you domain-bind to an IPFS://?
        - WYC: you mean if ipfs:// demanded a signature?
            - Content hash str isn't a very good UX
            - Kyle: it's not authoritative anyways cuz it's just a gateway
            - WYC: But IPFS has its own URI scheme
        - WYC: That's a good point
    - Oliver: I'm confused-- you don't propose JWTs because wallets don't support it, but you impose domain verification (which they also don't support)
        - WYC: UX tho; without wallet support, UX is terrible;
    - Juan: Oliver, could this signed string be represented as an EIP712 object? Are all these mandatory fields expressable first as an 191, later as a 712?
        - Kyle: DIDComm v1/2 analogy: breaking changes to v2, but if v1 works well no one wants to break anything - difficulty of incentivizing
        - Kyle: SSLv3 - only able to push people off of it at great cost and TLS 1 took forever; deferring safety to v2 bifurcates the market
        - WYC: Wallets are going slow; in the meantime
        - Kyle: Leverage conformance to pressure Wallets into an upgrade? What are the tradeoffs? You already have this forcing function, dApps are signing onto this spec and have adoption on your side…
        - WYC: But if we show the users an EIP712 JWT, these RPs will bail; their sign-in is contingent on good UX
        - Kyle: But we need to distinguish wallet UX and dApp UX…

Identification Minimization and Other Respectful Tech Principles

Wednesday 11M

Convener: Lisa LeVasseur
Notes-taker(s): Lisa LeVasseur

Tags for the session - technology discussed/ideas considered:

#RespectfulTech, #IdentificationMinimization

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

In this session, I presented the Me2B Alliance's Attributes for Respectful Me2B Commitments using this deck: https://ooqc943yvdw4abzes1q1ezta-wpengine.netdna-ssl.com/wp-content/uploads/2021/10/intro-me2b-spec-iis-101321.pdf

The purpose of the session was to introduce the principle of Identification Minimization and to get feedback on whether or not it resonated with people in the Identity space. Consensus was that it did resonate.

Clarifying discussion around:

- The difference between Identification Minimization and Data Collection Minimization,
- How the Me2BA tests for identification minimization,
- How the Me2BA standard for safe and respectful technology needs additional context/testing to better understand industry/sector technology behavioral norms to determine where the "passing" threshold is or should be.

You MUST have a Choice of Policy Managers - Credential Issuers MUST NOT be able to impose the policy manager

Wednesday 12A
Convener: Adrian Gropper and Alan Karp
Notes-taker(s):

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

1 - In Verifiable Credentials (VC) protocol designs, the Issuer is typically a sovereign (state or corporation) and the Controller of a mobile or custodial wallet is sometimes an individual human, like you.

2 - You have a policy _in mind_ when you tell an Issuer what to include in a verifiable credential (VC). Let's call this telling a **permission**.

3 - Your policies may change over time without the Issuer having any idea that a policy that may apply to them has changed.

4 - At any point the Issuer receives **permission** to issue a VC and is bound to respond to that specific instance according to _their_ policies, which are separate from yours.

5 - The point of this session is that protocols for an Issuer processing a permission for a VC issue **MUST allow for you to choose your policy manager** that decides on the components of the VC as encoded or linked to the **permission**.

6 - Giving the Issuer a role as your policy manager violates a number of human rights and security principles including the Law of Agency, Freedom of Association, Data Minimization, Separation of Concerns as well as Zero Trust Architecture.

Questions:

Q1 - What is the relationship between DIDComm and delegation?

OAuth2 AND GNAP could both be MUST

Supply chain use case - somebody signed

Audit

Q1: - DIDComm - with a notary tap uses KERI to keep the log or bust

Logging is an issue but has to be identity protected somehow (court order)

Conclusion: **Another session is needed in order to discuss the application of DIDComm to Zero-Trust Architecture**

Where do We Work on Interop as a Community?

Wednesday 12B
Conveners: Kai Wagner, Andreas Freitag, Hakan Yildiz, Euginu Rusu
Notes-taker(s): Conveners, and Charles Lehner

Tags for the session - technology discussed/ideas considered:

SSI; Interop; governance; Standards Bodies;

Levels of Interop:

- structural level
- syntax level
- semantic level
- organizational level

General:

- Testing has to happen in the standardization process, not after.
- Do we have a place for less technical groups to communicate interop

Useful Resources:

- Verifiable Credential Flavors Explained by Kaliya Young published by LFPH/CCI

Places where Interop of some type is being worked on:

- **DIF**
    - Interoperability Working Group (co-chairs Kaliya Young, David Waite, Snorre Lothar
        - Recently hosted Libraryplooza - current stack diagram
    - WG Applied Crypto (BBS+, revocation,..)
    - WACI-PEx

W3C CCG

- **CCG links**
    - Meeting weekly, Tuesday @ 9am PT / Noon ET / 5pm ST/GMT / 6pm CET
    - Main page + join: https://www.w3.org/community/credentials/
    - Other supporting documentation: https://w3c-ccg.github.io/
    - Mailing List (open and public on the web): https://lists.w3.org/Archives/Public/public-credentials/
    - Our github: https://github.com/w3c-ccg
        - Work items are sub repos
    - Work item process: https://w3c-ccg.github.io/workitem-process/
- **SVIP- Silicon Valley Innovation Program - supported work within it CCG**
    - VC-HTTP-API work: https://github.com/w3c-ccg/vc-http-api
    - Interoperability Test Suite
    - Traceability: https://github.com/w3c-ccg/traceability-vocab
    - Linked data signature suites, and other work items

Hyperledger

- **HL-Aries**

Trust Over IP

- Interop task force (semi-dormant)
- Good Health Pass Interoperability Blueprint

- **NGI Atlantic - Markus is trying to do interop between SVIP funded work and EBSI**
- **Interop in specific commercial / governmental ecosystems**

Between Market and Standards:

CCI - working on a vertical problem related to Covid Credentials

- Covid Certificate landscape

Government Funding:

- US DHS Grants (this work is done publicly in the CCG @W3C per the terms of the funding) Videos of last interop demos
- For European-based individuals/independents (incl UK), StandICT
- ESSIF Interop (EBSI)
- Canada - User-Centric Verifiable Digital Credentials Challenge (sister project to US DHS SVIP program listed above) - run by Treasury Board Secretariat of Canada (TBS) and Shared Services Canada (SSC) https://github.com/canada-ca/ucvdcc

Adjacent (Q: should we work on interop with initiatives that are not SSI centric, but play a key role in digital identity globally?)

- ISO? They have the mDL standard - tones of questions about how this aligns with VCs
- OSIA - https://secureidentityalliance.org/osia <-this is for large national ID systems not SSI.
-

SVIP Plug Fest Links

- Demo week announce & schedule: https://www.dhs.gov/science-and-technology/svip-demo-week
- Blockchain day playlist: https://vimeo.com/showcase/8833272
- Heather's recap of 3 questions from the panel moderation between Anil John, Tim Bouma, Olivier Bringer: https://medium.com/in-present-tense/three-governments-enabling-digital-identity-interoperability-bbcfc60c3a80

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

https://id4d.worldbank.org/guide/interoperability - focused on government issued IDs

Where are we truly trying to solve the same problem? Example would be the potential overlap/alignment of WACI-PEx and some of the HL-Aries Interop Profiles.

"You MUST have a Choice of Policy Managers - Credential Issuers MUST NOT be able to impose the policy manager"

- Credential Issuers are publishers of claims about Identity
- Interesting - Credentials may be useful outside of a governance framework but may not be. Example: a valid credit card works on a credit card network for payment - it can also be used for other purposes (e.g. car rental company use CC as a proxy for "is valid human" sometimes). The credit card itself would be of zero use if the Credential Issuer was NOT imposing policy.

Excerpts of some discussions

Heather: I'm independent… don't have corporate drive… happy to help facilitate work in CCG, but if consensus is that it's better to do the work elsewhere, recommend follow some of the same beneficial processes as CCG…

… Interop happens where it makes sense…

Brent: difficult to say where introp "should" happen… various considerations… but there seems to be enough cross-polination between standards bodies… WACI-PEx… makes use of little bits of everywhere… successfully… that work began here! Incubated at DIF… A great place to come together is IIW. Maybe have a session about how to get the interoperators to interop?

Kaliya: I'm co-chair of DIF Interop WG alongwith D. Waite and Snorre…
[Sharing screenshot of table regarding interop - "current stack diagram"]
Need vision moving forward…

Andreas: thanks, there is some work like what we have been doing…

Paul: taxonomy of interop… standards require some testing to prove it's valid… that interop is possible… I believe that must happen as part of the standards process… otherwise it's too late…
… But other kind of interop: trade organizations give a sticker that you comply with a profile… (e.g. bluetooth)... involves a pool of devices that have to work together…
… I think that must happen outside the standards organization… It can be very sensitive… a lot riding on that interop sticker… "product interop" difficult to disclose in a public forum. Vs "standards interop"... different concept

Andreas: thanks… any other comments/questions/additions?

C. Lanaham: confusion about running program…. Until document about three flavors of verifiable credentials gave us clarity… that's super-helpful, for that project at least…

Balazs: I work for DIF… To extend on what Kaliya said… from a steering committee level… there is definitely a search for an interim group hosted by DIF… the group wasn't created as a DIF group but as an effort to work on Interop, to provide initial infrastructure needs… the name was added not because it's a working group (not IPR protected) but to create trust for outsiders who might not understand it… Group has been meeting for the past 15 months, quite regularly… well-known… could go further with it…
… Question of what standards can do… DIF intends to be neutral on technology. Making specs on more established tech is possible… but doing full-on certification, giving the more wider approval, might not be in the framework of DIF… but if you would like to talk about it, there are many open ears… the steering committee is tackling this question… Reach out to me.

Lucy: To follow up on C. Lanaham's point… the paper on CCI… the work we're doing is also part of interop work… but very different from the technical community work… I had a session earlier about CCI sitting in between the technical communities and the mass market… Kaliya has been doing a lot of work communicating complicated standards work… My job is to communicate it to people who are not technical at all… I think there should be another category of organizations that have a position, like CCI, who could serve that in-between role. I notice there are special-interest groups within technical groups… that is great,

but very technical-driven still… How can we have actual non-technical groups with people who are not from technical community, and also from mass market? They should play a role in interop.

Kaliya: Verifiable Credential flavors explained paper was possible in part because the year before I was funded to do private research for a client, and then a year later it became obvious other folks were not understanding these critical differences, and I wrote this for public…
… There is another paper that I was working on about exchange protocols - which lead to the WACI-PEx work being catalyzed (Killer Whale Jello Salad). WACI-PEx developed between IIWs and reached version 0.1 completed between the two events…
It seems there is a layer of what Lucy is touching on, that I did by accident with that paper, that is explaining clearly the choice landscape to create alignment among a broader range of stakeholders, so that more interoperability is possible, because more understanding is possible, so choices start to align… Different strategies for interop… but wonder if we **can brainstorm key communications/documents, areas of articulation that can be helpful in the same way that paper was helpful last year.**

Andreas: Yes… it would be great for everyone to come together….
Kaliya: I'm asking a different question… I think we could try to do that… but there is also an opportunity to write additional papers to help alignment happen that is not getting everyone into one room.
Andreas: At the end of the day, need an objective decision…
Kaliya: Yes… people read that paper and got alignment on objective decisions… More than one way to get alignment?
Andreas: but also a risk the group splits and makes different decisions?
Kaliya: the world is already split.
Andras: but just papers… it's a good start, everyone can get an overview… but then the next step must be to agree on a way to go, to achieve real interop for SSI implementers…
… I work for Jolocom… I see the pain, because we have to decide which way to go, and we have no clue… Is it the interop where everyone is going, or will it just end up us using it?

Lucy: why you wrote that paper… to help the market understand… like how we wrote that paper on the Covid credential landscape…
… The technical community could consider this approach…

Heather: I like to get real. My real question is, what would be the deliverables for interoperability be? I'm thinking about it… maybe three things. First, the tech. A standard? Or maybe not a standard. I'm in W3C, a standards group… but I know there are other technologies… it's an open world... not everyone is going to use everything. The tech being used. The beautiful theory in our minds the perfect world. Second, the implmenetation, where it gets hard and ugly… that beautiful philosphy we have gets challenged, we have to get real and make tradeoffs. The third thing: need documentation to support implementers(?). If we were a company, with a CTO, product team, sales, we'd have documentation writers, community manager… If we follow that path, back to my initial question, to be pragmatic, what are the deliverables, or the one deliverable, that we want to do interop? Figuring that out could help us make sense of it. If there's multiple deliverables, maybe one gets done in one area, another in another area. Strength of W3C is it's tech-centric, but it's also a weakness… hard to understand it. What do we want to deliver, for interoperability?

Andreas: Thanks. I have an answer but will save it for later.

Richard: Me too. I work for Evernym… It's very expensive to test interoperability.. I think it's worth highlighting the drivers that make it worthwhile. I don't see there being a single SSI interop standard…. First key: customer demand. Even though I want to test interop, it will only happens when it's aligned… No

vendor lockin, want assurance to interop with vendor X (usually someone large), and third to support some specific use case (e.g. privacy)...
… The thought leadership Kaliya asks about is super valuable…
… Deliverables: most customers just want an assurance ("yeah, I did the test"). Some want a demo, or a spreadsheet (what specific features are supported). Customers have asked me if there is a certification, but there is not a credible one… But if there was a credible one like with privacy-first, I could see us doing that…

Andreas: Then we have to decide as a community, do we want to have chat apps where people can't talk to eachother, because of different apps (lock-in), or more like email clients (where anyone can write an email client)? That's the decision… The customer cannot make that decision, because they're not as deep as we are. We as a community have to decide… If we want the first world, we can stop here and everyone develop their own stack… Otherwise we need agreement. As far as I understand the community and Jolocom, we want the second one - real interoperability, everyone can create clients and they work together. If an issuer creates a verifiable credential, [any verifier can verify it]. That's my picture of interop…

Richard: important to recognize that email has survived around Slack, etc. Creating choice for interop is valuable… But premature standardization is dangerous, we've got it wrong… not confident we've got it right now… I'm confident to see what we can get that production adoption with, and then drive those standards through the ecosystem…

Paul: I think the education and making simple explations of the landscape (Kaliya, thank you for that chart)... As an end user, it's very difficult to understand what is possible, let alone interop… The way we are using the word interop may be different from how it is used in other communities… JSON-LD… two different standards… it's a decision people made to go different technical groups because they thought one was better than the other… When I think of interop… Same data model… I see our case as a combination of the two… People are still vetting the technical approaches… That disagreement is because we are still trying things out… That's natural… In the Internet, there used to be a bunch of internet protocols. Because this is a global interoperability challenge, like the Internet, this will sort itself out too… And community.... But if people are trying to interop but unable to, even using the same standards, that's a standardization issue…
… In front of external audiences in the market, we're all working together…
… But internally there are still differences of opinions…
… I'm a customer in this business, don't have a stack necessarily in what's better or not better.
… Documenting the decisions like Kaliya and Lucy [were doing] is very valuable for end users…
… Challenging for an end-user because we think we have to wait… But end-users want to commit and make purchases… But the understanding the fragmentation may be the best way to make a decision, if it's in one place, to make own decisions.

Paul B: I agree with other Paul's comments… There's always the "11th standard"... people think they have better choices… we have to find the best technical solutions… there will always be different solutions… I would love to have a unified stack… There will always be different stacks… Maybe it would be good to approach interop from the level of incentives… Maybe it depends on what role you are in the VC data model? Wallet vendor may work with everything… but issuer can look at what fits best for their tech stack and use case. Maybe different people in the community have different incentives; this must be regarded.

Andreas: Interop: issuer is also verifier. As verifier, may want to use credentials from others, to speed up process… so as issuer are also incentivized to interop…

Paul B: I agree… the biggest strength that you can use multiple credentials… Makes it difficult for verifiers to provide multiple tech stacks… But there are use cases where I as the issuer don't necessarily have to be a

verifier… Government use cases… usually just providing “identity” not verifying it… may be restricted by regulations…

Andreas: Yes, and no…

TelegramSam: We have to have the same goals and requirements in order to unify on an approach to make that happen. One reason for interop… the community tends to align around philosophical goals… One is whether you believe that zero-knowledge presentations are worth the effort or not… one of the deciding things between communities. If you can’t unify goals, can’t agree on underlying technical stuff… How do we get interoperability to a goal(?) We will reach it in the community with like-minded goals…

Andreas: Really valid point. One of the goals for us: is it a competition? Or a market? Is it a goal of the community to decide on a stack?

Evan W: This seems like a lot of independent players working on this… but there are massive giants… Amazon, Microsoft, Google, cloud providers, big IAM(?) providers, that can shape how this space (standards) evolve… Probably Government projects going on too, all over the world large government practices in Identity. How do we feel about doing interop before they are involved or have declared themselves?

Andreas: I think it’s an argument to move fast and set a standard…

Hakan: What Sam said… having goals for interoperability… very true… many issues happening now in SSI and in how SSI is perceived… One is the fundamentals - public trust infrastructure - decentralized public key infrastructure - decentralized identifiers - have requirements, high availability, …
… But still have disagreement about things like BBS+, envelopes…
… Maybe it could be good to think of like an email client? Complete the same set of [features?] to be used? But what is the ground(?)... verifiable data registries… DIDs…

Evan W: I think that’s fair.
… I would observe IBM’s strategy… they did this long ago, for decades, waiting until the market is big enough before setting their foot in the market… minicomputers… then come in with massive sales, marketing and business relationships, to overwhelm… The pioneers rarely had a chance to survive that.

Andreas: cannot be closing statement… depressing…

Lucy: Covid credentials…. UCC(?) SMART health card, [...]… not strictly verifiable credentials, but some using terms of verifiable credentials. How they are doing interop… Something major, a bigger one showing up… those people will find a way… if IBM has something, and Microsoft has something, and the market is expanding and using it, they will have to figure it out for the sake of the market… DIVOC being adopted by entire nation states… they are doing interop by adding EU DCC(?) to their stack… and also doing VCC… What we’re working on is different paths, that are interoperable with eachother… That’s what’s happening in the market… IBM came to the space earlier on… The world would be different if we all backed IBM… sounds impossible… but can we leverage the big names, already having some market share?

Kaliya: I’ve posted a link to a series that covers the main credential types being used globally…

Lucy: that’s DIVOC… but also…

Kaliya: India… this post writes about it… One reason those folks even know about it is that I went to India two years ago, and met the folks who created India's national ID standard, and told them about our standards. Human-to-human communication early on, an important strategy to consider.
[break]
… Can our groups collaborate more, at least in an information-sharing sense?

Heather: I wonder if we can bubble this up to our governments… I wonder if we can look to Tim Bouma or Diyak(?) or SVIP Anil, or Oliver R(?)... European organizations that fund things… Those governments have a lot more power than those of us in the room, to enforce regulation, comply with GDPR… and the ability to put money where their mouth is… I don't know how many of us in this room have deep pockets…

Lucy: Conversations in chat… Implementers trying to do the right thing, to serve the market… Can we shift our energy, to help… get it to market… technical pieces that need to happen in the open? Whether for interop or not... Let's just see who is doing good work, who can get our tech to be used by more people, look at what they need to get there… it must be developed in the open, I think everyone agrees with that here.

Andreas: Yes, thank you… But still… The people doing interop need a place to align and discuss technical stuff… I haven't found this place/foundation… not every 6 months but every 2-3 weeks… moving in directions, can we align or not… SSI is still small…
… Can we agree on a place to meet? We have so many places to meet…

Hakan: Kaliya is chair of DIF Interop group… Times are good for European…
Aaron(?): And a mailing list…
Andreas: but aren't there stakeholders involved?
Kaliya: what do you mean?
Andreas…
Kaliya: … I would love to come to your group… 70 different entities collaborating in Germany, that's amazing… You should keep doing that, but consider how to connect with other interop efforts.
?: It's an option… we'll use that as an update opportunity. Especially because of the current setup that allows anyone to join…
… DIF working group might be a good place to have… that conversation…
… This major challenge of feeling like there is not one place to speak to all the players via one mailing list…. Feels like we're missing something… Nobody can be blamed, it's cat herding… but IIW, many players meet. Maybe we can make DIF WG more attractive to others?
…
Kaliya: propose you come to DIF Interop… I'll post about it to CCG… It's not IPR protected, only talking about things people are working on at other places. If we identify a problem that needs solving, that it needs a container…
Andreas: Yes…
… Thank you for this lively conversation! The topic is hot and urgent. Thank you for your input and participation.

<u>Zoom Chat documentation</u> – including links to a lot of the mentioned articles
20:18:57 Von Kaliya Identity Woman an Alle:
Maybe we can work on a list of different places where interop is happening - maybe go around the room and hear from these different efforts.
20:19:03 Von Kaliya Identity Woman an Alle: Also we need a note taker
20:19:06 Von Kaliya Identity Woman an Alle: and are we going to recrod

20:22:22 Von Kaliya Identity Woman an Alle: can you share the slide deck link?
20:22:53 Von Paul DIetrich an Alle: it session 1 C
20:23:01 Von Andreas Freitag1 an Alle:
https://jolocom365-my.sharepoint.com/:b:/g/personal/andreas_jolocom365_onmicrosoft_com/EYOzZpPMjjZPoLBSzKIqgOIBCPjURAqD58_ku67Eoz0pOQ
20:26:18 Von Bart Suichies an Alle Are we considering bodies like EBSI and ESSIF as well?
20:26:29 Von Bart Suichies an Alle:
or, say, ISO ;)
20:26:31 Von Kaliya Identity Woman an Alle:
put them on the list
20:26:50 Von Bart Suichies an Alle:
do you have a link to the notes?
20:27:13 Von Bart Suichies an Alle:
oh never mind
https://docs.google.com/document/d/1tiwNrtL6qODC0wehBqU7TW2F0olJSHld5wHHXcR4850/edit
20:27:24 Von Charles Lanahan an Alle:
In addition to US there's also https://github.com/canada-ca/ucvdcc in Canada
20:27:38 Von Charles Lanahan an Alle:
done within the various domains of these groups but focusing on W3C VCs
20:27:47 Von Charles Lanahan an Alle:
(dids and dicomm)
20:28:00 Von Kaliya Identity Woman an Alle:
I don't think ISO cares or likes VCs and it is so secretive and closed - its hard to interact with it
20:28:36 Von Charles E. Lehner an Alle:
David C is in ISO? and likes VC?
20:28:39 Von Bart Suichies an Alle:
that's the thing with interoperability.. you don't always get to choose your standard ;)
20:28:46 Von Bart Suichies an Alle:
https://id4d.worldbank.org/guide/interoperability
20:28:58 Von Shannon Wells an Alle:
VC=Verifiable Claim or Verifiable Credential?
20:29:09 Von Darrell O'Donnell an Alle:
@Bart - actually in this case we get to pick 5 or 7 from a mixed bag
20:29:23 Von Darrell O'Donnell an Alle:
@Shannon - Verifiable Credential
20:29:26 Von Charles Lanahan an Alle:
Verifiable Credentials mostly but also claims were used in the UCVDCC project and the US DHS project
20:29:34 Von Heather Vescent an Alle:
I can make some comments re: W3C and SVIP and also interoperability desires btwn US & Canada & Eu based on a recent panel.
20:29:38 Von Kaliya Identity Woman an Alle:
ID4D is about getting government records digitized and focused on "government issued ID" almost exclusively
20:30:32 Von Bart Suichies an Alle:
so - interesting question: where does interoperability end? Jus tbecause we might not like how other systems are working shouldn't (imho) render them outside the discussion of interop
20:32:21 Von Bart Suichies an Alle:

note on the DHS funding - the work being done at the CCG is not an explicit term for the funding. Provable interop with the cohort members is however.
20:33:02 Von Bart Suichies an Alle:
the fact that it's done in the CCG has much to do with existing relationships towards CCG by the majority of the cohort members
20:35:34 Von Darrell O'Donnell an Alle:
+1 Heather
20:35:51 Von Kaliya Identity Woman an Alle:
I posted the video to the last one
20:37:44 Von Darrell O'Donnell an Alle:
+1 open, no mandatory fee, IPR clearance, low conflict…
20:38:03 Von Heather Vescent an Alle:
Thank you for my long knowledge share
20:38:21 Von Kai Wagner – Jolocom an Alle:
Thank you Heather
20:38:32 Von Hakan Yildiz an Alle:
Thanks a lot for sharing it with us. Was quite a background information ☺
20:39:20 Von Heather Vescent an Alle:
I can give more color, if you like, but don't want to hijack this meeting.
20:39:31 Von Heather Vescent an Alle:
+1 Michael's point about vendor lock in
20:39:47 Von Heather Vescent an Alle:
Here is a highlight of three of the questions that I asked: https://medium.com/in-present-tense/three-governments-enabling-digital-identity-interoperability-bbcfc60c3a80
20:40:15 Von Heather Vescent an Alle:
Here is the SVIP Demo day Vimeo playlist: https://vimeo.com/showcase/8833272
20:41:07 Von Charles Lanahan an Alle:
https://github.com/canada-ca/ucvdcc
20:41:19 Von Heather Vescent an Alle:
Here's the SVIP demo week announce, you'll probably be interested in the blockchain ones: https://www.dhs.gov/science-and-technology/svip-demo-week
20:42:25 Von Heather Vescent an Alle:
Here's the SVIP post event page with all their links: https://sri-csl.regfox.com/post-svip-demo-week
20:46:33 Von ChrisKelly (DIF) an Alle:
Thanks Kaliya
20:46:49 Von nembal an Alle:
:)
20:48:05 Von nembal an Alle:
+1 on Paul
20:48:45 Von Darrell O'Donnell an Alle:
+1 Paul - on a related note, I held a session yesterday about Premature Interop/Premature Standardization
20:48:58 Von Brent Zundel an Alle:
+1
20:49:02 Von ChrisKelly (DIF) an Alle:
+1 Paul
20:49:23 Von ChrisKelly (DIF) an Alle:
+1 Darrell's session was also useful on this
20:49:48 Von Paul DIetrich an Alle:

Kaliya, I saw you copy the link to that spreadsheet but didn't see it in the chat. Were you intending to share?
20:51:27 Von Kaliya Identity Woman an Alle:
its in the notes document "current stack diagram"
20:51:41 Von Paul DIetrich an Alle:
Thanks
20:53:05 Von Balazs Nemethi (DIF) an Alle:
balazs@identity.foundation
20:53:53 Von Bart Suichies an Alle:
So, who's willing to let go of some of the interop work in favor of a more coordinated approach? ;)
20:53:59 Von Lucy Yang an Alle:
https://docs.google.com/presentation/d/1n6OirMXMJN43PM7VpvypHMecV0J0ILvf0hAZSrPzBDE/edit?usp=sharing
20:55:28 Von Charles Lanahan an Alle:
second that for sure
20:58:27 Von Lucy Yang an Alle:
@Kaliya, you did the paper because the market needs to understand it. So that is a market driven approach we are using at CCI
20:58:40 Von Paul DIetrich an Alle:
Agree there, understanding the standards landscape will help the interoperability process and efficiency
20:58:45 Von Juan from Spruce an Alle:
Threw in another funding source for the Europeans (particularly independents and academics):
http://www.standict.eu/standicteu-2023-5th-open-call
20:58:57 Von Judith Fleenor(ToIP) an Alle:
+to clear communication to non tech people are needed, so they understand the questions to ask themselves the right questions about InterOp
20:59:30 Von ChrisKelly (DIF) an Alle: seconded Judith
20:59:58 Von Bart Suichies an Alle: Interoperability comes with opportunity costs of not getting to market, competing with worse alternatives.
21:00:01 Von Kaliya Identity Woman an Alle: what other topics should paper be written about
21:00:26 Von Bart Suichies an Alle:
@Kaliya - a framework for decision makers..
21:01:20 Von Bart Suichies an Alle:
Interop could be a metric for decision makers. But I feel it's more a means to an end. The end = no vendor lock in.
21:01:25 Von Bart Suichies an Alle: at least for buyers
21:01:30 Von Juan from Spruce an Alle:
^ INATBA is pretty good at framing things in a policy-oriented way
21:01:37 Von Bart Suichies an Alle: for users, it might be different
21:02:04 Von Kaliya Identity Woman an Alle:
can you post that good INATBA paper - in the resources section Juan
21:02:06 Von Juan from Spruce an Alle:
Policy-makers that impose firm constraints on funding around open-source, and/or open-standards, and/or guardrails against vendor lockin, make this a lot easier
21:02:32 Von Kaliya Identity Woman an Alle: the scenarios it paints are great.
21:02:34 Von Juan from Spruce an Alle: @Kai might be able to get the link faster than me ;)
21:02:55 Von Juan from Spruce an Alle: these notes are great-- could be a PDF on the dif interop repo unto itself :D

21:03:09 Von Charles Lanahan an Alle: I thought one good paper (or series of papers) would be a very high-level description of protocols/specs/what have you. That kind of covers

1. The security context the protocol/spec/what have you operates under
2. What they envision as the future if their protocol/spec/what have you will look like (to them) if their protocol/spec/ what have you gains hegemony
3. How difficult/easy that will/won't be based on the current state of technology

21:03:18 Von Charles Lanahan an Alle: focusing on particular areas
21:03:51 Von Heather Vescent an Alle: Great thanks.
21:04:46 Von evanwolf an Alle:
interop means trusting those the others trust.
interop means winner-take-all business models can dominate
interop sucks resources from other features and scale.
21:05:38 Von Kaliya Identity Woman an Alle:
de-gartnerifying analysis :)
21:05:59 Von Charles Lanahan an Alle:
For example. In our project people focused on did:key and did:web because it was a least common denominator among the various tech stacks that our teams had chosen.

1. The context is that we just want to implement software that will work with other current web 2.0 protocols/specs whatever today. Its easy to implement but it gets us to using dids, didcomm, VCs
2. it was chosen mostly because it was the easiest to implement in the time and with the money available. If it gains hegemony the web will operate much as it will today but we have the potential to move to more advanced did methods at a later date.
3. Right now that's pretty good for short term interop but long term it doesn't really gel with the greater SSI community because its not very secure, private, anonymous etc...

21:06:04 Von evanwolf an Alle: interop is vulnerable to a massive player redefining de facto standards
21:06:05 Von Bart Suichies an Alle:
+1 on richard's point.. most customers just want the shiny certification sticker
21:06:07 Von Bart Suichies an Alle: #iso
21:06:32 Von Darrell O'Donnell an Alle:
My working thesis that any sticker would be premature and turn into a “don’t use that one” mark.
21:06:43 Von Darrell O'Donnell an Alle: it is just too early
21:06:45 Von Bart Suichies an Alle: for sure
21:06:52 Von Darrell O'Donnell an Alle: that sticker will stunt our growth
21:07:02 Von Kaliya Identity Woman an Alle:
what I think I heard is that the Customers of SSI have to care about Interop - and that will drive it to happen.
21:07:17 Von Bart Suichies an Alle: I'd go one further, is that too much focus on interop right now is coming at a cost where we cannot go to market..
21:07:28 Von Kaliya Identity Woman an Alle: we have to get to market -
21:07:33 Von Bart Suichies an Alle: to andreas: or do we never want to have a chat-app at all, because we cannot agree on interop?
21:07:34 Von Michael Shea an Alle:
that sounds also like a very effective way to stunt the market
21:07:36 Von Kaliya Identity Woman an Alle: CommonPass will eat our lunch with SMART health cards
21:07:44 Von Darrell O'Donnell an Alle:

governments are shifting to open source on areas where “digital sovereignty” is at risk - e.g. UK - https://www.gov.uk/guidance/be-open-and-use-open-source#how-using-open-source-will-help-your-programme
21:07:47 Von Heather Vescent an Alle:
I think there are some problems with being driven from a customer motivation only… because they are profit driven, and that concerns me that the B2B customer really has the values of user privacy and data protection in mind.
21:08:27 Von Heather Vescent an Alle: +1 Andreas
21:08:52 Von Lucy Yang an Alle:
@Bart, I think it is a matter of short-term and long-term interoperability strategy
21:09:24 Von Heather Vescent an Alle:
But the standards community is more open than technology being built by a private company.
21:09:41 Von Darrell O'Donnell an Alle:
@Lucy - long-term interop testing and conformance is crucial - right now it’s helping guide change and that’s good but not converging necessarily yet.
21:09:51 Von Richard Esplin an Alle:
@heather You make a good point. We can guide our customers to focus on privacy (which is getting easier year-by-year), but at the end of the day, we have to stay in business.
21:10:18 Von Bart Suichies an Alle:
@lucy - true, but there's also a foundational point: we can be directionally in agreement, but operationally competing. Why not let the market decide on what the de-facto standard might be?
21:10:18 Von Lucy Yang an Alle:
@Heather, the idea is to understand what they are thinking and what they want to achieve and build things in a way that help them achieve goals without compromising the principles. And agree with Richard, a lot of guidance needs to happen.
21:10:43 Von Heather Vescent an Alle:
@Richard, right! And I don’t fault your corporate perspective. But it is not the only one, and it contributes to a capitalist perspective that is not necessarily supportive to human existence.
21:11:13 Von Kaliya Identity Woman an Alle:
right now folks are keen to do JSON-LD but finding it hard - like walking on broken glass … so that doesn’t seem like a recipe for success unless we really focus and make it substantially easier.
21:11:22 Von Lucy Yang an Alle:
@Bart, you are assuming market force will lead us to a good place, which is a very dangerous assumption.
21:11:33 Von Balazs Nemethi (DIF) an Alle: +1 lucy
21:11:52 Von Richard Esplin an Alle:
I absolutely agree that there are some solutions which, though potentially lucrative, should not be brought to market. But solutions have to serve the market to survive.
21:11:57 Von Bart Suichies an Alle:
nope, rather the opposite: I'm assuming that focusing on interop for the sake of interop will never let us get from our current place to begin with.
21:12:02 Von Judith Fleenor(ToIP) an Alle:
+1@lucy
21:12:21 Von Darrell O'Donnell an Alle:
@bart - agreed, we’ll end up interoperable and not adopted anywhere meaningful
21:12:23 Von Bart Suichies an Alle:
And this is coming from an incumbent view where I see 10/15 year vendor-locked-in contracts being pushed
21:12:37 Von Heather Vescent an Alle:

@Richard, there are other paradigms…. broad governments infrastructure investments that do not care about what the market wants. They are the backstop to market failures.
21:13:00 Von Bart Suichies an Alle:
the SSI community has a decision to make in that sense: we can be PGP if we don't compromise on our ambitions. Very valuable for 7 people.
21:13:02 Von Heather Vescent an Alle:
So both paradigms must survive and co-exist, and they can and be very supportive of each other.
21:13:02 Von evanwolf an Alle:
If we are talking interop, are all the players who can (and are likely to) shape this space here at IIW?

The biggest IAM vendors (Okta et al) and cloud API services (msft, goog, aws) seem missing here. Same for US federal government, and proxies for the billion-person regions.
21:13:31 Von fundthmcalculus an Alle:
https://xkcd.com/927/
21:13:43 Von Bart Suichies an Alle:
I'd like us to go to market with better solutions, in the realization they are (nowhere near) perfect
21:13:58 Von Darrell O'Donnell an Alle:
@evanwolf - they are well served by OIDC and looking at OIDC as the solution.
21:14:20 Von Bart Suichies an Alle:
the conversations I'm hearing is about how this is all 'conceptual' , 'not seriously in production', etc..
21:14:40 Von Richard Esplin an Alle:
@heather Agreed. Government investment plays an important and valuable role in shaping the commercial market. But my interop efforts are going to follow those trends, instead of trying to set those trends.
I've tried to set those trends for three years, and it hasn't been effective.
21:14:42 Von Lucy Yang an Alle: @Bart, that is the approach we have at CCI. We still need to talk about interoperability, but it doesn't have to take up our whole day.
21:14:48 Von Bart Suichies an Alle: which might not be entirey true, but it's a very real dynamic
21:15:05 Von Heather Vescent an Alle: @Richard, fair enough.
21:15:08 Von Judith Fleenor(ToIP) an Alle:
+1 @evanwolf… I've been wondering that about the traditional IAM vendors as well. At least Ping was here yesterday… but their view of what a VC and InterOp is is very different that this conversations.
21:15:34 Von Kaliya Identity Woman an Alle: David Waite that I co-chair the interop group at DIF is from Ping
21:16:18 Von Kaliya Identity Woman an Alle:
Okta isn't really "engaged" in any way that i know but they are on the edge of the community - Vitorio from Auth0 was here presenting the OAuth 101 session.
21:16:50 Von Heather Vescent an Alle: +1
21:16:54 Von Michael Shea an Alle: @PaulB You have assumed that Gov are not going to verify other kinds of data that are tied to a DID/VC. Cross border shipping of goods is a good example of where they will be in a verifier role.
21:17:04 Von Richard Esplin an Alle: +1 Sam: I'm feeling good about the BBS+ approach in Good Health Pass. Previous standards provided fundamentally different technical capabilities that prevented us from accepting them even if the DHS pushed them.
21:17:18 Von Kaliya Identity Woman an Alle:
mDL was built by issuers for issuers.
21:17:36 Von Juan from Spruce an Alle: ^ They're pretty aligned already
21:17:43 Von Paul DIetrich an Alle:

+1 Sam. Goals are sometimes driven by end user requirements. For example B2C versus B2B might need totally different requirements which lead to different stacks/solutions etc.
21:18:17 Von Kaliya Identity Woman an Alle who isn't in this room - MSFT
21:18:24 Von Kaliya Identity Woman an Alle: they are definitely doing "something"
21:18:45 Von Kaliya Identity Woman an Alle:
(they are at IIW) but they definitely have their own path/strategy
21:19:10 Von Hakan Yildiz an Alle: Maybe we should create a IIW level goal setting for the SSI interop
21:19:30 Von Kaliya Identity Woman an Alle:
WACI-PEx was motivated by moving faster together to be the killerwhales to kill the otters.
21:19:41 Von Richard Esplin an Alle: MSFT have been participating in TOIP Good Health Pass. That's part of my optimism.
21:19:53 Von Michael Shea an Alle: @Kaliya, I like otters!
21:19:53 Von Bart Suichies an Alle: as did IBM
21:20:33 Von Kaliya Identity Woman an Alle: MSFT was not involved in Good Health Pass (they drove the competing SMART Health Cards) MSFT is definitely not in ToIP
21:20:33 Von Bart Suichies an Alle: +1 on sam.. think you need to dive deeper as well on that one - what's the incentive design for the community and the individual (orgs) that are part of it
21:21:39 Von Kaliya Identity Woman an Alle:
what they (MSFT) do understand is developers and their needs - and SMART cards do that in spades - cause JSON blobs are EASY
21:22:40 Von Darrell O'Donnell an Alle: SHC is "good enough" for the job right now. It met the market with a solution that filled the urgency need. Privacy commissioners are starting to push back and say "won't do that again" but that's going to take time.
21:22:42 Von Juan from Spruce an Alle: nothin' easier
21:22:47 Von Kaliya Identity Woman an Alle: IBM was very involved in Good Health Pass and was a good actor there - doing their best to have the better privacy preserving version win .. but the technical details don't matter.
21:22:47 Von Heather Vescent an Alle: LOL, yes, I give up. Everyone will do their own thing and there is nothing we can do about it.
21:22:51 Von fundthmcalculus an Alle: +1 to MSFT understanding devs.
21:23:14 Von Bart Suichies an Alle: To the earlier point on product-thinking: Do we have joint metrics for success as a community? (as in x million credentials issued, xx million users, etc)
21:23:21 Von Heather Vescent an Alle: Those who want to do introp will, but many others will not, and a whale could completely overturn all smaller efforts.
21:23:52 Von evanwolf an Alle: IBM (1940s to 2000) used to wait until a market was big enough (about a billion dollars annually) before entering a space. Then would overwhelm the pioneers with better sales forces, scale, business operations, and brand trust.
Today there's a chance for small players in a new space to redefine things and get scale before incumbents can respond (Zoom comes to mind).
21:24:21 Von Kaliya Identity Woman an Alle: more about DIVOC - https://www.lfph.io/2021/10/13/divoc/
21:24:56 Von evanwolf an Alle: The point of interop in a nascent space like this is to reveal our hidden assumptions and to converge on better architectural and governance choices.
21:25:08 Von Lucy Yang an Alle: https://www.lfph.io/2021/10/12/global-covid-certificate-landscape/
21:25:21 Von Darrell O'Donnell an Alle: DIVOC = COVID backwards too
21:27:01 Von Judith Fleenor(ToIP) an Alle: +1 Human to Human communication!
21:27:10 Von Heather Vescent an Alle: If you are interested in other standards orgs - Andrew Hughes is doing a presentation on mobile drivers license using ISO standards.
21:27:30 Von Balazs Nemethi (DIF) an Alle: +1, there is a change DIF will come up finding ways to speed up certain test suit developments. :)

21:27:40 Von evanwolf an Alle: "IIW Opens Hyderabad Embassy"
21:27:43 Von Judith Fleenor(ToIP) an Alle: What time his Andrews session, I thought it was early this AM.
21:27:45 Von Judith Fleenor(ToIP) an Alle: ??
21:27:53 Von Darrell O'Donnell an Alle: Andrew is doing Part 2
21:28:05 Von Darrell O'Donnell an Alle: 1:30pm PT - Room A
21:30:31 Von Kaliya Identity Woman an Alle: what is wrong with the DIF interop
21:30:33 Von Bart Suichies an Alle: The great thing about SVIP is that is was a forcing function.
21:30:35 Von Kaliya Identity Woman an Alle: we meet every week!
21:30:41 Von Heather Vescent an Alle: I can offer the CCG at the W3C.
21:30:43 Von Hakan Yildiz an Alle: Nothing its great 😁
21:30:49 Von Sandeep Bajjuri an Alle: @evanwolf: I am surprised to see the name of the city I come from. What do you mean by IIW opens Hyderabad Embassy
21:30:57 Von Heather Vescent an Alle: We have a strong track record of technical discussions.
21:31:01 Von Balazs Nemethi (DIF) an Alle: Indeed, Interop WG meets every week
21:31:14 Von Balazs Nemethi (DIF) an Alle: Let's repurpose accordingly!
21:31:21 Von Balazs Nemethi (DIF) an Alle: (Yes there is mailing list)
21:31:26 Von Juan from Spruce an Alle: ALL?
21:31:27 Von Heather Vescent an Alle: No, not all stakeholders are in DIF.
21:31:27 Von Lucy Yang an Alle: Probably finding one place to discuss this is as difficult as finding one standard for interoperability :)
21:31:32 Von Heather Vescent an Alle: And also DIF doesn't do standards.
21:31:38 Von Bart Suichies an Alle: :D +100 Lucy
21:31:48 Von Heather Vescent an Alle: SVIP interoperability doesn't do their work in DIF
21:32:06 Von Bart Suichies an Alle: like companies, communities also ship their org-chart
21:32:15 Von Juan from Spruce an Alle:^^
21:32:24 Von Heather Vescent an Alle: +1 to Andreas inviting everyone to *your* meeting
21:32:30 Von Bart Suichies an Alle: you cannot be a community about decentralization and expect to align on 1 standard :)
21:32:31 Von Michael Shea an Alle: +1 to DIF group
21:32:34 Von ChrisKelly (DIF) an Alle: https://lists.identity.foundation/g/interop-wg/
21:32:36 Von Hakan Yildiz an Alle: +1 as well
21:32:37 Von Kaliya Identity Woman an Alle: DIF interop group does not "do" standards development
21:32:54 Von Kaliya Identity Woman an Alle: SVIP is mandating standards development for key interop things that is happening at CCG
21:32:59 Von Kaliya Identity Woman an Alle: which is great
21:33:01 Von Kaliya Identity Woman an Alle: all needed
21:33:09 Von Juan from Spruce an Alle: VC-API, for example, NEEDS IPR
21:33:15 Von Juan from Spruce an Alle: API design is very patentable
21:33:29 Von Juan from Spruce an Alle: but interop PROFILES, testing harnesses, etc don't
21:34:07 Von Juan from Spruce an Alle: SVIP defines interop as a royalty-free, common, open API
21:34:22 Von Kaliya Identity Woman an Alle: So - lets have you come and present in the next few weeks.
21:34:30 Von Bart Suichies an Alle: Well that's sorted then ;)
21:34:38 Von Charles E. Lehner an Alle: Thank you for the session. You might want to copy-paste the chat log into the notes
21:34:42 Von Richard Esplin an Alle: Thanks for leading a lively discussion!
21:34:43 Von Juan from Spruce an Alle: BART ON DIF INTEROP
21:35:08 Von Balazs Nemethi (DIF) an Alle: To get an introp wg invite, shoot me an email to balazs@identity.foundation

DID Registration Architectures

Wednesday 12C

Convener: Markus Sabadello, Azeem Ahamed, Cihan Saglam
Notes-taker(s):

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

https://dev.uniresolver.io Universal Resolver (via DIF) Resolve-a-DID
https://uniregistrar.io Register-a-DID: Create / Update / Deactivate

Since DIDs can be in many forms (on the blockchain, a file system, etc) how do you architect this registry?

Work started on https://identity.foundation/did-registration with CRUD methods that seem to be architecture neutral.

Strategies For Bridging to Next-Generation Identity Systems (from the bottom up)

Wednesday 12D
Convener: David Schmudde
Notes-taker(s):

Tags for the session - technology discussed/ideas considered: #OAuth, #OIDC, #VCs, #schema

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

Session Slides: https://schmud.de/download/bridging-to-next-genid-systems.pdf

Zoom Chat Window:
20:23:35 From Joe Hsy To Everyone : +1 on relationship vs identity
20:29:48 From Bogdana Rakova To Everyone : +1 on relationship vs identity too! I'm deeply involved in work on ethical/trustworthy/responsible AI and recently worked on a proposal for a 'relational view on ethics of AI' and think the bottom up efforts in our field has recently been present in media, and I wonder what do you think is the intersection between the IIW community and the ethical AI work? What relationships exist and how do we help make them stronger through a bottom up approach?
20:32:38 From Robert To Everyone : I would add that actually to maintain relationship you need to have proper identification not necessary identity. Means if I prove the the store that I bought already 10 times is equvalent to having "stable" relationship under some identifier/session
20:32:46 From Robert To Everyone : so identification vs identity
20:34:51 From Joe Hsy To Everyone : Risk of reidentification becomes greater the more VC and other data is gathered.

20:36:23 From Dan Robertson (he/him) To Everyone : I've heard it suggested that bulk address updates are an example of something that could be made very low-friction once DIDComm is widely adopted
20:40:47 From Dan Robertson (he/him) To Everyone : In addition to the info collected being more reliable (verifiable) than if the consumer filled out a form, it should also be much lower-friction for the consumer to provide. e.g. One-click checkout should be possible even the first time visiting an e-commerce site
20:42:13 From Padungkiat Tamasee To Everyone : How to find the side link please
20:42:49 From Bogdana Rakova To Everyone : @Dan, could you say more about what kinds of verification do you envision?
20:42:59 From Bogdana Rakova To Everyone : From the standpoint of the consumer
20:47:39 From Dan Robertson (he/him) To Everyone : @Bogdana, I think that theoretically (once SSI is more widely adopted) a consumer could present a ZKP that proves some issuer (e.g. local government) had given them a VC that asserts the consumer's home address (for shipping). They only disclose the "address" attribute of the VC.
20:51:33 From Bogdana Rakova To Everyone : Thanks!
20:57:58 From Dan Robertson (he/him) To Everyone : Amazon is exactly who does not want this kind of innovation, because it will erode their moat (competitive advantage) built up over decades of customer acquisition and customer relationship management. However, the long tail (vendors on Shopify, WooCommerce, Squarespace, etc) of e-commerce merchants could benefit from a network effect of all supporting the same standard and allowing for instant customer onboarding (once a user has setup to use SSI for shopping on any other site already).
21:03:26 From Robert To Everyone : https://media.sitra.fi/2018/12/22091907/ihan-blueprint-2-5.pdf
21:08:03 From Robert To Everyone : https://oca.colossi.network/
21:10:24 From Joe Hsy To Everyone : @Dan, agreed form Amazon perspective that they won't want to erode their competitive advantage. If the 2nd tier and long tail vendors can share data and user experience in a safe way, it could provide similar kind of consumer benefits. It will be challenging though.
21:11:45 From Joe Hsy To Everyone : What could be interesting to track is the trend toward DTC (direct to consumer) vendors and how they are successful.
21:13:13 From Dan Robertson (he/him) To Everyone : There is some consumer benefit as well, if the UX is good and onboarding only needs to happen once. I'd love to buy from other merchants more often — but don't want to create account, enter shipping info, add credit card, etc. at a store I've never shopped at (unless I have to). Amazon gets my business even when I wish they didn't.
21:14:24 From Robert To Everyone : maybe worth to mention is that eIDAS 2.0 would introduce digital wallet specification which means in EU people not only would have digital identity but as well "own" walllet which can serve as this gateway towards services - and you already onboarded ...
21:14:26 From Joe Hsy To Everyone : "Amazon gets my business even when I wish they didn't." - I can relate to this feeling. Also Costco.
21:15:36 From Robert To Everyone : what I found interesting is that solution which I am mentioning is supper interesting for SMEs since they can't compete with amazon or ebay and they need to find a way through so they are eager to try new solutions
21:15:57 From Robert To Everyone : amazon for sure would not be super happy to support stuff like that :)
21:16:10 From Robert To Everyone : maybe alibaba would since they have siilar way of thinking about supporting SMEs
21:17:29 From Joe Hsy To Everyone : Actually, I can see Amazon doing this if they can still play a critical role.
21:19:15 From Robert To Everyone : They for sure would try

Some problems with JSON-LD and Content Based Addressing

Wednesday 12E
Convener: Burak Serdar
Notes-taker(s):

Tags for the session - technology discussed/ideas considered: JSON-LD, RDF, JSON, digests

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

Main points

- JSON-LD is not namespaces for json
- @context does not enforce structure. It is a key mapping
- @context does not define the semantics, it defines mapping to a terminology
- JSON-LD is extremely difficult to understand and debug.
- Readability ≠ Clarity
- JSON data is usually self-explanatory without processing.
- Go Motto: Clear is better than clever (https://dave.cheney.net/2019/07/09/clear-is-better-than-clever)
- Expanded JSON-LD might be more workable in the VC domain, but then, it is JSON
- Content based addressing (digesting)
    - Normalized representation
    - Self-contained (i.e. digested object should not have external links)
- Is normalization really necessary? I believe it is not. Treat JSON as a BLOB, no normalization
- Hashing self-contained objects is the key (e.g. no external @context)
    - There are ways of doing that even with external references
    - Manifests: JSON file pointing to all references

Other discussion points:

- SAIDs: A SAID is equivalent to an envelope containing hash and payload.
- Layered schemas example: weak-references to schemas (IRIs), strong references to schemas (digest)

Link to the document shared during the presentation:
https://docs.google.com/document/d/1IS8tOcrVvL2PcvzPk0JAYnZIVtcHsaXmyObk0bYA5TY/edit?usp=sharing

Link to the slides:
https://docs.google.com/presentation/d/1mrj2DiDGhASNfGY788odm-Mm3kABdqFUdegLAxePmWA/edit?usp=sharing

12:20:43 From Timothy Ruff : The problems with JSON-LD for VCs are many, both for security and semantics, and are detailed in Dr. Sam Smith's paper here:
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/VC_Enhancement_Strategy.md

12:23:07 From Timothy Ruff : For these reasons, GLEIF is not compatible with 1.0 of the W3C spec, but is compatible with 0.9. Here is their position paper about why:
12:23:28 From Brian Richter : @Timothy the vc spec ya?

12:23:45 From Timothy Ruff : Yes! Label Proper Graphs are the way forward.
12:23:59 From Timothy Ruff : @Brian - Yes, I meant the VC spec
12:25:22 From Timothy Ruff : If you guys read Sam's paper linked above, you'll have all the reason you need to avoid JSON-LD completely. The presenter is 100% correct: you only need JSON, JSON schema, and LPGs (label property graphs).
12:25:36 From Dmitri Zagidulin : Timothy: that paper is full of FUD, though..
12:25:58 From Timothy Ruff : That sounds like FUD. Need to be specific, refute Sam's points.
12:26:29 From Timothy Ruff : Sam backs up every point with references. FUD doesn't provide references.
12:27:51 From Timothy Ruff : This presenter is independently coming to the same conclusions, for the same reasons.
12:28:41 From Brian Richter : I have also started to come to these conclusions on my own
12:29:41 From Brian Richter : I believe there's some parts of jsonld that can be saved though
12:30:02 From Timothy Ruff : Gotta run to another session. When I saw what this was about, I wanted to share these docs and head back. Done. Have fun debating the "FUD"! :)
12:37:37 From Dmitri Zagidulin : have hashlinks (the IETF draft) been considered for SAIDs?
12:37:55 From Kyle Den Hartog : https://github.com/kdenhartog/context-integrity
12:38:05 From Kyle Den Hartog : That's the path I started working down
12:39:02 From Dmitri Zagidulin : nice, thanks Kyle
12:50:24 From Dmitri Zagidulin : I think I'd argue with the "JSON is self-explanatory" :)
12:53:43 From Brian Richter : I've seen a lot of "name" properties meaning a lot of different things
12:54:07 From Kyle Den Hartog : https://www.iana.org/assignments/jwt/jwt.xhtml
13:16:47 From Nuttawut (Finema) : Question: Does Sam Smith's paper propose an alternative to JSON-LD?
13:20:32 From Dan Yamamoto : I agree with too-much complexity of JSON-LD/RDF ... but at the same time prefer its ability to combine heterogeneous documents issued by multiple issuers. Hope there might be kind of lightweight format with LD functionality in simpler way
13:24:04 From Burak Serdar : https://dave.cheney.net/2019/07/09/clear-is-better-than-clever

DIDComm Messaging with LibP2P

Wednesday 12F
Convener: Oliver Terbu and Alan Horvat
Notes-taker(s): Oliver Terbu

Tags for the session - technology discussed/ideas considered:

DID, DIDComm, libp2p, IPFS

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

Slides can be found here: https://docs.google.com/presentation/d/1rVbP5-YE7rz0yEGDMtKxeL6XWRGgPWn4KhujaaA0iPs

Get involved and reach out to the hosts of the session on either LinkedIn or DIF Slack.
References:

- https://identity.foundation/didcomm-messaging/spec/
- https://libp2p.io/

DID Tethics & Mandatory Vaccine Passports

Wednesday 12G
Convener: Timothy Holborn
Notes-taker(s): Amanda Jansen

Tags for the session - technology discussed/ideas considered:

In preparation for putting forward the session topic concept, I've made a few notes.
These are provided below (TCH NOTES: #NoMandatoryVaccinePassports)
The Main purpose of the session is to give space to the global issues linked to 'vaccine passports' exhibited world-wide. The intention is to operate the session as a round-table.
So I'll be trying to ask questions, to hear what people's views & concerns are, etc. #Humility.

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

DID Tethics & MandatoryVaccinePassports
#NoMandatoryVaccinePassports?

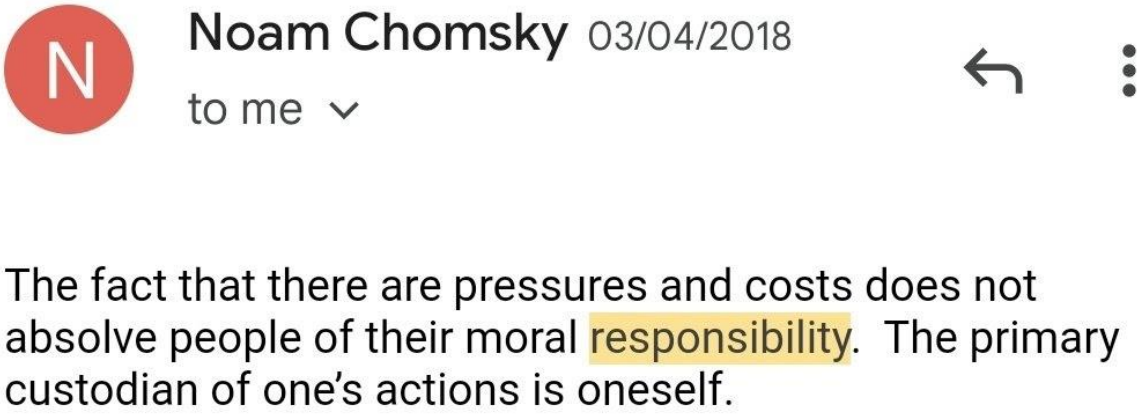
"I disapprove of what you say, but I will defend to the death your right to say it."
— S.G. Tallentyre

Summary

This session is intended to respond and provide space for persons who do not support Mandatory Vaccination Passports, as are being rolled-out around the world, impacting the human rights of many.

The Concept of 'Identity' has a few different meanings; therein, this discussion looks at the effect of our work, our behaviours upon others throughout the world and provides support for people to think about what that means in relation to their identity, as 'identity infrastructure' is deployed as a consequence of our choices.

Below I have provided a bunch of input, relating to my thoughts on the problem domain. The group is encouraged to provide their own contributions also, as a means to catalogue dissenting views with respect to the global (mostly western world?) impacts of VaccinePassport Agendas impacting the lives of billions of members of our human family in very troubling ways.



https://twitter.com/DemocracyAus/status/1447925073650794516

Tethics (Silicon Valley Clip): https://www.youtube.com/watch?v=nfRUQh_EHoQ

What does this have to do with DIDs, Verifiable Credentials, Etc.?

DIDs - First W3C Post: https://lists.w3.org/Archives/Public/public-webpayments/2014May/0033.html
Post RE: Establishing Credentials CG: https://www.w3.org/community/credentials/2014/08/06/call-for-participation-in-credentials-community-group/

DIDs Current Issues: Formal Objections by Mozilla, Google & Apple.

- https://lists.w3.org/Archives/Public/public-credentials/2021Oct/0045.html
- https://lists.w3.org/Archives/Public/public-credentials/2021Oct/0053.html

Historical Suggestion re: Healthcare industry: (2015) https://soundcloud.com/ubiquitous-au/credentialscgtelecon2015-06-02medical (from: https://opencreds.org/minutes/2015-06-02/)

Which led to: https://web.archive.org/web/20210227133444/https://w3c-ccg.github.io/meetings/2016-04-19/ (UN / ID2020 → original link taken down: https://w3c-ccg.github.io/meetings/2016-04-19/#topic-2)

The history of how these works evolved is different to the version of history promoted by 'DID/CREDENTIAL trust vendors".

It appears the global Interoperable Platforms for 'Vaccine Passports' is built on Credentials / DIDs

- California (first) https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201920200AB2004&showamends=false (old links associated to it now unavailable)
- https://github.com/decentralized-identity/healthcare/blob/main/agenda.md
- https://fpf.org/wp-content/uploads/2020/10/10-CovidCredentials.pdf
- https://www.covidcreds.org/
- https://thecommonsproject.org/newsroom/press-release-commonpass-trustassure-and-affinidi-announce-global-solution-for-end-to-end-health-status-verification-for-international-travel
- https://www.ibm.com/watson/health/resources/digital-health-pass-blockchain-explained/
- https://vci.org/about
- https://docs.microsoft.com/en-us/azure/active-directory/verifiable-credentials/decentralized-identifier-overview

IS COVID19 DANGEROUS? Most Certainly….

- PATHOLOGY https://youtube.com/playlist?list=PLCbmz0VSZ_voaBc3BRgHWCkrLKaS3Qa_6
- Medical Lectures: https://www.youtube.com/playlist?list=PL_voXEIX5Xhvo-4N-Wg7rFuG7JwY8AOHp
    - https://www.springer.com/gp/book/9783030220938
- JohnHopkins Tracker: https://www.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6
- Google Statistical Information: https://www.google.com/search?q=google+global+covid19+deaths (~4.5m people).
- https://www.google.com/search?q=global+population+2021

It is believed the majority of deaths have occurred to persons above the average life expectancy. https://ourworldindata.org/life-expectancy

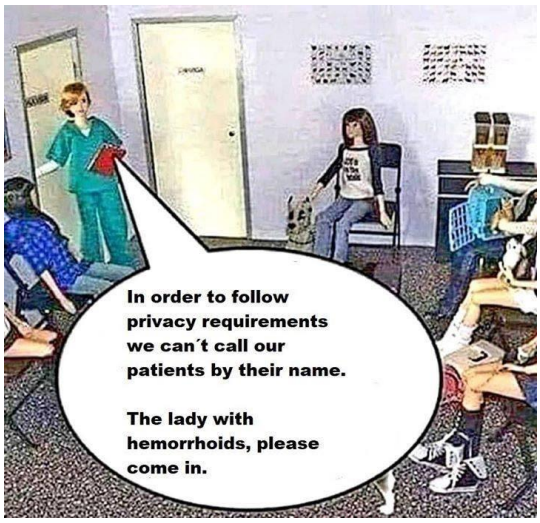
Are All Systems of providing access to health-care the same world-wide? No.

Australia has a Medicare system that provides a medical identifier and free access to the vast majority of health-services required to support basic needs. Pharmaceuticals generally cost ~$6 for those in poverty.

Other places (like the USA) are believed to have a very different system of healthcare with different problems.

A few Medical Information standard compatible with 'Credentials' has been produced

- https://www.snomed.org/
- These medical ontologies have been mapped to SchemaOrg for SEO https://github.com/schemaorg/schemaorg/tree/main/data/ext/health-lifesci
- Will your medical circumstances (or indeed also, false statements in records? Or bad data?) end-up being part of the knowledge about a person that is distributed globally for commercial employment by corporations world-wide?
- Should your local media provider store your health profile? https://www.bbc.co.uk/rd/blog/2021-09-personal-data-store-research



Suggestion: Get a Smart Watch and Health App stuff. Lots going on, lots of low-stakes use-cases.

Are the principals employed to support 'privacy', being deployed to support 'dignity enhancing' outcomes for human beings?

Human Rights - Have VaccinePassports (DID commercialisation) led to Crimes Against Humanity?

What is the role of technologists to support the rights '*granted by birth*' for all mankind?

What are crimes against Humanity?
Source: https://www.un.org/en/genocideprevention/crimes-against-humanity.shtml
According to Article 7 (1) of the Rome Statute, crimes against humanity do not need to be linked to an armed conflict and can also occur in peacetime, similar to the crime of genocide. That same Article provides a definition of the crime that contains the following main elements:

1. A physical element, which includes the commission of "any of the following acts":
    1. Murder;
    2. Extermination;
    3. Enslavement;
    4. Deportation or forcible transfer of population;
    5. Imprisonment;
    6. Torture;
    7. Grave forms of sexual violence;
    8. Persecution;
    9. Enforced disappearance of persons;
    10. The crime of apartheid;
    11. Other inhumane acts.
2. A contextual element: "when committed as part of a widespread or systematic attack directed against any civilian population"; and
3. A mental element: "with knowledge of the attack"

3 billion people locked down
https://www.weforum.org/agenda/2020/03/todays-coronavirus-updates/
Q: how could this have been brought about before broadband & smartphones?

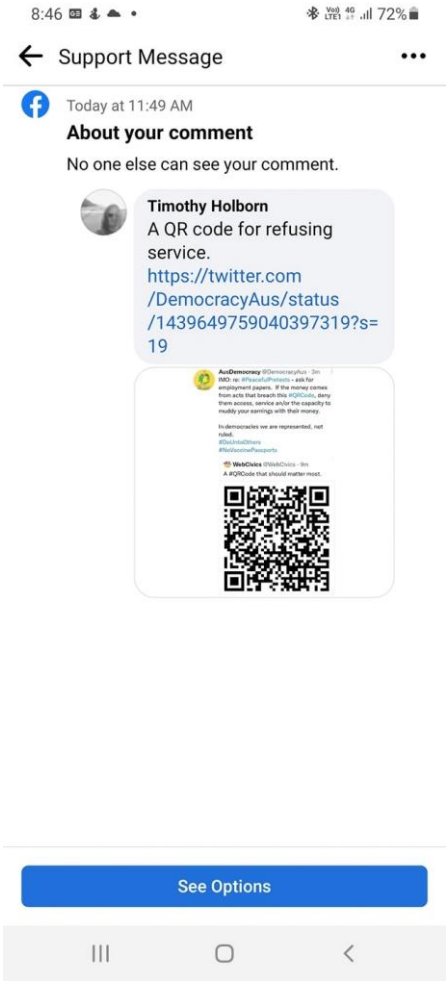
'Locked Down for more than 267 days' https://www.theguardian.com/australia-news/2021/oct/02/how-melbournes-short-sharp-covid-lockdowns-became-the-longest-in-the-world

Breaches to HealthOrders warrant Violence: https://twitter.com/search?q=%23VicPolViolence
Alleged Crimes; protesting, not wearing a mask, making social media posts that criticize measures, etc.

- https://twitter.com/search?q=%23NoVaccinePassports
- https://twitter.com/search?q=%23NoVaccineMandates
- https://twitter.com/search?q=%23ApartheidDay
- https://twitter.com/search?q=%23CrimesAgainstHumanity
- https://twitter.com/search?q=%23protest
- https://twitter.com/hashtag/Freedom
- https://twitter.com/search?q=mask%20children

Censorship & manipulation.
UDHR Considered by Facebook to breach its community guidelines
LINK: https://twitter.com/DemocracyAus/status/1439649759040397319

Penalty dished-out by Facebook.



It is now safer to communicate via MEME: https://photos.app.goo.gl/gvjkAq7mTSP6oxaU8

There's countless examples of persons being targets of 'fact checkers' making wrongful decisions, people who are illustrating obvious signs of mental illness being penalised online, whilst 'locked down'.

Increasingly, it is said that persons are not allowed to participate in society without a 'vaccine passport'. The implications include people losing their jobs (employment / income), ability to go outside, ability to go to government buildings, retailers and much more. These initiatives appear to be synchronised world-wide in their deployments, they appear to depend upon a mobile app to support policies.

Whilst the biosphere and all flora / fauna have developed over millions of years; within a decade of mobile apps, it appears we are coercively required to accept that our lives are void without carrying with us a mobile app. These policies could not have occurred earlier.

Arguably, if the infrastructure for COVID (Testing Facilities, Work related 'health credentials', etc.) were deployed to drug-test every person whose gainful income for work was sourced via TaxPayers Funds; there would be a significant impact on organised crime, mental health, improved decision making; and, i speculate, the lives of more children and working age adults would be 'saved' than the same policy deployed against COVID-19. Part of this is in-turn also, about the importance of rule of law - if the laws of the people are not suitable for the jurisdiction, then, they should be changed to be made appropriate. Where this applies to drug-affected decision making (about the lives of others); it may then become a mental health issue. Yet, the underlying reality is - even though it is illegal for public servants to illegally purchase, consume and attend work drug-affected (making decisions about the lives of others); it is entirely unlikely any meaningful action will ever take place to sort this problem out.

So, are the measures put upon society world-wide about Health, Welfare, Safety & Rule Of Law?

There are also significant implications for SiliconValley. Increasingly people are migrating away from traditional platforms in protest of the applied theology put upon the means for locked-down people to communicate. Presently, the biggest problem is a lack of alternatives, this is likely the subject of WIP.

California may have provided an opportunity to produce a Global Social Graph,.

- https://en.wikipedia.org/wiki/Alien_(law)
- https://www.google.com/search?q=daml%2Boil
- https://www.youtube.com/watch?v=9zXqHIJJVxk
    - Source: https://www.youtube.com/watch?v=sKOk4Y4inVY

DESIGN IMPLICATIONS:
There are many, many different potential applications for Verifiable Claims, Verifiable Credentials, Decentralised Ledger Technology Records (ie: diversification from HTTP/s).

What are HumanRights?

- https://www.un.org/en/about-us/universal-declaration-of-human-rights
- Video Versions: https://www.youtube.com/playlist?list=PLCbmz0VSZ_vrquCoCDtBpVIYLAdTfqhVH

Some links to UN Human Right Documents (and a few associated to AU)

Human Rights Links:

https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination

Commonwealth Charter: https://thecommonwealth.org/about-us/charter

QLD Act: https://www.legislation.qld.gov.au/view/whole/html/asmade/act-2019-005

ACT Act: https://www.legislation.act.gov.au/a/2004-5/

VIC Act: http://www5.austlii.edu.au/au/legis/vic/consol_act/cohrara2006433/

Universal Declaration of Human Rights:
https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=eng

International Covenant on Civil and Political
Rights: https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment
https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-9&chapter=4&clang=_en

Convention on the Rights of the Child:
https://www.ohchr.org/en/professionalinterest/pages/crc.aspx

Convention Relating to the Status of Stateless Persons: (cannot find link)

COMMITTEE ON THE RIGHTS OF PERSONS WITH DISABILITIES
https://www.ohchr.org/EN/HRBodies/CRPD/Pages/ConventionRightsPersonsWithDisabilities.aspx

RE:DEFINE DIGITAL IDENTITY?
(Human Agency, AI Ethics & DigitalTwin Semantics of Natural Persons)

- https://www.webizen.net.au/about/references/social-informatics-design-concept-and-principles/
- https://medium.com/webcivics/humancentricwebecosystems/home
- https://www.slideshare.net/Ubiquitousau/
- https://www.youtube.com/playlist?list=PLCbmz0VSZ_vr9VW6CjOqyYVedHw_Ql2fa

Human Centric – DID Related Applications

- How can Credentials support the means for people to have evidence about facts relating to their activities as to support their human agency, personhood.
    - Digital Receipts
    - Digital Payslips
    - Transcripts of Interactions / Conversations
    - *Minted* AI Semantics (with a particular vendor who may develop 'trustworthy' reputation)
- Decentralising 'Biosphere' 'Commons' information
    - Creating ledgers that decentralise the storage and distribution of key 'commons' artifacts, not on one ledger; but on many, with different permissions that create 'corpus' digital twins around subject-matter areas of expertise; and, means to form inference between different topical ledgers (ie: jurisdictional considerations in Australia having semantic relationships to similar constructors in other jurisdictions, such as the United States, UK, etc.)
    - Biosphere Information
        - Botany

Societal Infrastructure

- History
- Languages
- Human Rights Charters
- Collaborative Projects - Producing modern work infrastructure to support Workers Rights in relation to contributions (both benefits & responsibilities)
    - https://docs.google.com/drawings/d/1oUsSlPEh8erOdkQJCLzFHBaqp7AYOJCqDw82YrCg9f4/edit?usp=sharing
    - https://www.tandfonline.com/doi/full/10.1080/01442872.2020.1724926

- Improved 'temporal' support, including both provenance & the ability to support temporal informatics, etc.
    - People who are attacked by others are rarely prepared. As such, further information is often made available later, down the track.
    - An ideological decision could be made about which modality is preferentially supported to support 'good faith' relations; therein, how to address issues such as usury (or afore mentioned 'digital slavery', etc.).
        - https://drive.google.com/file/d/0Bz_os8GdvH2nUGR3TERGMzJnNVU/view?usp=sharing&resourcekey=0-w9A9cKD7plKm6yBc-yjtHA
    - So, the ability to add 'verifiable claims' that may relate to historical circumstances has a role or opportunity to impact what can be considered a beneficial form of conduct.

- STEM Commons
- Browser Plugins to Snapshot a page, and turn it into a DID supported Verifiable Claim artifact.
- #RealityCheckTech

Pre-session noted – Conclusionary Remarks:
Pink Floyd, Turning Away 2021 remix: https://www.youtube.com/watch?v=i2C8YiT_9nQ

The works produced via W3C, over about a decade, have a plurality of different, very positive applications. However, it is my position that if we decentralise ICT Power to support many different groups participating in different ways, as is required at this time when our libraries go digital; there are moral and ethical questions, burdens and common-sense requirements. Whilst i support the growth of Credentials, DIDs and related ecosystems linked to frameworks i believe can support 'identity fabrics' or 'inforgs' that have a far different type of interpretation of 'identity', made via w3c in ways that are already fairly-well supported technically by many major US platforms (Facebook, Google, etc.),

I do not support Mandatory Vaccine Passports. I am mortified by the choices that have been made, the functionality that has been delivered and the very significant volume of use-cases (protecting citizens, human rights, rule of law, access to justice, fair-pay-for-good-work) that has been broadly set aside.

Few links about historical (web) Concepts

- https://videos.cern.ch/record/2671957
- https://www.youtube.com/watch?v=4RiWgiBT5bs
- My Video (Christmas day 2016 as was prepared for: https://2017.trustfactory.org/ https://www.youtube.com/watch?v=e9vROTibKiE&list=PLCbmz0VS

Z_vr9VW6CjOqyYVedHw_Ql2fa&index=2 providing some considerations that may help 'inference' a different identity concept?

Some of Manu's Old Credentials Docs Links
AUG 2014: https://docs.google.com/drawings/d/17mfHu4EqsnZQ2eFI115qC8FUuLOX-ZSnWpCjo7q1Vlc/edit
October 2015: https://docs.google.com/presentation/d/1644G7jJZbUTpyEGALWj6t4m5kJc-bt90QCfRmW5IRuk/edit#slide=id.p
https://docs.google.com/presentation/d/1ithW3t-ahelw_0jsAbVmhXi5NyRl_-BAW6hMnJmoixc/edit#slide=id.p
March 2016:
https://docs.google.com/document/d/1dYup3KC2nak3LVTzyapr996TKxDj1w5Eyp4g13rQQBA/edit
June 2016: https://docs.google.com/presentation/d/1mL0MsPpdxdKiYFWVIyGVOFzypBsjylxepACN2MYw-yg/edit
Sep 2016:
https://docs.google.com/presentation/d/1pFGC1G7CbizUuvbmjECfnNRL4fZk9QLxG8d3nehgwNU/edit
OCT 2016 IIW (IIW 23)
https://docs.google.com/presentation/d/1pY6TGsCBzmui_KVM5Q71t1LbHgdv10vRPov7SoISjqU/edit
https://docs.google.com/presentation/d/1BsGY6YOlkfTQQyxm0jJadxBhJwBCE3QLDoyRENzhS0k/edit
April 2017:
https://docs.google.com/presentation/d/13ztihmZSl7nIBW2TuJxgkNmwFcOjOFvxSDAQ0ACiyYg/edit
Nov 2017:
https://docs.google.com/presentation/d/1woq0pZD872NvhBIu90GIZMf8MQLWCtXM1NCx8n6s0VM/edit

Some of My Old Docs
Sep 2014: https://docs.google.com/drawings/d/1oUsSlPEh8erOdkQJCLzFHBaqp7AYOJCqDw82YrCg9f4/edit

May/June 2015:
https://docs.google.com/document/d/1pRtTu9EssjhyyK3qkQymZepIUkqCwvMo6imnr4fqsrg/edit

Jan 2016: https://docs.google.com/document/d/1pzZJ-pb-luy0jNryY2lrfJUNntjDGNm4-2wXKt72C6k/edit
ADD YOUR OWN COMMENTS, LINKS, ETC!!

Transcript / notes
Present:
Timothy Holborn https://www.webizen.net.au/

Amanda Jansen https://www.linkedin.com/in/jansenam/

Jan Rietveld
https://janrtvld.nl/
https://twitter.com/jan_rtvld
https://www.linkedin.com/in/jan-rietveld/
Simon Nazarenko
https://www.linkedin.com/in/slavanaz/

Round table discussion.
Motivation: some of the discussions on the concept of identity: going back to the original presentations and objectives and see what happened afterwards & moderate a conversation about it

Simon: third month working on some solutions for issuing credentials; lacks possibly a deep understanding of the theory behind it.

Timothy: It is about ethics. A group makes ethical choices and an individual makes individual moral choices. People in the world are locked out of individual rights, there are protests etc. and is this the way to go about it through technology?

Simon: this can go really deep and political / philosophical really soon. It is the government trying to create a situation of health and temporarily create solutions and even perhaps try to save lives, but not necessarily acting in the line the technology was meant for.

Technology, philosophy, politics: three topics that are relevant here.

Timothy: showing a presentation.
https://docs.google.com/document/d/1t1LnjnnU8JW8rfNsunPx80cyCblAXjkGnFEchYrj3dY/edit
https://www.iana.org/assignments/uri-schemes/prov/did
https://lists.w3.org/Archives/Public/public-webpayments/2014May/0033.html

First thing we can do is look at the original intention of the technology:

1. Save the lives of millions of people.
2. Banking the unbanked.
3. Use verifiable claims.

How do vaccine passports improve the lives of people? Have the original goals been met? Are there ramifications for what is now happening?

What is our role and responsibility as technologists?

Simon:
I will try to express my opinion and experience. I am based in Idaho, but am from Ukraine. Here are my thoughts about the technology. Ukraine, I don't know how much you follow the news lately, but Ukraine was part of the Soviet Union for quite a bit. But now we are considered to be living in a free Ukraine, which is for over 20 years. We have multiple elections going on which were not very successful and led to revolutions. One time we ended up having the Soviet Union invading certain parts of Ukraine. We still fight, but officially it is not a war. Our president had to flee and a new president was democratically chosen. In the meantime we had several crashes going on amongst which an economic crash. Just recently after new elections a new digital ministry was started. The goal was to convert all of the paperwork that is circulating in our country to digital work for the general citizen to be able to get digital certificates. The transition from paper to digital: the problem with this approach done on the government level is: go digital or stay with paper. The credentials are not owned by the people, but by the government. I.e. your driver's licence is not yours, but your government's. There are some credentials that are issued by your government and there are credentials that are owned by people. We have huge discussions about this also in the tech community.

A self sovereign approach would be to put the credentials on the ledger and have them verified on request. It will be really hard to change the minds of people to make them trust this new technology and realise the credentials are theirs.

Timothy:
It is not really the case that you are not forced to present those credentials. You won't get certain information or credentials from institutions or the government. Government has not produced infrastructure to provide evidence or information and credentials to citizens. The consequences are punitive to citizens. It seems like there is an implication or gap between what is the vision or what these self sovereign credentials are doing and what they are doing in reality.

Simon: Would you like to have all the information you just mentioned handed over to citizens?

Timothy: You cannot access justice without evidence. That evidence should be accessible to citizens as well as police i.e. government institutions.

links: https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-digital-revolution-is-gaining-momentum/
https://www.capgemini.com/au-en/2020/08/three-perspectives-on-government-as-a-platform/

Simon: Can you show how a citizen is discriminated against by the evidence that is provided? Is there a specific use case?

Timothy: showing a link.
https://www.theguardian.com/australia-news/2021/jun/11/robodebt-court-approves-18bn-settlement-for-victims-of-governments-shameful-failure

Showing the robodebt link of a vital accident in providing proof in Australia harming about 2000 people. The answer to that was to make machine readable payslips in order to show how much you have spent of your benefit and whether or not behaviour was fraudulent.

Ability for workers to do accounting. Ability for people to comply with what is being expected of them.

Doing good & inforgs information.

An inforg as opposed to identity: representational identifier for making verifiable claims.
Continuing the presentation: citizens should have their own information about what happens and not be asymmetrically dependent on government institutions.

Short presentation on knowledge banking as a solution.

Considering the impact of vaccine passports, lockdowns, protests etc.

Simon: demonstrating the 4th amendment of the US Constitution as a solution: mandatory vaccines: it may be decided on in court.

"The Constitution, through the Fourth Amendment, **protects people from unreasonable searches and seizures by the government**. The Fourth Amendment, however, is not a guarantee against all searches and seizures, but only those that are deemed unreasonable under the law."

Amanda: wonders how Simon feels the 4th amendment is being held firmly by courts right now, other effects and impacts are visible globally about constitutional rights in general in which rights are temporarily being set aside.

Tim: a digital twin should be owned by you as part of your human agency. Currently credentials are not being protected in such a way.

What happens if people cannot speak their truth and feel safe?
Life is not free.

Simon: asks Timothy's opinion about 'life is not free' and Elon Musk's strong opinion about basic income.

Timothy: I am not so much in favour of it. I will show you a page for discovering the vocabulary. Schema.org and showing more sites. It would be better to associate work with the benefit from it, then we would need no basic income.

Timothy: Privacy also considers the right to ensure information stored about a person is correct.
https://www.ag.gov.au/about-us/privacy-policy/accessing-and-correcting-personal-information

Timothy also noted:
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

KERI for Muggles - A Basic Intro to KERI IDs & Key Management

Wednesday 12H
Convener: Drummond Reed & Sam Smith
Notes-taker(s): Trent Larson

Tags for the session - technology discussed/ideas considered:

KERI, identifier management, 101

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

Presentation slides are here.

https://docs.google.com/presentation/d/1lpzYcPrIox9V4hERtn4Kcf7uq01OVU9u3PuVm1aYzR0/edit#slide=id.ga411be7e84_0_0

Aiming at 7 basic points in this talk. Go to KERI.one for everything. Summarized in one chapter from SSI Book https://www.manning.com/books/self-sovereign-identity

Sam developed this approach to fill in the trust layer of the internet, even between systems. White Paper

The python implementation of KERI can be found at https://github.com/WebOfTrust/keripy
... and the draft IETF spec will be published at https://github.com/WebOfTrust/keri

Point #1: It's based on public-private key pairs and self-certifying identifiers (SCIDs).

DID is a namespace. SCID is a type of DID. SAID is not a SCID, it's a content-addressable ID. (You could make a SCSAID.)

Benefit #1 - You can prove control of a KERI ID without relying on any external source (including blockchains)

Point #2: Self-Certifying Key Event Logs: keep a log of all keys, including rotated keys (which you might create ahead-of-time)

Benefit #2: You can again prove control of that key without relying on an external service.

Point #3: Witnesses for Key Event Logs: as you sign your key log events, you can have witnesses sign to record/attest those events.

Benefit #3: Witnesses provide additional evidence that the originator is consistent: both tamper- & duplicity- evident

Point #4: Pre-rotation as simple, safe, scalable protection against key compromise: KERI alone can't protect against compromised private keys, stolen by someone, but it allows for throwing away old keys.

- Log a whole series of public keys in your Key Event Log (KEL).
- Go into vault and get a private key & use it.
- Ack: someone stole it!
- Declare that key as compromised, go back into the vault and get the next private key (whose public key was already published in the Key Event Log) and use that from now on (either until the next compromise, or maybe you rotate on a regular basis).

Benefit #4: You can lock away your next private key, and have a provable path for use of the next keys
The key protection is post-quantum proof. A hash is published, not the actual public key.

Point #5: System-Independent Validation. There is no restriction on the number of logs.

Benefit #5: These IDs & keys are not ledger-locked, fully portable, and validated in multiple ways

Point #6: Delegated self-certifying identifiers, even for enterprise management. Keys can be delegated.

Benefit #6: Enterprises can scale and manage delegation hierarchies of any size & complexity

Point #7: KERI is compatible with GDPR "right to be forgotten"

When a DID is written to a public immutable ledger then that's a problem but KERI allows for erasure. Use witnesses that allow mutability.

Benefit #7: Doesn't require immutable ledgers.

The identity system on top of KERI has to manage things like whether you want the IDs to be private (not on blockchain!) or public.

Tim says that KERI helps with provable control... much like proof you own your email or phone with temporary links or Google Auth. We can now have provable control of our private keys.

There are two KERI sessions following this:
- Sam on "Privacy Authenticity Confidentiality Tradeoffs: KERI and Zero Trust Architecture"
- Phil on "Practical Intro to KERI: What can you do today?"

VCs Meet Reality - Custom VC Evaluation with Privacy

Wednesday 12J
Convener: Neil Thomson
Notes-taker(s): Neil Thomson

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

Slides for the session

Note: there were no attendees after 30 min so ended the session

ISO 18013-5 Mobile Driving Licences AND Verifiable Credentials - Even Better Together

Wednesday 13A
Convener: Andrew Hughes
Notes-taker(s): David Waite

Tags for the session - technology discussed/ideas considered:

MDL, Mobile Drivers License, ISO 18013-5, MDOC

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

Overview slides covering ISO 18013-5 mobile driving license are here - from Session 9A 5:30am PDT 2021-10-13:
https://docs.google.com/document/d/1FtWfULPqCyNqbXf3ekPlWs42LNjgWukPRaYCG5fPU10/edit?usp=sharing

Andrew reviewed the above deck, to provide an overview for those who are not familiar with the ISO standard.

Topic ideas:

- Issuer-controlled, restricted use credentials (a.k.a. mDL)
- Credential derivation from mDL
- Transport protocols for ISO 18013-5 mDL credentials

Important to remember these credentials, being state-issued, are legally restricted documents (to certain uses) and the property of the State.

Questions on Derived Credentials, to create credentials which do not have the same restrictions.

Do restrictions impact use for identity proofing - depends on whether that is defined as an official use.

Restrictions on official use are unlikely but a concern, and would push toward more derived credential use.

Apple has announced mDL will be going into the wallet, but has not announced ways to get them out to present them.

TSA is particularly conservative, and wants particular guarantees from their vendors when false negatives strongly impact security.

Selective Release vs Selective Disclosure - DW summarizes it as subatomic release, e.g. date of birth being released as an "over 20" value, rather than needing an "age_over_20" claim.

The Zoom Chat Transcript Follows:

13:31:39 From Andrew Hughes1 to Everyone:
https://docs.google.com/document/d/1FtWfULPqCyNqbXf3ekPlWs42LNjgWukPRaYCG5fPU10/edit?usp=sharing
13:31:45 From Kristina Y, to Everyone: why are you awake Naohiro?
13:31:51 From Vic Cooper to Everyone: Will you be recording this session?
13:32:57 From Juan from Spruce to Everyone: some of us have seen it and tried reading it quickly and still didn't understand it :D
13:33:15 From Naohiro Fujie to Everyone: @Kristina, good morning! I awoke now.
13:34:30 From Kristina Y, to Everyone: Juan, you need a lot of contxt, that's true
13:35:43 From Kristina Y, to Everyone: 23220 and 18013-5 and not dependant on each other in a simple statement
13:37:50 From Darrell O'Donnell to Everyone:
intended for Issuers - got it - but is it intended for Verifiers?
13:38:26 From Juan from Spruce to Everyone: one set of verifiers (law enforcement) are discussed a lot 🚘
13:40:33 From Darrell O'Donnell to Everyone: agree on co-existence
13:40:34 From Drummond Reed to Everyone: that's a pretty strong opinion, Andrew!
13:40:47 From Drummond Reed to Everyone: ;-)
13:41:15 From Darrell O'Donnell to Everyone: YES / NO / Maybe - as a strong "opinion"!
13:41:47 From David Waite to Everyone: Do not understate how strong of a maybe it is
13:42:08 From Drummond Reed to Everyone: Ha!
13:42:26 From Kristina Y, to Everyone:
funny how issuers cannot prevent secondary use in physical, but can in digital - by limiting access to the PKI only to the selected verifiers
13:43:11 From Juan from Spruce to Everyone:
germany is POCing left and right, not sure what's a realistic timeline for prod tho
13:43:15 From Andrew Hughes1 to Everyone:
https://docs.google.com/document/d/1FtWfULPqCyNqbXf3ekPlWs42LNjgWukPRaYCG5fPU10/edit?usp=sharing
13:43:25 From Drummond Reed to Everyone:
Yes, the same is actually true of ePassports - only verifiable by government agencies
13:45:03 From Kristina Y, to Everyone:
but nothing in 18013=5 prevents DPKI, just saying
13:45:35 From Kristina Y, to Everyone:
very shocking
13:45:35 From Drummond Reed to Everyone:

Doesn’t it assume X.509 certs?
13:46:24 From @PrivacyCDN to Everyone:
Scope is essentially in person presentation, not a web transaction
13:46:34 From Drummond Reed to Everyone:
It sounds very much like the ICAO PKD. Which is pretty much the antithesis of DPKI.
13:46:55 From Drummond Reed to Everyone:
Just sayin’ ;-)
13:47:26 From JEFF NIGRINY to Everyone:
lol- we submitted a response to AAMVA's RFP suggesting an ICAO trust model approach was a mistake, didn't go anywhere
13:48:42 From Drummond Reed to Everyone:
Yes, the same happened with WHO for their COVID-19 credential recommendations
13:49:32 From JEFF NIGRINY to Everyone:
you'll have to mention that unfortunate outcome in rev1 of your book ;)
13:49:58 From Drummond Reed to Everyone:
True…OR…we can tell the story of how we came together and made it all work!
13:50:13 From Drummond Reed to Everyone:
(have a happy ending ;-)
13:50:34 From Kristina Y, to Everyone:
can I give a quick pitch on 23220-2 than?
13:50:56 From Margo Johnson1 to Everyone:
I would like that Kristina!
13:51:31 From Darrell O'Donnell to Everyone:
+1 Kristina - provide a new view/perspective
13:51:37 From Drummond Reed to Everyone:
Can you explain what 23220-2 is?
13:51:58 From Andrew Hughes1 to Everyone:
23220-2 is the data model and structure
13:52:13 From Christian Paquin to Everyone:
You said that, today, the only ID proofing of the mDL is your face (i.e., the photo embedded in the credential). Are there other mechanisms considered by the WG?
13:54:28 From Andrew Hughes1 to Everyone:
@Christian - for in-person modes, the person’s face and portrait photo is the commonly-available biometric
13:54:38 From Andrew Hughes1 to Everyone:
Fully-online modes cannot do that well right now
13:55:04 From @PrivacyCDN to Everyone:
Is one of the issues that mDLs are explicitly Identification and Authorization as opposed to VC’s?
13:55:30 From Christian Paquin to Everyone:
@Andrew, ok, just wanted to see if there were other mechanisms being investigated...
13:55:33 From Juan from Spruce to Everyone:
lol
13:56:24 From Kristina Y, to Everyone:
@Christian, 23220-5 is the spec considering that
13:56:37 From Kristina Y, to Everyone:
for online it becomes biometrics
13:57:31 From Drummond Reed to Everyone:

I'm curious, given that Andrew and Kristina are deep into this work at ISO and also understand VCs and DIDs pretty well: what are each of your thoughts about how we should best work together? What would be your recommended roadmap of concrete steps forward?
13:57:50 From Kristina Y, to Everyone:
If SSI is about direct presentation of my digital ID to the verifier, mDL is a perfectly valid SSI solution
13:58:45 From JEFF NIGRINY to Everyone:
I would be very interested to hear what their specific reason or citation was for not relying on blockchain. I did a project with Anil John (as did almost everyone - I know ;) for CBP at DHS specifically for their use of multiple blockchains. There is no prohibition I'm aware of whatsoever.
13:59:07 From Kristina Y, to Everyone:
Jeff, blockchain for what?
13:59:14 From Christian Paquin to Everyone:
Thanks @Kristina for the pointer
13:59:32 From Margo Johnson1 to Everyone:
@Kristina curious for the biometrics piece how far in is 23220-5 going / what does the data model or structure describe?
13:59:42 From Kristina Y, to Everyone:
23220-2 does give a stab at using DIDs too btw, because it does not have a dependency to use device bound keys like in 18013-5
14:00:15 From Darrell O'Donnell to Everyone:
@Kristina - you should consider giving a session
14:00:22 From Juan from Spruce to Everyone:
the problem with blockchain and NIST is that they certify one algorithm/library at a time-- if you limit yourself to what's allowlisted today, it's pretty hard to build something conformant. but one by one they're approving lots of the bits and bops... secp is street legal now (but not keccak :/)
14:00:28 From JEFF NIGRINY to Everyone:
My project was a data aggregator across multiple DLTs so you could see things like food as it went from producer to transport to retailer. Bascially it let you act as a participating node in several different DLTs - it's in GitHub - DLT Gateway.
14:00:41 From Kristina Y, to Everyone:
Margo, I think 23220-5 has been focusing on the transmission and APIs
14:00:59 From Judith Fleenor1 to Everyone:
I would also love to hear "I'm curious, given that Andrew and Kristina are deep into this work at ISO and also understand VCs and DIDs pretty well: what are each of your thoughts about how we should best work together? What would be your recommended roadmap of concrete steps forward?"
14:01:03 From Juan from Spruce to Everyone:
what about DERIVED credentials
14:01:18 From Darrell O'Donnell to Everyone:
For clarity the Issuer may NOT be the government - but the actual Vendor?
14:01:24 From Juan from Spruce to Everyone:
can a notary or intermediary issue to a holder a more self-sovereign "snapshot" of that issuer-controlled credential, at least partially?
14:01:48 From Kristina Y, to Everyone:
Android API will give you a Boolean whether a person in front a phone is the same person who was in front of the phone when the mID was issued
14:01:57 From Dan Robertson (he/him) to Everyone: +1 Juan: good question
14:02:37 From Nader Helmy to Everyone:
@Juan wonder if it would be theoretically possible to issue a verifiable credential version of an MDL
14:02:55 From Kristina Y, to Everyone:

@Darrell, if you mean a vendor contracted by the gov. yes, from the user perspective, the issuer is always the gov, I guess
14:02:57 From Juan from Spruce to Everyone: hypothetically ;)
14:03:01 From Michael Shea to Everyone: lagging indicators?
14:03:17 From Kristina Y, to Everyone: @Nader, yes, it is being defined
14:03:38 From Darrell O'Donnell to Everyone:
@Kristina - but is the Issuer the vendor or does Govt retain its control to revoke, issue, etc.?
14:03:40 From Kristina Y, to Everyone:
Juan, what is the use-case for the derived creds?
14:04:00 From Juan from Spruce to Everyone: oh, idunno, most of them
14:04:18 From Kristina Y, to Everyone:
@darrell, I think that question is out of scope of the technical spec, and btw revocation is not defined in 18013-5
14:04:19 From Juan from Spruce to Everyone:
everything you don't want the issuer in the loop for :D
14:04:28 From nembal to Everyone: :P
14:04:42 From Kristina Y, to Everyone:
Juan, in mDL offline presentation there is NO ISSUER INVOLVED
14:05:14 From Juan from Spruce to Everyone: 🖷
14:05:26 From Kristina Y, to Everyone:
mDL offline presentation has session encryption, authentication of the app and optionally authentication of the verifier
14:05:32 From Juan from Spruce to Everyone:
the only thing funner than "show me your papers" is "hand over your phone"
14:05:53 From Drummond Reed to Everyone:
that's a very real danger, Juan
14:06:03 From Kristina Y, to Everyone:
the offline mDL presentation is **contactless**
14:06:18 From Juan from Spruce to Everyone:
"hold your phone against this magnet", then
14:06:22 From Kristina Y, to Everyone:
no need to hand over your phone, just scan the QR code that police shows on their device
14:06:39 From Juan from Spruce to Everyone:
iisn't that the online mode?
14:06:41 From Kristina Y, to Everyone:
you are holding your device over the magnet everyday when you pay contactlessly
14:06:42 From Drummond Reed to Everyone:
@Kristina: "Juan, in mDL offline presentation there is NO ISSUER INVOLVED". Are you saying the mDL is not even signed by the issuer?
14:06:58 From Kristina Y, to Everyone:
ofc it is signed by the issuer
14:07:03 From Kristina Y, to Everyone:
no issuer at the presentation
14:07:04 From Juan from Spruce to Everyone:
(I think she meant realtime phone home!)
14:07:10 From Drummond Reed to Everyone:
thanks, I was confused
14:07:48 From Nader Helmy to Everyone:

@Kristina but you still have to check the issuer PKI system (which is tightly controlled) at the point of issuance right
14:07:55 From Nader Helmy to Everyone:
**point of presentation
14:07:56 From Kristina Y, to Everyone:
so by derived creds you mean no issuer involvement at the issuer?
14:07:57 From Nader Helmy to Everyone:
Apologies
14:08:32 From Juan from Spruce to Everyone:
notarial issuer - issuer says THEY checked the signature, and resigns it with a more open-world signature
14:08:37 From Juan from Spruce to Everyone:
is one option
14:09:00 From Juan from Spruce to Everyone:
only if keccak is not involved
14:09:07 From Kristina Y, to Everyone:
@Nader, yes, but that does not equal issuer call home - AAMVA wants to run PKI in the US for all DMVs
14:09:15 From Drummond Reed to Everyone: "keccak"?
14:09:25 From @PrivacyCDN to Everyone: New Crypto Protocol "Rabbit in the Hat"
14:09:39 From Judith Fleenor1 to Everyone:
Magic Crypo… is that defined by muggles?
14:09:40 From Kristina Y, to Everyone:
I just still do not understand a use-case for derived creds
14:09:48 From Kristina Y, to Everyone:
this WG is very use-case driven
14:09:49 From Juan from Spruce to Everyone:
(the hash function used in all EVM contexts to create Ethereum addresses)
14:10:25 From Juan from Spruce to Everyone: Indeed
14:11:15 From JEFF NIGRINY to Everyone:
I was trying to figure out the use case for derived as well. I support US Fed quite a bit and maybe I cannot get out of that mindset but derived there is solely about getting from smartcard form factor to smartphone. In this case, you are starting on the smartphone. Where else are we going?
14:14:04 From Kristina Y, to Everyone:
derivation is different from transforming MSO signed CBOR mDL into an JSON VC
14:14:25 From Darrell O'Donnell to Everyone: "may not be usable in the general case" - oops
14:15:50 From Kristina Y, to Everyone:
In any case, if anyone on the call have requirements for mDL as a VC or have concrete mechanisms they want to see in mDL as a VC, please reach out - would love to reflect in 23220-2
14:19:03 From Kristina Y, to Everyone:
Andrew, I think blocking of "secondary use" will depend on jurisdiction - will be very different in the US and Europe and Japan
14:21:16 From Drummond Reed to Everyone:
Apple has also NOT announced any support for W3C VCs. Neither has Google. Or Mozilla.
14:22:26 From Ringo from Spruce to Everyone: ^^
14:22:46 From Kristina Y, to Everyone: Apple's SMART Health Cards are VCs..
14:23:33 From Kristina Y, to Everyone:
the bottomline is, VC is only a data model, while mDL spec also defines everything else ("data representation syntax, transmission technologies, data element definitions or request and response mechanisms or messages")
14:23:43 From @PrivacyCDN to Everyone:

Vic Cooper wins the takeaway quote of the session
14:23:59 From @PrivacyCDN to Everyone:
"Organizational immune system against innovation"
14:24:16 From Kristina Y, to Everyone:
from one perspective, mDL is already a VC in CBOR signed with an external claim that is MSO
14:24:33 From Kristina Y, to Everyone:
that is how flexible VC-data-model is!
14:25:16 From Michael Shea to Everyone:
I don't know, they implemented some pretty slowing down processes that extended time out without much consequences .
14:25:37 From Kristina Y, to Everyone:
given the current state of 18013-5, the realistic starting point would be a wallet being able to handle both - ISO-compliant mDL AND VCs
14:25:45 From Kristina Y, to Everyone:
(I am just brandumping in the cht)
14:26:09 From Darrell O'Donnell to Everyone:
@kristina 100% agreed - wallets will need to be flexible
14:27:27 From Ringo from Spruce to Everyone:
But if mDL is a huge lift and proprietary and requires OS-level access to NFC... not exactly an equal playing field
14:28:10 From Ringo from Spruce to Everyone:
"just handling both" sounds great if you already support mDL and want to support VCs, not so great if you are a tiny startup supporting VCs that wants to support mDLs :D
14:28:22 From Drummond Reed to Everyone:
+1
14:28:59 From Darrell O'Donnell to Everyone:
Agreed - add in the accreditation that will be required for ANY high assurance credentials and we'll see a small number of wallet apps and SDKs in time
14:29:59 From Judith Fleenor1 to Everyone:
https://wiki.trustoverip.org/display/HOME/EFWG+2021-09-23+Meeting
14:30:15 From Judith Fleenor1 to Everyone:
Recording of that meeting is on the above page
14:31:12 From Vic Cooper to Everyone:
Regards of the specs and the bridging, seems like the right to drive part of a Driver's License would best be turned into a ZKP proof while the identity proofing should move into some sort of mirco-ledger/KERI/ADP solution with biometric validation at the mobile edge device
14:32:04 From Ringo from Spruce to Everyone:
but only high-assurance vendors that can support the whole spec get access to those VCs
14:32:11 From Ringo from Spruce to Everyone:
derived credentials are a little more portable and open...
14:32:39 From Kristina Y, to Everyone:
well, the point of mDL is to be high-assurance and those are requirements
14:33:03 From Ringo from Spruce to Everyone:
so the use-case for derived VCs is every medium- and low-assurance use case
14:34:49 From Judith Fleenor1 to Everyone:
If we need to spin up a Task Force at ToIP to start the discussion… we could make a space for that… we'd just need the right people in the room.
14:34:53 From Darrell O'Donnell to Everyone:

@ringo - no, it's just that if you want to do high-assurance there are table stakes that mean the market will converge on a smaller number of players, where we add value on top of that.
14:36:26 From @PrivacyCDN to Everyone:
mDL's are artefacts with a number of use cases, where VC's are more general tool
14:37:53 From Juan from Spruce to Everyone:
the question was about selective disclosure?
14:39:38 From Kristina Y, to Everyone:
oh! and this group needs to know about "intent to retain" of mDL)
14:39:44 From Judith Fleenor1 to Everyone:
selected release not selective disclosure
14:40:19 From Kristina Y, to Everyone:
which would need to be enforced by the regulations if verifiers are actually not retaining when the user set "intent to retain"= false
14:40:29 From Darrell O'Donnell to Everyone:
"intent to retain" meaning, in SSI terms the Verifier needs to tell you what they will use and/or keep?
14:41:06 From Richard Esplin to Everyone:
But the entire credential hash is always sent, even if certain data elements are not released.
14:41:14 From Richard Esplin to Everyone:
If I understood this morning's discussion correctly.
14:41:47 From David Waite to Everyone:
What is the difference between selective release and selective disclosure?
14:42:17 From Darrell O'Donnell to Everyone:
gotta roll - keep being awesome folks!
14:43:11 From Drummond Reed to Everyone:
I believe the difference is that "selective release" is limited to yes/no on claims. "selective disclosure" is more robust, including proving you do/do not have a claim. And when selective disclosure is done using ZKP, you also get correlation protection on the digital signatures.
14:43:12 From Michael Shea to Everyone:
Thank you Andrew, Kristina, great session.
14:43:29 From Juan from Spruce to Everyone:
online mode is pretty OIDC-friendly though, right?
14:43:40 From Juan from Spruce to Everyone:
correlation protection seems a major difference here :/
14:44:32 From @PrivacyCDN to Everyone:
That is why we are doing a Privacy Enhancing Mobile Credential WG in Kantara
14:44:35 From David Waite to Everyone:
Ahh so there are things being included in selective disclosure that are subatomic :-)

Crossing the Chasm → Mass Market Adoption of SSI and VC: What is Needed to Make Triangle of Trust Work?

Tuesday 13B
Convener: Tim Heidfeld (IAMX), Jochen Leinberger (IAMX)
Notes-taker(s): Dennis Mittmann
Tags for the session - technology discussed/ideas considered:
Identity, Decentralized Identity, Self Sovereign Identity (SSI), Decentralize Identity Documents (DIDs), DID methods, verifiable credentials, authentication agent, chasm, triangle of trust, gateways, use cases

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

Link to full PDF of presentation - Here Includes: 1-pager big picture
https://drive.google.com/file/d/1uTHo5-MpUDqWcW7uHv_uFuQjb6EzCVJD/view

Crossing the chasm

1. How to → enable mass market adoption of SSI and VC?
2. Is the preservation of human rights the correct design-principle?
3. What is needed to make triangle of trust work?
a) How to design verifiable credentials ZKP and GDPR conform?
b) How to onboard verifiable credentials?
c) What are the use cases?

IAMX Company Introduction by Jochen
Handover to Tim to welcome Everyone for the Session
Look at SSI from a Business Development perspective.

1. SSi is a Marketplace, and we need to balance seller and buyer in this marketplace in order to make this work.
2. Identity is a human right and therefore our approach is pure and
3. The Triangle of Trust
3a) The Allegra Model from IAMX is ZKP by design and not by any fance mathematics.
3b) Onboarding on the IMAX SSI solution is done in different ways.

Onboarding of around 10 mil KYC Proofed Telco Customers by Invitation Letter and a Process, where these customers/holders can convert their KYC proofed data into the Allegra Model by Import Credential generation.

Onboarding via an Hardware/Software Solution called IAMX Gateway. It is a terminal equipped with government certified Document and Biometrics scanners. This Terminal lets customers generate credentials for any kind of documents like Paper, Plastic, IC2, NFC, etc. in combination with a Biometric Passport. The holder has to stand in front of the Device and has to match the Passport Biometrics in order to generate credentials.

Onboarding via Mobile App in Combination with NFC, etc. in the future

3c) One-Click-Fulfillment.
The Holder wants to purchase a Mobile Phone Contract and provides the necessary Data via a 3rd party Solution. This Data will be converted with the Allegra Model Schema and can be verified via the IAMX Gateway or any 3rd party Interface to the leger. In this case the Contract can be fulfilled, because the necessary Data like minimal Age and Street Address could be verified within the payment process. And that is what enables smart contract.

Updates On The Global COVID Certificate Network

Wednesday 13C
Convener: Lucy Yang & John Walker
Notes-taker(s): Lucy Yang

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

Session Summary:
Linux Foundation Public Health launched the Global COVID Certificate Network in June 2021 to enable interoperable and trustworthy verification of COVID certificates between jurisdictions for safe border reopening. One key priority is to respond to the lack of a global trust architecture. This presentation and discussion is to provide an overview and most up-to-date information of this work.

Session Slides:
https://docs.google.com/presentation/d/11HYpzX0919ga0CihYE68bIbjRwwDRnRIkUQK1XlP3qM/edit?usp=sharing

Verifiable Credentials Policy Committee - Come Help us Pass a Trust Framework in California

Wednesday 13D
Convener: Kaliya Young, Ally Medina
Notes-taker(s): Kaliya

Tags for the session - technology discussed/ideas considered:
California, Legislation, Trust Frameworks

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

https://docs.google.com/presentation/d/1VyxmWan3qbxynxhKvw1CHhWZINiPRF9gjeqSCSDh1MY/edit#slide=id.p

The Video has more information about what we are doing.
Please reach out if you want to join our work getting legislation passed in California.

Time is Running Out - Get to Market - Revenue, Costs and Who Pays For What

Wednesday 13E
Convener: Kimberly Linson
Notes-taker(s): Kimberly Linson

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

Presentation Slides: https://app.slidebean.com/p/7a7x2xix31/ALl-hands-101921

What are the business strategies for digital identity solutions? Per credential, tokens, subscription models.

What are examples of when an issuer, holder, or verifier might pay for a credential and/or the exchange of that credential? - YES. There are situations where each of these actors might find value and thus be willing to pay for a credential.

The example of The Lifelong Learner Project's Teacher Wallet was dissected. Other industries were considered for comparison - organic farmers, sustainably recycling of technology.

Taking the Adoption of SSI to the Next Level

Wednesday 13F
Conveners James Ebert, Timo Glastra, Karim Stekelenburg
Notes-taker(s): Neil Bourgeois

Tags for the session - technology discussed/ideas considered: Aries, JavaScript, ReactNative

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

IIW33 Presentation

Need to include developers who are not focussed on identity. Can't just be a small group of tech enthusiasts. We need a broad and widescale adoption.

- steep learning curve
- time and resource intensive
- knowledge of standards and protocols is required
- ssi space is continuously evolving
- frameworks and apis not stable yet

What do we need:

- familiarity - support for languages to ensure integrations work

- easy api without having to dive into all the protocols or deep knowledge of ssi
- docs are important
- devs want to just get the job done without knowing every detail
- extend functionality of an ssi framework
- want a framework that gives e2e soln : not just a holder, verifier etc.

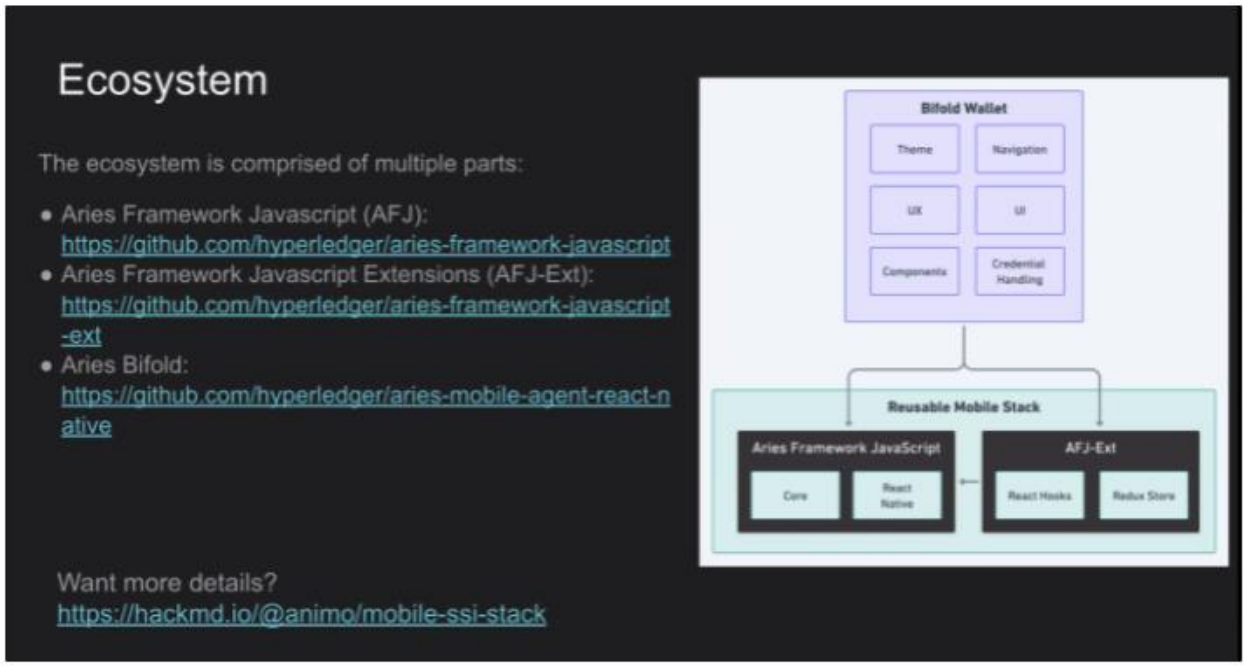
Aries Framework Javascript ecosystem:

- hosts are maintainers
- Why JS? JS is a popular language, lots of solns use it, runs on various envs
- Some concerns about _another_ implementation

AFJ Feature Overview - HackMD

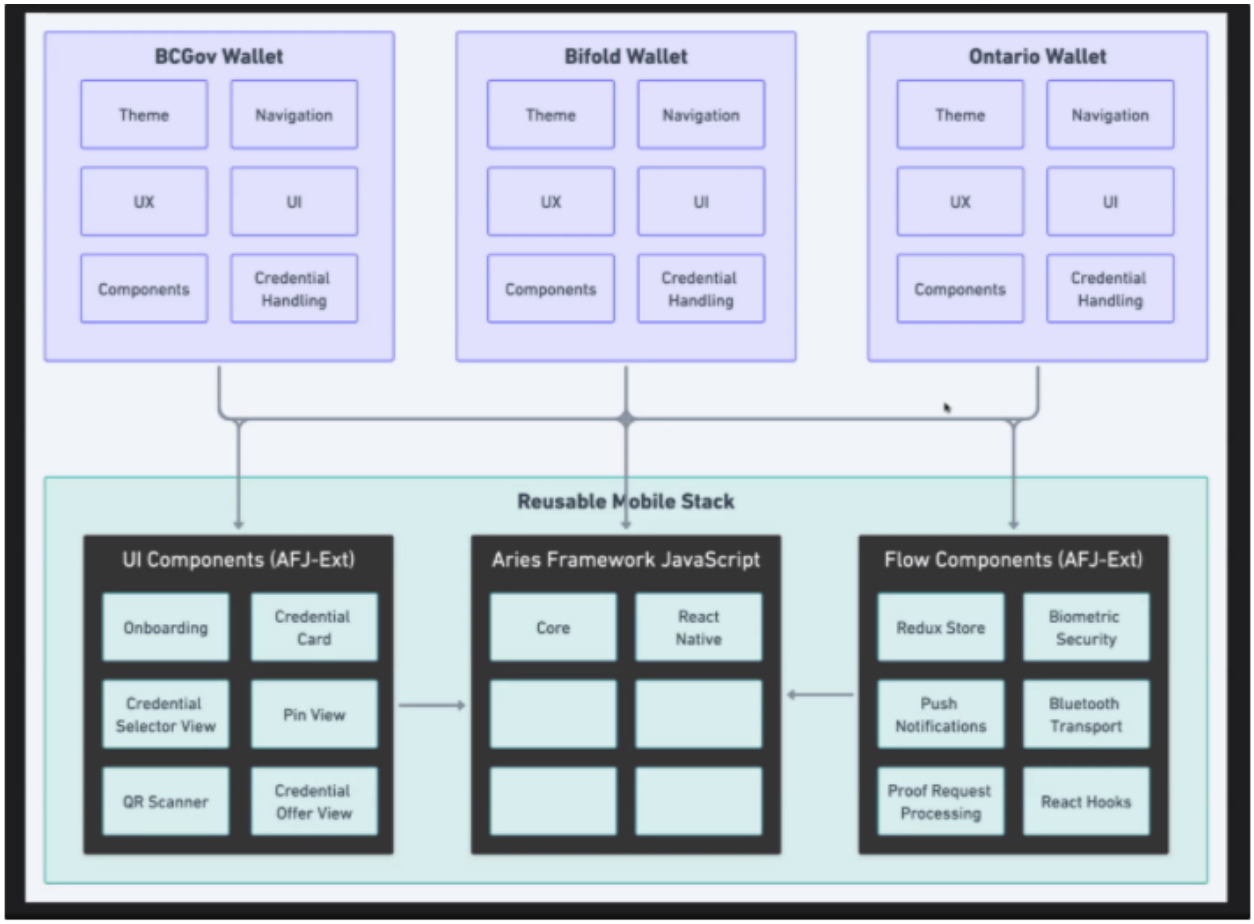
ACA-Py Feature Overview - HackMD

- can write your own modules in TS to extend core functionality



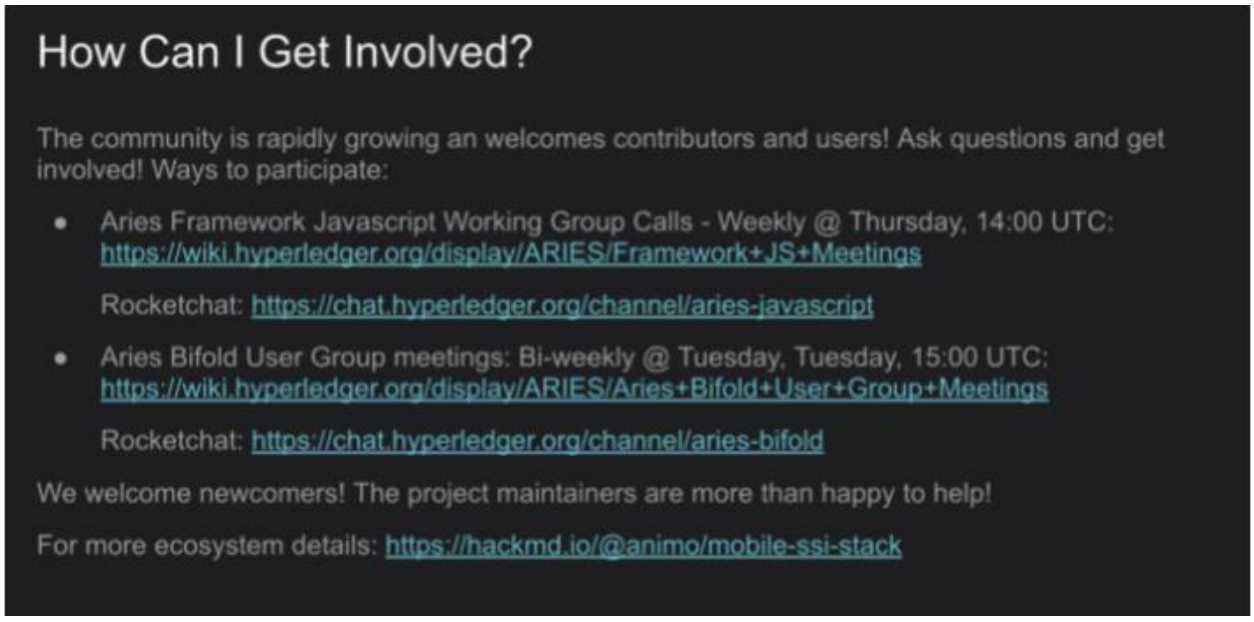
Aries Framework JS Extenions:

- give you the tools
- UI components, workflow libs.
- make it simple



https://aries-interop.info

WG Call weekly Thursdays at 1400UTC



BC Gov + Ontario using this for their wallets

SITA, Indicio pave way to safer travel experience with launch of Aruba Health App

"Emergency" situation in Netherlands:

- sharing location data over SSI
- group people by hexagon (https://h3geo.org)

See also: https://israelrescue.org/

Privacy Signal Standard Update (IEEE P7012)

Wednesday 13H
Convener: Scott Mace and Lisa LeVasseur
Notes-taker(s): Scott Mace

Tags for the session - technology discussed/ideas considered:

#Privacy #PrivacySignal #IEEE #Standards #MachineReadableTerms

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

Presentation here: https://www.slideshare.net/secret/xPfgXsyv29jkXZ

Lisa LeVasseur introduced attendees to the IEEE P7012 working group, the standard for machine readable personal privacy terms. She explained the purpose of the group - to provide individuals with means to proffer their own terms respecting personal privacy, in ways that can be read, acknowledged and agreed to by machines operated by others in the networked world, in a legally-binding way. The group does not address privacy policies themselves, since these are one-sided and need no agreement.

We need a software agent that works on behalf of the individual that can proffer and ultimately negotiate these terms, expressed as privacy agreements. This is a deliberate attempt to empower people and mitigate the traditional power asymmetry between individuals and organizations.

Peripheral entities participating in this include registries of terms and of agreements.

The status of the spec: Draft spec is in progress. We have some clarifying activities under way. We seek to refresh and reinvigorate our work. This includes revisiting and clarifying requirements, assumptions and scope. We seek to have a ballot spec by the first quarter of 2023.

We have draft versions of the spec and of a data schema to embody the processes involved (e.g. contracts or licenses).

Lisa shared a framework out of the Me2B Alliance to illustrate how P7012 can matter in the arc of a digital relationship, such as between an individual and a web site.

Proffering privacy terms are an example of a privacy signal, which Lisa overlaid onto the states of the relationship arc she previously illustrated. The Global Privacy Control work in W3C is akin to do not track redux, but Lisa is concerned that no default is specified. Therefore, P7012 probably doesn't cover agreements between anonymous individuals and organizations. But P7012 can reference work done elsewhere, and not be obliged to define standards in the entire relationship arc.

We need greater diversity and representation, including from marginalized communities of all varieties. We also seek more non-STEM disciplines, in particular legal experts. Since this machine-readable thing is intended to be legally binding, this is key.

Mary Hodder, the spec technical editor, echoed the need for help, and people can help in smaller chunks of the work.

Moira Patterson requested a bullet list to help identify specific people to address these smaller chunks of work.

Scott Mace (and P7012 WG member Tom Mahon) are creating a boilerplate recruitment letter, and that letter could address the different kinds of expertise required for this work.

Mark Lizar offered the GDPR as a privacy agreement, which can even be between countries. Says we need some breakthroughs.

Lisa mentioned a recording of permissions (consent receipt) and then there's also a usage record (what actually happened - what did the org do with your stuff). Those two artifacts - the record of the agreement, and the record of the behavior - exist alongside the agreement process itself. Consent, contracts, and licenses are legal vehicles.

Mark Lizar says the GDPR has something called a valid state of consent. Putting a cookie on your device breaks the GDPR law. Right now there's no proof of notice, we just click boxes. An alternative method of consent comes with privacy rights applied with privacy law and dealt with regulators through privacy complaints, or contract law. But children can't defend themselves in some of these venues. CCPA is like consent/surveillance by default. If you had your own record of who the controller was, you could create receipts. We did an NGI project to make an anchor record, controlling your own privacy preferences.

Lisa hears from Mark that IEEE is on the right track. She also referenced a news story describing Facebook's attempt to possibly bypass the concept of consent receipts.

Mark mentioned ISO 29100 as another effort to broadcast privacy preferences, which will be described in a subsequent session at this IIW.

Mary echoed the importance of the P7012 work being interoperable with other aspects of solving the general problems created by various privacy issues.

Stay tuned for future possible collaborations, and please join IEEE P7012 in its work! Monthly meetings are on the second Tuesday of the month, from 8:30am to 10:30am East Coast time.

Working with JSON-LD and Best Practices to Make It Easier

Wednesday 13J
Convener: Kyle Den Hartog
Notes-taker(s): Kyle Den Hartog

Tags for the session - technology discussed/ideas considered:

Developer discussion, JSON-LD, verifiable credentials

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

Powerpoint slides I used here:
https://docs.google.com/presentation/d/16OTHsmxk_WQsbTfbIGkBUadpryMcSEeR/edit?usp=sharing&ouid=110568419126541350920&rtpof=true&sd=true

Proof of concept code here: https://github.com/kdenhartog/context-integrity

PAC Theorem KERI Zero Trust

Wednesday 13K
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:

Session Presentation link provided by Sam Smith:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI_PAC_Theorem.pdf

Privacy Enhancing Mobile Credentials (Building on Prior Kantara Report)

Wednesday 14A
Convener: John Wunderlich
Notes-taker(s): Andrew Hughes

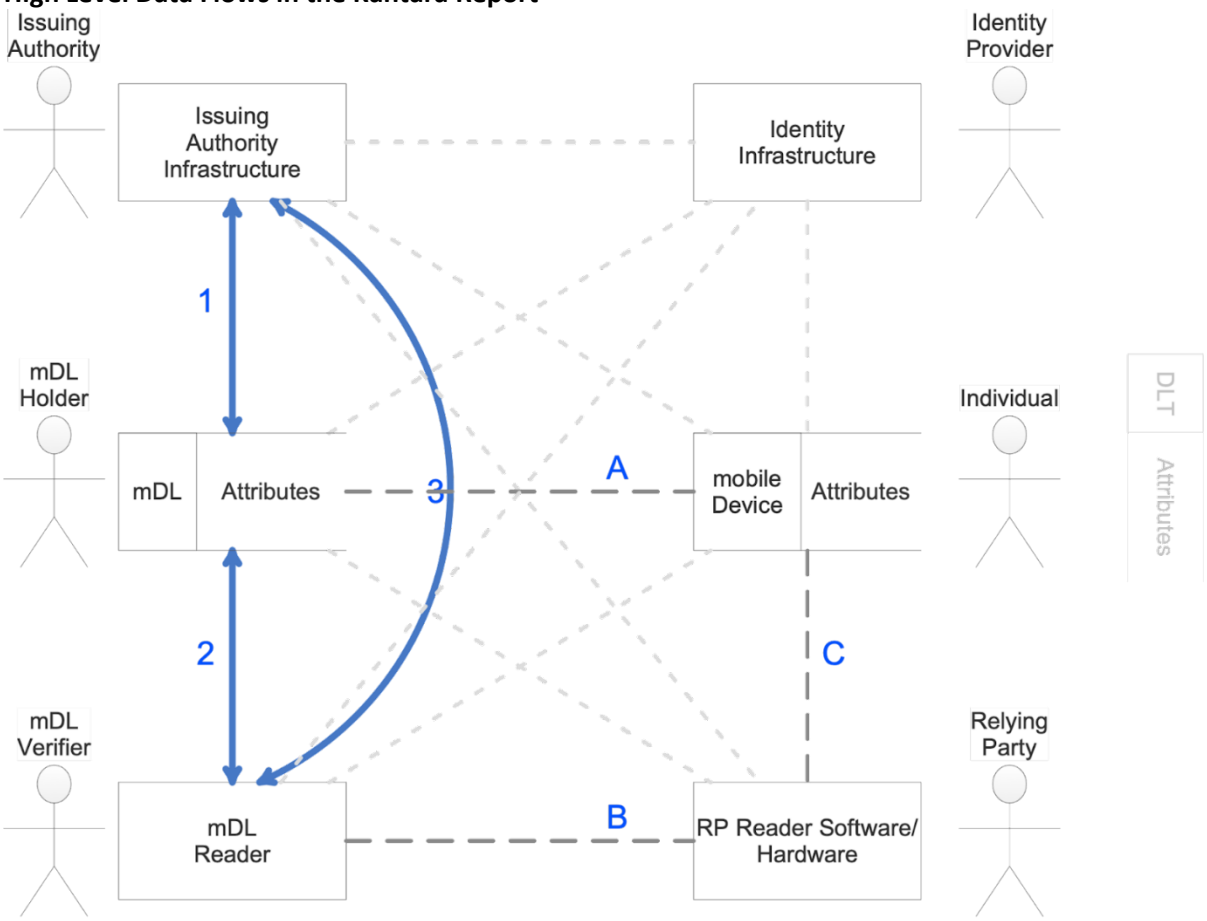
Tags for the session - technology discussed/ideas considered: mDL ; VC ; Mobile Credentials

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

The purpose of this session is to walk people through the existing report on mDL ecosystems and to talk about the new Work Group to get input (and possible volunteers)
Links:

- Kantara Report on mDL ecosystems: https://kantarainitiative.org/download/pimdl-v1-final-html/
- Kantara Charter for Privacy Enhancing Mobile Credentials WG: https://kantarainitiative.org/confluence/display/PEMCP/WG+Charter

High Level Data Flows in the Kantara Report



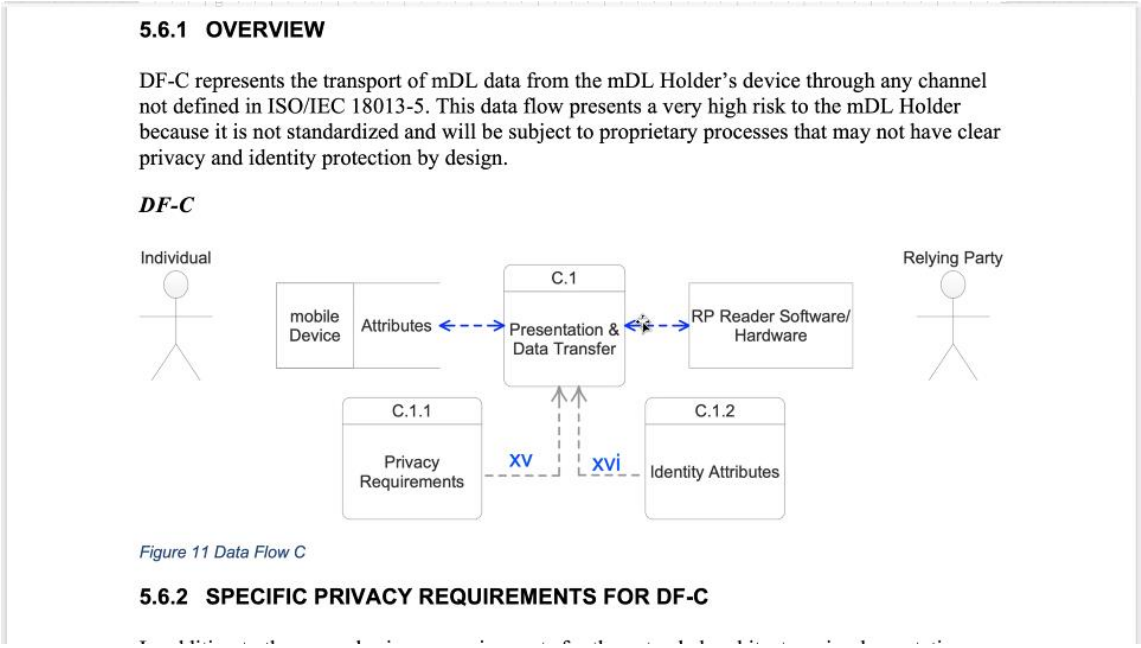
Purpose of the PEMC WG:
The purpose of the proposed workgroup is to create a set of requirements and conformance criteria to protect the privacy of individuals holding or using mobile credentials such as mobile Driving Licenses. This includes, but is not restricted to, technology ecosystems based on ISO/IEC 18013-5 compliant mobile driving licenses. Existing standards can provide technical and transactional assurances of user choice and

data minimization at the point of presentation of the credential, but do not provide assurances to the holders of mobile credentials that relying parties that may collect their identity attributes will use those attributes solely for the fulfilment of the purposes for which the mobile credential was presented. Failing to respect the consent of the mobile credential holder or the legal authority of the verifier to collect the identity attributes could violate the privacy of the mobile credential holder.

We propose a phased approach to writing requirements and conformance criteria for the various endpoints of data flows in a mobile credential ecosystem which we characterize as Issuer, Holder, and Verifier, including the software, hardware, individuals, and entities at the technical endpoints. In ISO/IEC 18013-5 these are the “Issuing Authority” and “Issuing Authority Infrastructure”, the “mDL Holder” and the “mDL” (credential and holding software), and the “mDL Verifier” and “mDL Reader”.

NOTES

- John sets the context for the Privacy Enhancing Mobile Credentials Work Group just starting up at Kantara Initiative
- John walks through the Kantara report
- Starts with the data flow diagram - describes the Data Flows in focus
- Eleven privacy considerations for the extended ecosystem - they come from ISO 18013-5 Annex E (Privacy and security considerations)
- The Kantara report takes parts of the 18013-5 standard and starts to elaborate the risks and mitigations
- Q: Is there consideration of defining a profile for consideration?
- A: A good consideration as input into the PEMC WG
- A: 18013-5 does provide the technical capability to allow the mDL app to not send data elements which were requested by the mDL Reader
- The PEMC will define requirements for operators, as the basis for third party conformance evaluation and attestation
- Discussion about ‘digital notary’ - a trusted third party that acts as an attribute oracle
    - Might not work in the 18013-5 ecosystem due to issuer rules
- Looking at a specific data flow - eg DataFlow-C



5.6.1 OVERVIEW

DF-C represents the transport of mDL data from the mDL Holder’s device through any channel not defined in ISO/IEC 18013-5. This data flow presents a very high risk to the mDL Holder because it is not standardized and will be subject to proprietary processes that may not have clear privacy and identity protection by design.

DF-C

Figure 11 Data Flow C

5.6.2 SPECIFIC PRIVACY REQUIREMENTS FOR DF-C

-

- For this data flow, there are specific privacy requirements and specific identity considerations spelled out, as well as interoperability risks
-
- John starts describing the new Kantara Privacy Enhancing Mobile Credential WG
- The WG will document requirements, based on the Report analysis - from the Charter:

Privacy Enhancing Mobile Credentials (PEMC)

Purpose:

The purpose of the proposed workgroup is to create a set of requirements and conformance criteria to protect the privacy of individuals holding or using mobile credentials such as mobile Driving Licenses. This includes, but is not restricted to, technology ecosystems based on ISO/IEC 18013-5 compliant mobile driving licenses. Existing standards can provide technical and transactional assurances of user choice and data minimization at the point of presentation of the credential, but do not provide assurances to the holders of mobile credentials that relying parties that may collect their identity attributes will use those attributes solely for the fulfilment of the purposes for which the mobile credential was presented. Failing to respect the consent of mobile credential holder or the legal authority of the verifier to collect the identity attributes could violate the privacy of the mobile credential holder.

We propose a phased approach to writing requirements and conformance criteria[1] for the various endpoints of data flows in a mobile credential ecosystem which we characterize as Issuer, Holder, and Verifier, including the software, hardware, individuals, and entities at the technical endpoints. In ISO/IEC 18013-5 these are the "Issuing Authority" and "Issuing Authority Infrastructure", the "mDL Holder" and the "mDL" (credential and holding software), and the "mDL Verifier" and "mDL Reader"[2]. The table below presents the proposed phases, with estimates of their durations. Note that we expect that some of the work in the phases will overlap to ensure that expectations are aligned across the ecosystem.

- The intent is to use the WG outputs as the basis for a new Kantara conformity assessment program and trustmark - so that operators can put their systems through the program and be able to say that their system meets these requirements for privacy enhancing mobile credential systems.
- An example of a requirement that might be in the WG output

Sample Requirements

The following are sample requirements that indicate the level of detail for the proposed specification. There is one sample requirement for Verifiers, Issuers, & Providers.

Reference	A_IS_01
Primary Consideration	Information Security
Identifiers Included	Direct: ☒ Indirect: ☒ Unique: ☒
Statement	All identifying data shall be transacted through encrypted channels.
Description	To provide holders and verifiers with confidentiality, verifiers shall only transact identifying data through encrypted secure channels to prevent exposure to third parties. **Note**: In the context of a digital ID, identifying data also includes unique identifiers such as public keys and digest salt values.
Related Requirements	TBD

UX: Continuing the Mid-2021 IIW UX Conversation

Wednesday 14B
Convener: Phil Wolff
Notes-taker(s): Phil Wolff

Tags for the session - technology discussed/ideas considered:
UX Design, UX, Design,

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:
Ongoing concerns with user experience in our space?

Consent overwhelm.
There are going to be 10^x consents for humans and other entities to manage daily. Hourly. Current UX is for consent behavior, one at a time. Cognitive overwhelm means your consent is isn't meaningful in life or in law.

No common (and simple) spoken language for talking about this stuff: identification, consent, governance, authorization, human relationships, cloud systems graphs, safety, security, privacy, human identity proofing (KYC), service/entity identity proofing, etc.
These areas have many common interactions, nouns and verbs, and a gazillion ways they are named, used, represented. Confusion is harmful to onboarding, usability, churn, error rates, etc.

No common visual language for this stuff.
"VCR" Play buttons go back to reel-to-reel sound recorders. We still use them for linear streams that can be played.

What is the visual language we can all use for the common interactions in all our spatial designs?

Missing screenless experiences. No common audible/sonified design language.
Many connected devices don't have screens. A pacemaker or streetlight or Alexa can have a rich identity but no screens. How do we enable spoken and "gestural" conversations via

Access: accessibility, internationalization, localization.
No designing to protect against antipatterns.
Going Forward
Don't prematurely standardize. Keep doing UI for specific use cases.
Hashtag #SSIdesign

Chris Butler - thought about this paper after the fact but wanted to leave it here for people: Against Notice Skepticism In Privacy (And Elsewhere)

DID Spec Formal Objections

Wednesday 14C
Convener: Brent Zundel
Notes-taker(s): Drummond Reed, Markus Sabadello

Tags for the session - technology discussed/ideas considered:

DIDs, W3C, standards

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

Not recorded for more open discussion.

Mostly a Q,A format. Please raise your hand

- DID working group began 2 years ago—defining proposed specification (https://www.w3.org/2020/12/did-wg-charter.html)
    - Did URL
    - Did method implementers
- In September, DID Core moved to "Proposed Recommendation" status
- 2 independent implementations of each feature

Wide review of W3C Advisory Committee

- Three formal objections were raised by Google, Apple and Mozilla
- Suggestions for changes (not formal objections) from Lawrence Berkeley and Microsoft

Formal Objection Text:
Google:

"DID-core is only useful with the use of "DID methods", which need their own specifications. These specifications are listed in the did-spec-registries WG Note, but none has made it past "PROVISIONAL" status, and the Note doesn't even define what its Status column means. It's impossible to review the impact of the core DID specification on the Web without concurrently reviewing the methods it's going to be used with. As the DID WG's charter states, we should follow the precedent set by the development of URLs, in which RFC 1738 standardized 10 schemes at the same time as it standardized URLs in general.

We strongly support the goal of decentralizing identifiers, but a review of a few of the provisional methods raises questions about how effective and ethical DID will be at accomplishing this. Some, like did:ccp:, are centralized under a single server. Many rely on proof-of-work cryptocurrencies, which fail the sustainability goals of the Ethical Web Principles. The process of advancing a few of the best methods through the Recommendation track will help focus review on them, and is likely to reveal places the did-core specification should change to fit the ways they improve.

We suggest holding off on advancing did-core to REC status until at least 3 or more methods are also ready to advance to REC."

Anonymous:

“We agree in full with the concerns raised by Google in their Formal Objection. The specification should have at least one, interoperable method that works out of the box, either (preferred) included or (less preferred) registered. To borrow Microsoft's words, the Working Group must take up "the challenge of defining a[...] fully interoperable DID method that meets industry use cases and can be specified as a mandatory to implement[...] method."

Lawrence Berkeley National Laboratory requested adding a requirement "to provide a system- and processor-independent assessment of the energy requirements of a DID method." Whatever this mandatory method is, it must not be unsustainable / in violation of the Ethical Web Principles.

The spec should not move to REC until such a method is in place.

Additionally, we agree with Microsoft's compatibility concerns re: JSON and JSON-LD.”

Mozilla:
Summary:
* No practical interoperability.
* Encourages divergence rather than convergence.
* Centralized methods allowed, in contradiction to WG & spec goals & name.
* Proof-of-work methods (e.g. blockchains) are harmful for sustainability (s12y).

No practical interoperability. As Microsoft & Google expressed, the DID “Core” spec has not demonstrated any degree of practical interoperability, instead delegating that to a registry of 50+ “methods”, none of which themselves have interoperable implementations. We agree with the analogy to URLs & schemes, as Google noted: “precedent set by the development of URLs, in which RFC 1738 standardized 10 schemes at the same time as it standardized URLs in general”. The Web has similar experience with the img tag & image formats, and the video tag & video formats. In each of those cases, there were multiple interoperable formats before the tags themselves were standardized. In addition, we agree with the comments made by Microsoft to “recommend that implementers use the simpler JSON representation, to enhance interoperability and avoid complications and incompatibilities arising from JSON-LD processing.”

Encourages divergence rather than convergence. The DID architectural approach appears to encourage divergence rather than convergence & interoperability. The presence of 50+ entries in the registry, without any actual interoperability, seems to imply that there are greater incentives to introduce a new method, than to attempt to interoperate with any one of a number of growing existing methods. Note this is in contrast with prior examples given (URL schemes, image & video formats). Thus, whether intended or not, the DID specification (and perhaps its inherent architecture) is designed in such a way that encourages divergence of implementations, rather than convergence & interoperability.

The lack of restrictions on the registry are allowing methods diametrically opposed to the principles of the group & spec, and methods which are actively globally harmful to sustainability. In particular:

* Centralized methods allowed, in contradiction to WG & spec goals & name. As Google noted, some methods in the registry such as did:ccp use a single server, and thus any interop with such a method would bias toward centralization, and likely be literally centralized rather than decentralized. Centralization might be at an architectural level, or – at a minimum – a service level, even if multiple “implementations” claimed to support it.

* Proof-of-work methods (e.g. blockchains) are harmful for sustainability (s12y). Also as noted by Google, the registry contains methods which rely upon proof-of-work which is wasteful. “Successful” proof-of-work systems waste a staggering amount of electricity world-wide (e.g. Bitcoin consumes more energy than most countries <https://www.forbes.com/sites/niallmccarthy/2021/05/05/bitcoin-devours-more-electricity-than-many-countries-infographic/>) demonstrating that the more such methods are adopted, the more their energy requirements grow, without any discernible upper bound, which is grossly irresponsible given the global environmental crisis (recent IPCC report <https://www.bbc.co.uk/news/science-environment-58130705>).

Lawrence Berkeley National Laboratory suggested “the registry should include a requirement to provide system- and processor-independent assessment of the energy requirements of any methods being registered.” We don’t think this goes far enough.

We (W3C) can no longer take a wait-and-see or neutral position on technologies with egregious energy use. We must instead firmly oppose such proof-of-work technologies including to the best of our ability blocking them from being incorporated or enabled (even optionally) by any specifications we develop. If anything we should pursue the opposite: develop specifications that supersede existing specifications, but with much less power consumption. We believe this is consistent with the TAG Ethical Web Sustainability principle (<https://www.w3.org/2001/tag/doc/ethical-web-principles/#sustainable>).

For these reasons we believe the DID specification may not be fixable (MUST NOT become a Recommendation). We suggest returning the specification to Working Draft status.”

Suggestions for changes (not formal objections):
Lawrence Berkeley:
“The document looks well thought out and comprehensive, but there is one area of significance that probably ought to be addressed in the requirements for DID method specifications, and that is energy consumption. Including a requirement to provide a system- and processor-independent assessment of the energy requirements of a DID method (e.g., a specific computational complexity analysis) would enable comparisons and hence selection of more energy efficient methods. I recognize that this was not included in initial requirements for the document, but waiting to include it in a future version will prevent its application to methods that are described based on the initial document.”

Microsoft:
“Microsoft has implemented and plans to use the W3C DID-core specification in our products, and we support the publication as a W3C Recommendation.

We also have additional feedback that we would like to see addressed in future work (if such work is taken up):

* Interoperability could be improved with a single foundational key representation. We would prefer implementers to use JSON Web Key for representing cryptographic keys. We believe JSON Web Key would be a great baseline of support that could be extended with additional formats. Any additional formats included in the spec text should include the appropriate usage context. Related to: DID-Core Section 5.2.1.

* We recommend additional non-normative guidance on cross-compatibility between the JSON and JSON-LD representations in Section 6. We further recommend that implementers use the simpler JSON representation, to enhance interoperability and avoid complications and incompatibilities arising from JSON-LD processing.

* We would like the Working Group to take the challenge of defining a new fully interoperable DID method that meets industry use cases and can be specified as a mandatory to implement reference method."

Background blog post on the whole issue published by Evernym yesterday:
https://www.evernym.com/blog/w3c-vision-of-decentralization/

W3C process begins with Charter.. Then the group agrees on a "First Public Working Draft". WGs are encouraged to start with documents that have been incubated. In our case, there was a DID Spec document from the Credentials Community Group. DID WG iterated over this for 1,5 years, then entered "Candidate Recommendation", when we requested "wide review" and "horizontal review" (this if for specific groups in W3C, such as Privacy, Security, Internationalization, Accessibility, TAG).

We got feedback from each of these group. We addressed all feedback as well as all issues that were raised on our repo. We adhered to the process, made changes in response to feedback and implementation results.

As soon as we had implementation results, we moved to "Proposed Recommendation". Then the process continued.. Call for review, received Formal Objections.

W3C team convened meeting between Objectors and DID WG representatives.
https://www.w3.org/2021/09/21-did10-minutes.html

We were not able to come to consensus with objectors on path forward. Next step is for the decision to be given to W3C Director. This means the W3C team looks at it, Ralph is "acting director".

W3C is trying to figure out how to act without a Director. Various committees and councils try to create consensus-based standards for the Web. W3C Council is composed of Advisory Board and TAG.

Question: About the objection of interoperability. This also has to do with data portability. In the Charter, there is a point about portability. DID spec doesn't define the way how you can independently move between DID methods. Is this taken into consideration?

There are numerous levels were interoperability could be shown. The Charter specifically outlines interop on the DID URI and data model level, along with an interface for DID Resolution. Out of scope were particular DID methods, so we couldn't show interoperability there. The type of interoperability you mentioned in the question I believe is addressed by having DID documents that are resolvable and understandable by consumers. The statement about data portability can be interpreted as being about Verifiable Credentials.

Question: The Charter didn't have in scope data portability in the sense of moving between networks, but in the sense of interaction.

We achieved interoperability on the data model level. Because specific DID methods were out of scope, we felt that showing interop between multiple implementations of particular DID methods was also out of scope.

Some DID migration mechanisms have been proposed, but they require protocols, not just data models. What's the typical migration mechanism for the web? 301 or 302 redirect, but this is a protocol. Such functionality was out of scope in our Charter.

Question: It seems to me one course of action is to pick 2 (or small number) of DID methods that don't use blockchain, and define them quickly. Is this doable? Any estimates how complicated this would be, technically, politically?

Technically, it might take longer than we think. Fitting this into W3C process, it would take at least a year. Politically, there seems to be relative agreement. Changing the scope of our work right now would be strange considering that we are the end of our timeline. The DID WG may support standardizing did:web and did:key.

If you read the minutes of the meeting with objectors, it could be that did:web and did:key would not be acceptable to them. It could take much longer than we would want to. We feel like we did good work and provided a solid foundation for other future standardization work.

Why are we being asked to do something now that wasn't in our charter?

The "customer" here is the WG. W3C approved the Charter 2 years ago. Now there is frustration, since the WG fulfilled all its requirements. Three W3C members (who happen to be the largest browser vendors) are saying they don't want this to go forward.

Now this goes to the Director to decide. We try to explain why we think the objections are not well-grounded, and how they are really motivated.

If the Director doesn't approve, we can request a simple-majority vote by all W3C members.

The argument that we "do not achieve interoperability" misses a major design principle of DIDs. DIDs are designed for interoperability. There are >100 DID methods that can be resolved to the same data model.

Question: Is the W3C of the opinion that DID Core should go back to draft status?

Only one organization (Mozilla) suggested this. This is an opinion by one member, not an opinion by W3C as a whole.

Question: What are the things that may have non-maliciously down the path to assume that we didn't achieve what we were supposed to do? Is it about the data model and a browser API? Do we also need to define a DID Resolution architecture, plus a few methods?

From the perspective of objectors, next step for the group could be to define specific methods. From the perspective of some WG member, we need to define the Resolution process. This may be related to defining specific DID methods. If we define a DID Resolution process, any compliant resolver would have to stick to.

Question: The objection came at a late stage, it's a pity that it comes so late in the process. Were they not aware of how this is shaping?

Mozilla is one of the organizations that nearly objected to the Charter, they strongly requested changes and were concerned from the beginning. None of the objectors participated by filing issues or actively contributing to the conversation.

Question: Microsoft also had substantive comments on concerns about lack of interoperability. I've never worked on a spec before where there was not a mandatory-to-implement set of features. This is a problem for interoperability. The bigger goal should be to have broader acceptance. It's a big red flag that all browser vendors except for Microsoft objected. We would be better off if we collaboratively work with them. Having a narrow victory in the face of objections doesn't serve the working group. Winning hearts and minds is more important.

About DID Resolution.. It's intentionally defined as an abstract interface, it's not a concrete protocol (like DNS). Details are dependent on the DID method.

It's key to address recommendations that objectors made. How can we get them to agreement, so that we get them to support the specification. We're upset about comments, but there has to be a way to address them. If we get the spec adopted without browser vendors, it's not a huge victory.

We were told by powerful companies that what we did is not good enough. This is similar to the "go get me a rock" problem (get me a bigger one, or a shinier one, etc.). The frustration has to do with lack of participation by objectors.

The DID spec may not be perfect, but we believe it is ready to be made into a Recommendation. If objectors believe we should re-charter to get DID methods specified, and if they will help do the work, that would be a different conversation.

We haven't seen any indication of that. Their objections didn't feel like they have serious understanding of DID architecture and objectives. It seems more like they are trying to find ways to delay it.

Comment: I'm a big believer in Charters, since they constrain what you do. Objections go beyond what's in the Charter. This may or not be fair. They say, we want to see a functioning ecosystem. There is not a single DID method that everybody supports. There is not a single key representation that everybody supports. They may feel that if we add a major new piece of functionality of the web, the expectation may be that the browsers implement this. There is no such expectation for DIDs. We should not try to read into people's motives. We should rather try to constructively engage, such as addressing the JSON vs. JSON-LD interop problem, or reducing key representations. There is a reason that major organizations like OASIS, W3C, OpenID Foundation have a broad review at the end. So that those who were not able to participate have a chance to object. They say it is bad for the ecosystem. It's not a process violation to participate at the end of the process. It's not a coincidence that so many important players are saying that there is something really wrong here. We ignore this at our peril.

Comment: I got some input on how much we should talk about objectors' potential motivations. It's dangerous, but also relevant. We act as if those objections are the bar. We miss the larger picture. When you have 112 different implementers, you can't say there is something wrong with the ecosystem. It's a sign of a very vibrant ecosystem. I personally think the political issue that there are so many DID methods will be solved by the market. See URIs, they were also standardized before the set of various concrete URI schemes was defined. Question should be turned around: What is the harm of going ahead with this first step of work, so that the 112 implementers can do their work?

Comment: There may be a middle ground here. Tension may come from immaturity of the ecosystem? If you look at certain methods, some of them are (.. not good ..). Once we find philosophical alignment, where do we go with it in technical terms. Objectors may think that allowing things to go forward may be a slippery slope. I saw what happened with Sidetree, where there was philosophical alignment, but still it took a long time to come to good technical interoperability. We should close gaps and work together, and ultimately try to get DIDs into the browsers.

Comment: As an innovator. .The DID spec represents a new paradigm, it's the future of the Internet. Everyone here knows that. The arc of decentralization is hitting every aspect of our life. It's challenging because it requires a new business model. It's a distribution that incumbents typically don't welcome. There are many books about the friction between the present and where the future goes. How we do privacy on the web needs to change. The current pathway is very dystopian. Here we are innovations and we stand for values. I love the large organizations, but I see their flaws. Apple doesn't take risks on new techn until they are confident that they can own the aspect. Google enables surveillance capitalism that created many problems today. I'm really confused by Mozilla, I understand why. Maybe they lost their innovation edge. I'm confident 100% that this is the future. Do we really need to ask for permission? This isn't going to die even if they kill the spec. Those organizations should open their minds to the future. It's a huge opportunity for them to innovate their business models. We got to look bigger. This is the future. If they put obstacles in front of us, we will still continue to do it. These organizations should be aware that they need to get on board. If they don't they will get disrupted.

We got a good conversation, recorded several viewpoints. We look forward to working with the Advisory Council if they should take up the issue.

Next steps are.. Right now there is an ongoing conversation on the AC mailing list. All W3C participating companies can interact. The conversation is at a more meta-level than about DID Recommendation. It's about the organization of the Advisory Council, what should the rules of recusal be, should there be better guidelines for reviews.

There are conversations about Ethical Web Principles, next steps, what should priorities be, etc. Should this serve as normative guidance for spec implementers. There is discussion about the Charter process. It's raising a lot of W3C process-level concerns and conversations. All of that is happening.

The Advisory Board will decide whether or not to form a Council to look at the formal objections. Either that will happen or it won't. Then the Acting Director will make a decision. Whichever way the decision goes, the next step could be an appeal to the W3C membership (the body of the AC). It would be a majority vote whether or not to uphold the Director's decision.

The DID WG has been extended until end of December. It's possible it may get extended longer.

Thank you for coming, this was a very valuable conversation.

Privacy Broadcasting for Privacy Awareness and Assurance

Wednesday 14D
Convener: Mark Lizar & Salvatore D'Agostino
Notes-taker(s): Scott Mace

Tags for the session - technology discussed/ideas considered:

@rights @individualrights @privacyagreements @legalterms @privacycontracts @privacyasexpected

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

Mark: The concept is a person sending a privacy controller credential to get witnessed or notarized to establish the person's privacy rights. Privacy broadcasting uses standards, this is the button or link to use your rights, rather than accepting (clicking through) a privacy policy. It would have a link to your privacy rights. We're exploring what that is by defining a privacy controller credential.

Sal: The browser could automate that process.

How can a person capture the privacy controller information and create their own cookie?

This can be made easy by the creation of a privacy controller credential which is publicly available and can be used as a basis to create receipts that can form a privacy agreement.

Making this information available (discoverable) and operational is the key to privacy broadcasting.

Consent by default is needed for privacy by design.

Clearly we need a new flow.

One that creates a record of your preferences.

Use ISO 29100 (a free standard) as a privacy framework

A Consent Gateway with a Notary service can provide proof of notice as evidence of consent

This is distinct from a contract agreement.

Receipts are compared over time to see if there are changes.

Notices of changes are broadcast

Centralized control of preferences and decentralized governance

What does it take to make this privacy state machine and how to make it available and public?

Trying the elevator pitch ….

Providing controller information and consent by default is consistent with the 1st and 4th amendment.

For example its imp

Prefix to the consent receipt is the anchor record which is your own cookie about the nature of surveillance and then move onto the creation of a receipt/proof of notice, these two factors (notice of risk and proof of notice) establish conditions for decentralized governance of online interactions.

Gaps are regional (interregional).

Scott David:
Don't conflate consent and permissions.

Data vs. Information

Reference to Rothman…
We need to be able to negotiate.
4 torts

Negotiation:

- Consent is a sorry second to negotiation, battle of the forms..
- Who controi the terrms - offer and acceptance
    - Privacy Agreement - to put forward privacy framework for contracts
        - Accept our terms
            - Binding terms

4 tortts on privacy

1. Peeping tom - intrusion
2. public ation of public facts - false light
3. Defamation - reputational harm -
4. mis-appropriation (publicity) - a right of publicity -
    1. 1906 NY - flour of the south

Convert a tort to a contract - or to a code of practice -- >>

- Unconscionable Conrtact -- too bundled -
    - Cant be understoond - which means you go back to tort

First Amendment - Only to gov - not companies

- Right to access info --
- Freedom of association

Individual rights vs. privacy rights
Bob Gellman - Fair information practices a basic history
https://bobgellman.com/rg-docs/rg-FIPShistory.pdf

Self-regulatory entity of individuals needs to ride along on other rights questions to deliver
Control the record, you can use multiple tools to enact rights preferences
Contact for a bank account for information, and the responsibilities of anyone else in possession.
Transferring the warehousing and duty to the data holder <- in front of the receipt.

Privacy is the human facing component of a contract
Interoperability is equality of duty in this case

FROM ZOOM CHAT:
From Mark Lizar2 to Everyone: 05:49 PM https://docs.google.com/
From Mark Lizar2 to Everyone: 06:16 PM https://wiki.hyperledger.org/display/ursa/
From Scott David to Everyone: 06:40 PM The Right of Publicity - Jennifer Rothman
From dsearls to Everyone: 06:42 PM
https://www.rightofpublicityroadmap.com/
https://www.hup.harvard.edu/catalog.php?isbn=9780674980983
https://www.amazon.com/Right-Publicity-Privacy-Reimagined-Public/dp/0674980980
From dsearls to Everyone: 06:48 PM Scott, given the problems with "privacy," how would you change the mission wording for IEEE P7012? It currently says, "The standard identifies/addresses the manner in which personal privacy terms are proffered and how they can be read and agreed to by machines."
From windley to Everyone: 06:49 PM Very quaint thing: legislators saw a harm and addressed it!

Idea to map rights to contract - so that provider of rights can provide contract upstream on services - b2b

- Rights

Practical Intro to KERI: What Can You Do Today?

Wednesday 14K
Convener: Phil Feairheller
Notes-taker(s): Phil Feairheller

Tags for the session - technology discussed/ideas considered: KERI KERIpy

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

Slides for the presentation can be found here:
Practical Introduction to KERI: How Can I Actually Use it Today

In this presentation we introduced the KERI command line tool “kli” and used it to introduce, demonstrate and explain the basic concepts of KERI’s key management.

We started with basic inception of the 2 types of identifiers, non-transferable and transferable and moved on to perform key rotation, anchor data into a KEL and finished with delegation and creating a multi-signature group.

We ran out of time and did not have any discussion beyond answering questions during the demo to further explain topics covered.

Notes Day 3 Thursday October 14 / Sessions 16 - 24

Let's Talk About Layer 1

Thursday 19A
Convener: Richard Esplin
Notes-taker(s): Stephen Curran

Tags for the session - technology discussed/ideas considered: Ledgers, Layer 1

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

Introduction:
Richard - Evernym

- Recent investigation with cheqd on different ledger implementations
  - Chose Cosmos
  - There were a lot of options - Polkadot, Ethereum, etc.
  - There were new options
- Evernym plans to support several ledgers
- What are the other ledgers that people plan to support?

Rouven: Difference in terminology -- Ethereum/Bitcoin terms Layer 1 and Layer 2.

- Different from ToIP Layers 1 (DID layer)
- Contrast - Ion is a ToIP DID Layer 1 that uses Blockchain Layer 2

Context to start here -- where do you want to anchor DIDs? But could lead to discussions of tokens, governance, payments etc. Rouven questions if those are the same problem, or at least have the same solution. Separate DID rooting from tokens/payments -- separate ledgers.

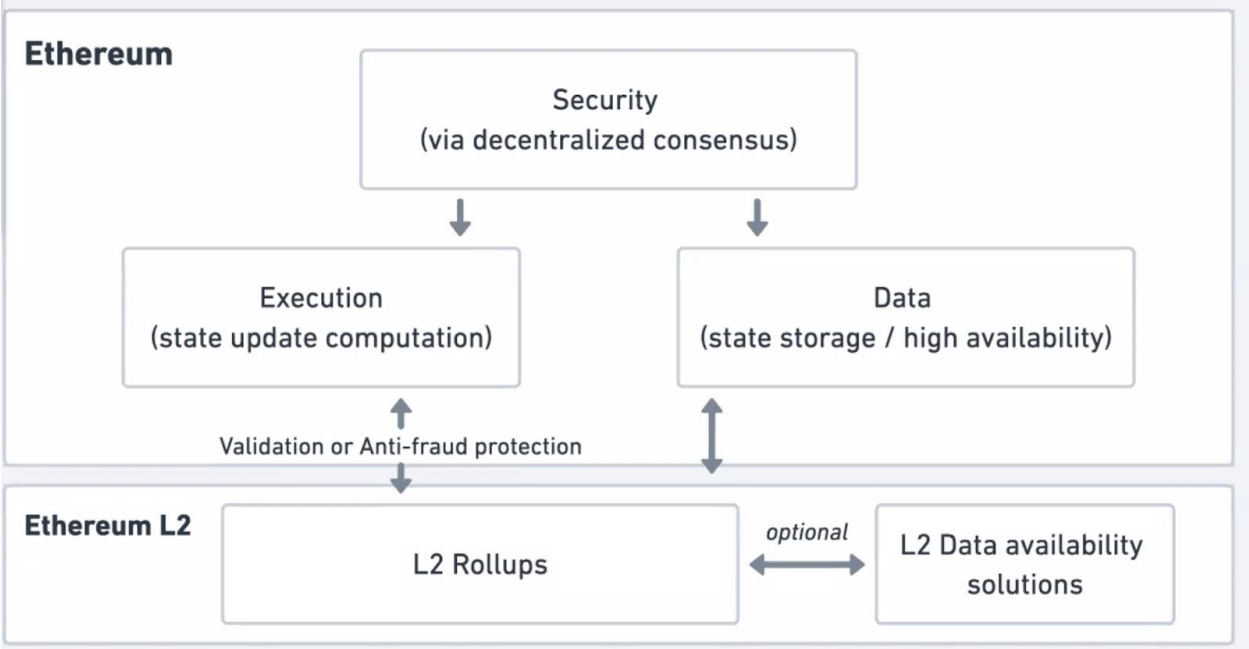
Richard -- networks often want to be all-included, but application developers might prefer to pull features from various locations. Assembly is likely: DIDs in Sovrin, Ethereum tokens, Google Doc for Governance, etc.

Networks

- Evernym
  - Indy (Sovrin, ID Union)
  - cheqd
  - Ion
  - Ethereum
- GLEIF -- KERI
  - KERI tunnel to Indy network (ATTRIB points to key event log)
  - Pilots for Ethereum and Quorum
  - Instead of Witness pool, uses a ledger as registrar to the ledger
    - Essentially, KERI is the Blockchain Layer 2, anchored to the ledger
    - KELs are the Layer 2
- Rouven
  - Ethereum, Layer 2

    - Polygon (Ethereum) — PoS ("Proof of Stake" vs. other meanings) instance of Ethereum
        - Compatible to Ethereum with different tradeoffs
        - Bridges are easier to use
        - Other versions of these are Layer 2 networks rooted in Ethereum
            - Do transactions, etc. at Layer 2
            - But can always go back to Layer 1 to access tokens
            - Layer 2 Computations offchain, ZKP put on Layer 1
                - Link to list of Ethereum layer 2 networks: https://l2beat.com/
    - Ion — easiest, scalable
    - Vision:
        - Don't have to trust a Layer 2 vendor (e.g. MS), but can create your own transactions to anchor to Layer 1 Blockchain.
- Other Indy Networks
    - ID Union
        - Currently setting up an external endorser.
        - Currently it requires a number of signatures to join the network — paper-based.
        - Working on automated alternative.
    - Governmental ones
    - (I missed some, please add)
- Token is "great for Governance" — Richard
    - Why?
        - Sovrin Governance is by people and documents
        - Token incentivized — pay for play for proposals
            - Submit stake with proposals
                - If accepted, get reward
                - If rejected, lose stake
                - Voting is with the token.
            - Example - cheqd
                - Starts centralized, but as more join, becomes decentralized.
        - For technical operations for securing the network — goal is to have a global network with incentives built into the network vs. paid out.
- Performance — Cosmos is higher performance because of Consensus
    - Order of magnitude performance (TPS) and larger (number of nodes) vs. Indy
- With Layer 2 protocols, can optimize for different metrics.
    - E.g. optimizing the writing and reading of DIDs
- Funding the Utility
    - Incentivized development of the utility to increase token value
        - If you have tokens, you want more — e.g. startup mentality, those in early want to drive up the token price over time
            - Economic mechanisms shift over time, impacting the security model — e.g. Bitcoin
            - Management trick is how to keep moving without spending your tokens
        - Voting to pay utility providers
    - Incentivized operation of the network
- Evernym/cheqd — reviewed a number of ledger implementations, set criteria and evaluated to make their decision to use Cosmos.
- Question from Rouven — why build token into network for storing DIDs vs. keeping payments separate?

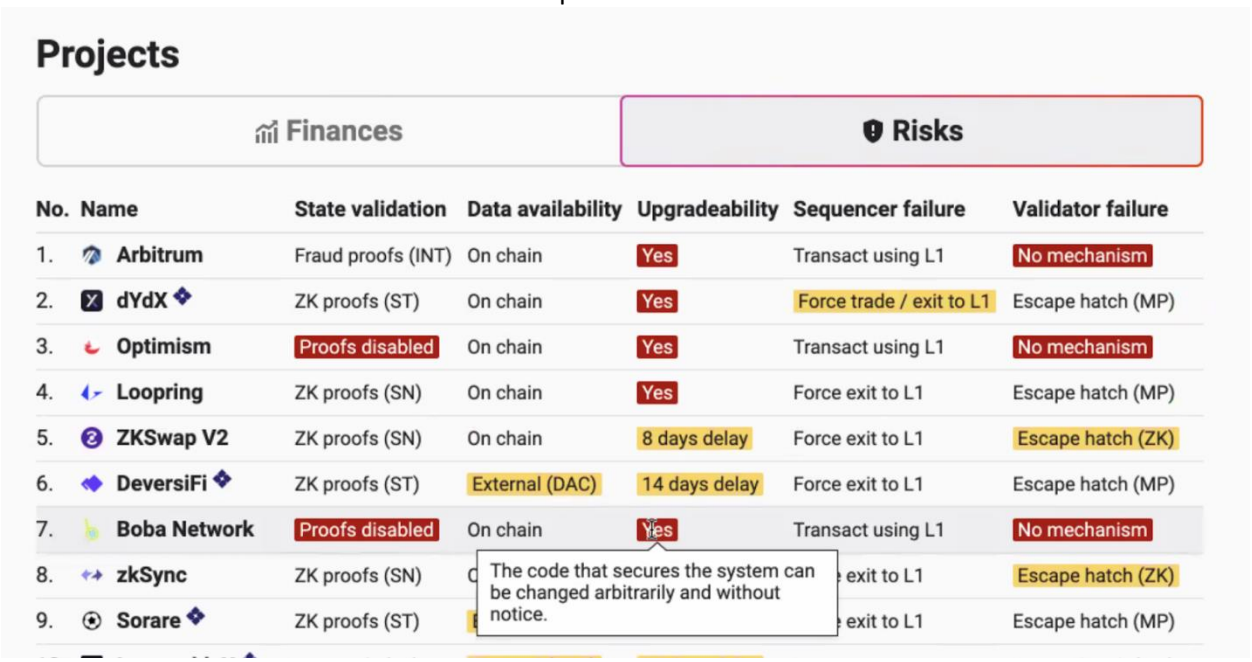
    - Kaliya — SAFts are driving that — those that funded launching Indy/Sovrin (2017) and now cheqd (2021).
        - Lots of ugliness behind the scenes as a result of that.
    - Richard — cheqd is offering a single network for all capabilities in a single place is a valuable business. Makes it easier for some that want that "all-in-one" vs. going to multiple places.
- Operators can become a challenge for global networks where liability can increase as use builds up and geo-political issues come up. Is the risk worth the benefit?
- What about other DID methods?
    - Anyone using them?
    - did:web is important to leverage existing infrastructure / DIF "Well Known"
        - Starting place for company/organization IDs
    - did:key — everyone using
        - Just sending public keys ;)
    - Hadera
    - Kilt (Polkadot)
    - Cosmos Cash — intended to be the default DID Method on the Cosmos inter-blockchain
    - did:evan (public permissioned ethereum based network + polkadot + IPFS)
- Business Partner Agent (BPA) — public profile VCs — publish information
    - https://id.eecc.info/profile.jsonld
    - Based on ACA-PY on HL Aries, including Indy AnonCreds and BBS+ VCs
- Rouven draft mental model of Layer 1/2 on Blockchains:



    - L2 enables optimizing for extreme performance for metrics of an execution and/or storage — data, TPS, etc.
    - For DIDs, that means doing things like all the content and logic is on L2 and the only checking is the "who is allowed to update" — that security layer enables.
    - Polkadot does that separately. Cosmos combines onto the same ledger.
- Discussion on the state of Ethereum L2 approaches by reviewing l2beat.com
    - Most popular with Finances and the technology used:

No.	Name	Value Locked	7 days change	Market share	Purpose	Technology
1.	Arbitrum	$2.19B	+27.26%	60.89%	Universal	Optimistic Rollup
2.	dYdX	$811M	+11.63%	22.51%	Exchange	ZK Rollup
3.	Optimism	$258M	-0.67%	7.18%	Universal	Optimistic Rollup
4.	Loopring	$113M	-1.68%	3.14%	Payments, Exchange	ZK Rollup
5.	ZKSwap V2	$80.30M	-0.16%	2.23%	Payments, Exchange	ZK Rollup
6.	DeversiFi	$47.02M	-11.99%	1.30%	Exchange	Validium
7.	Boba Network	$38.56M	+1.11%	1.07%	Universal	Optimistic Rollup
8.	zkSync	$16.57M	+0.92%	0.46%	Payments	ZK Rollup
9.	Sorare	$15.22M	-14.62%	0.42%	NFT, Exchange	Validium
10.	ImmutableX	$13.21M	+15.74%	0.37%	NFT, Exchange	Validium
11.	ZKSwap	$5.82M	-4.76%	0.16%	Payments, Exchange	ZK Rollup
12.	Aztec	$3.31M	+3.38%	0.09%	Private payments	ZK Rollup

-
  - Risks associated with the various L2 implementations.



- Per Rouven — expectation is that L2 will become “the way” to use the networks and only the L2s will be using the L1, with ability to access tokens at L1 if necessary. L2s are optimized for cost, storage etc.
  - The only thing that L1 is for is the token update and signature checking, with tiny proof that the L2 is correct.
  - L2 can’t steal your money — they can block you, but if they do, you can access L1 to get your tokens. But those txns you have to pay the full price. When using L2, the L1 txn costs are distributed across the participants in the L2 transaction.
  - NFTs are using L2s to eliminate the cost of gas from the transactions.
  - Question — is there a concern about spam if no gas? Do you control who can use it?
    - Totally up to the L2 implementation — optimized for the use case.
    - Incentives and disincentives can be applied.
    - Don’t have to worry about security, because users can go to L1.

JSON Web Proofs - JWTs with Superpowers

Thursday 20A
Convener: David Waite
Notes-taker(s): Andrew Hughes

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

Github: https://github.com/json-web-proofs/json-web-proofs
Slides:
https://github.com/json-web-proofs/documentation/blob/main/JSON%20Web%20Proofs%20IIW%20XXXIII.pdf
DIF Applied Crypto Slack: https://difdn.slack.com/archives/C021JUSRXC0

Notes:

- 40+ attendees
- Work happening at DIF
- Screen shots of slides follow - go to the github link above to get updated versions

JSON Web Proofs
What it is

- Data container for supporting "anonymous credentials" style use cases
- Features such as:
  - Selective Disclosure
  - Multi-use without linkability
  - Predicate Proofs

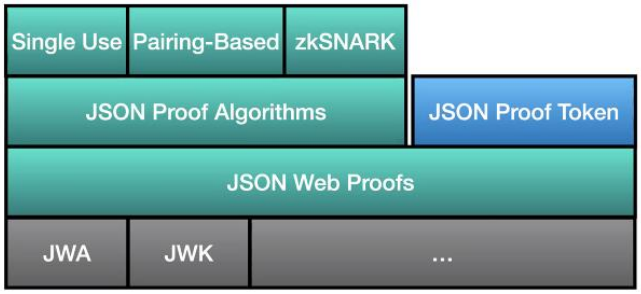
- Supports a wide array of algos

JSON Web Proofs
Standards Relations

- Incubated within Decentralized Identity Foundation Advanced Crypto WG
- Very Early!
- JOSE (JSON Object Signing and Encryption) inspired
  - Various JWA, JWK, JWT dependencies
- Would like to see it moved to IETF following incubation
- Also motivated to define an equivalent CBOR-format container

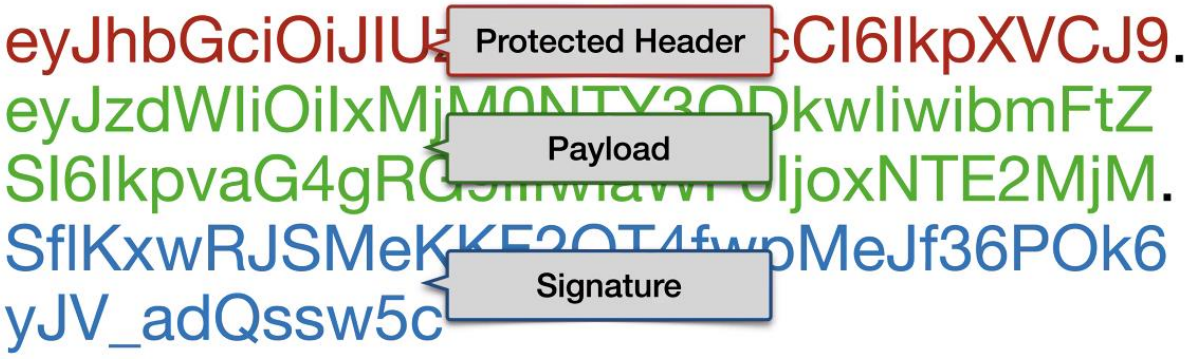
- DIF group = Applied Crypto WG
- IETF has their own crypto tech research group

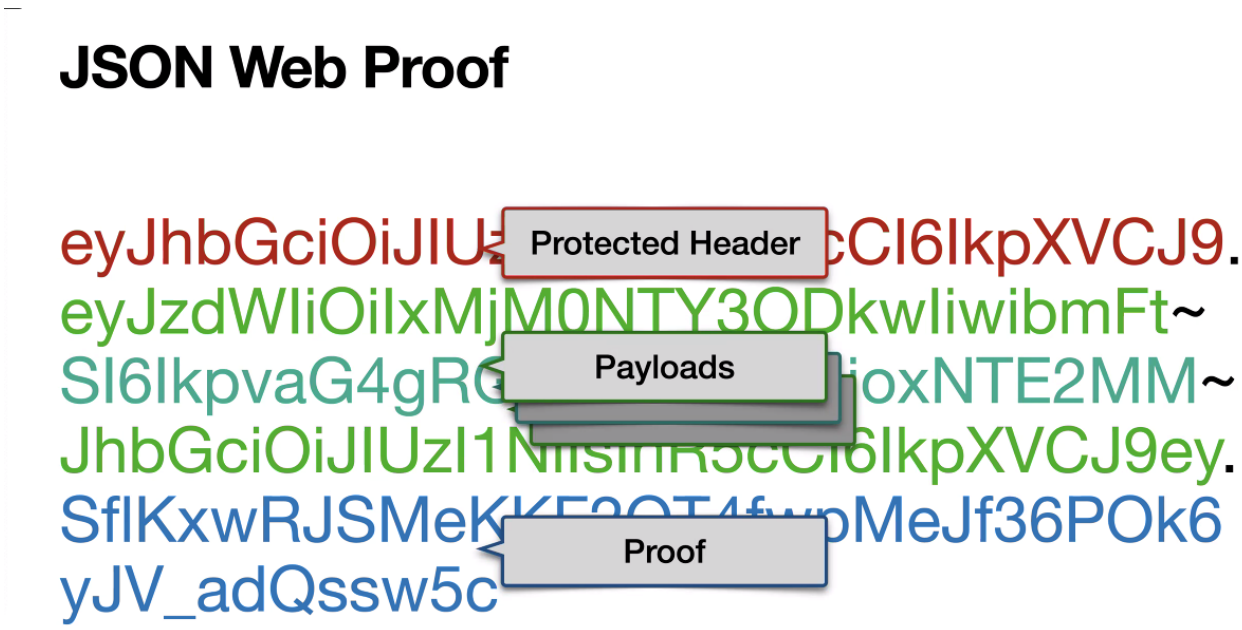
JSON Web Proof Structure
(As envisioned)



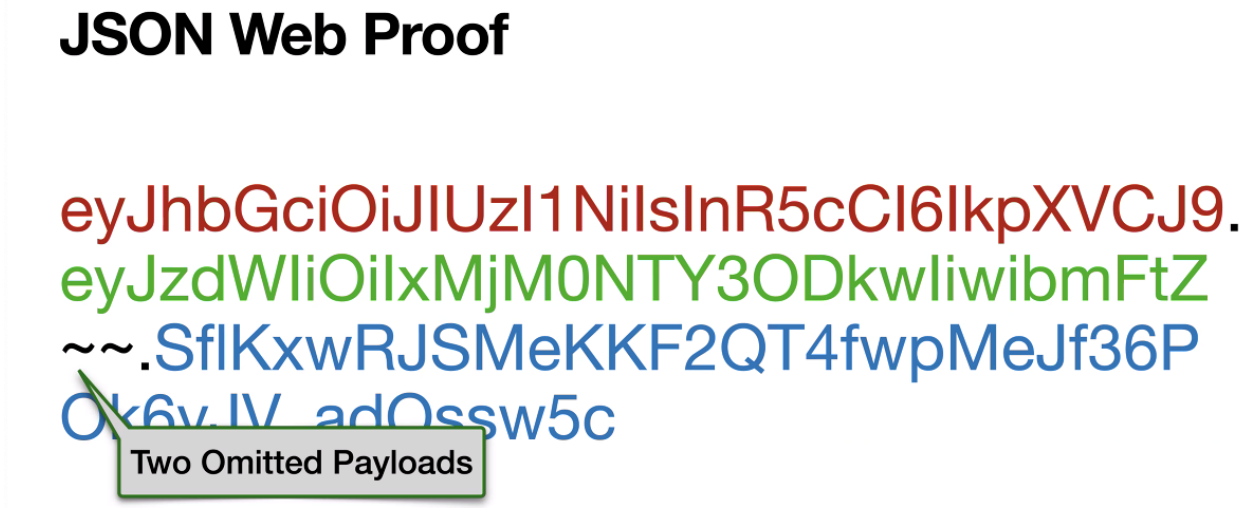
-
- JSON Proof algorithms - defines the primitives needed for the algos
- Top layer - a realization of how to use the system

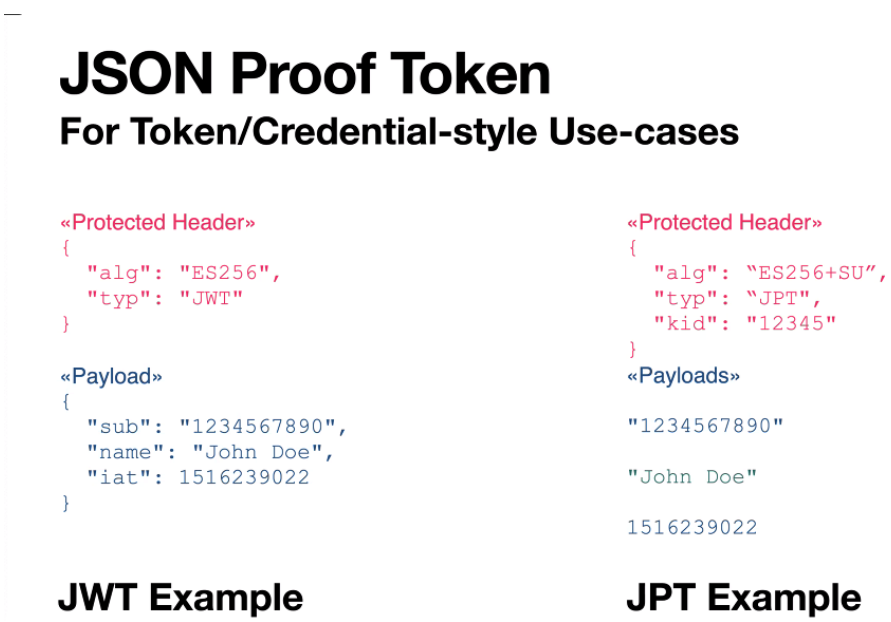
Classic JSON Web Signature

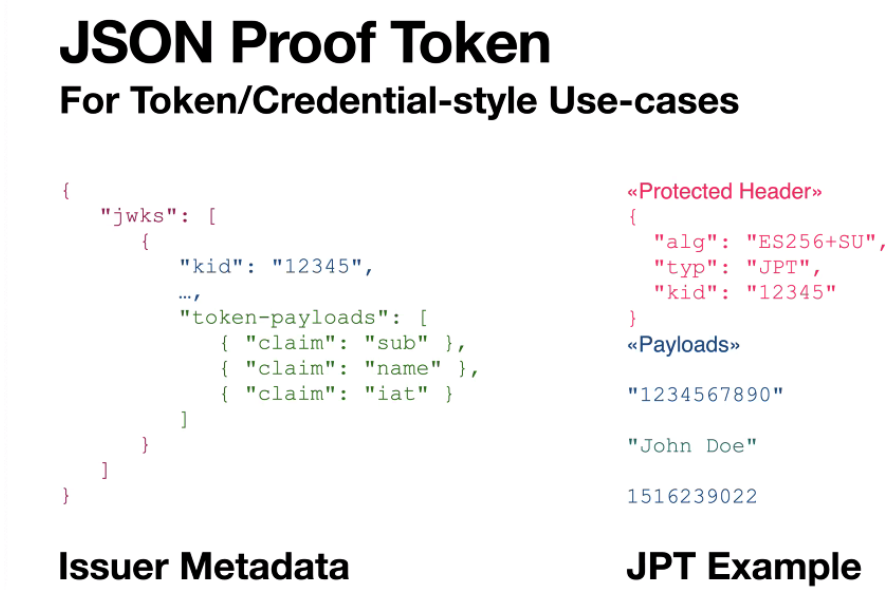




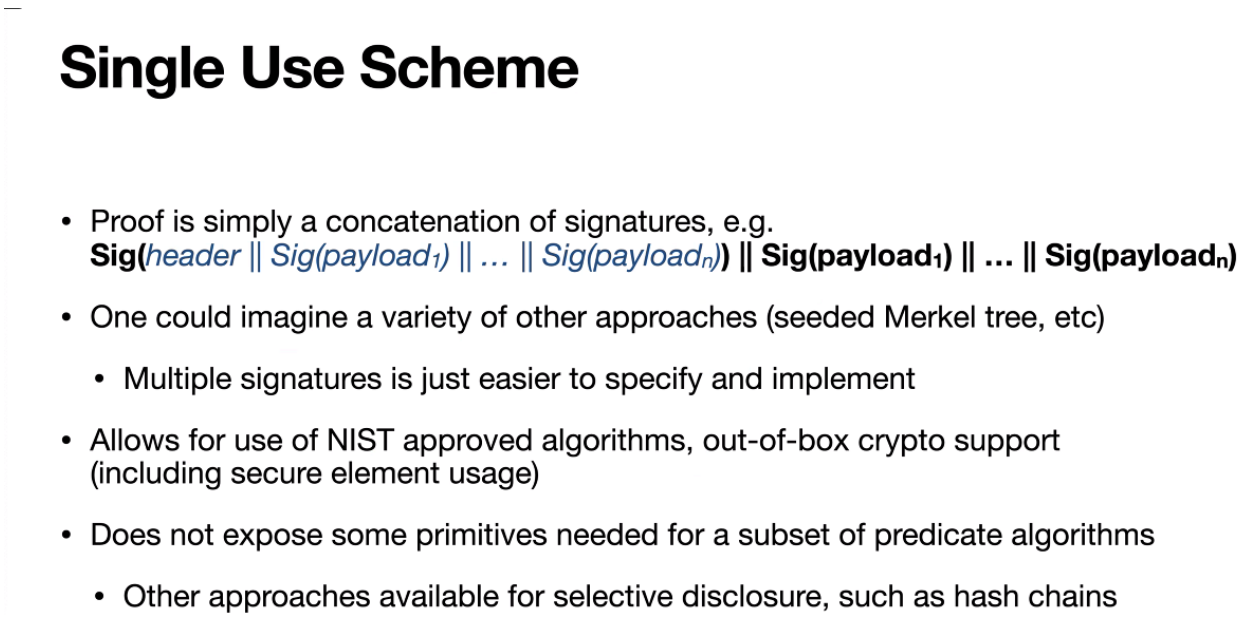
- Similar to JWS - but has multiple payloads
- Can omit payloads





- 

-
- The issuer metadata defines how the right side should be interpreted
- Q: is the jwks normative? Wonders about the presence of the token-payloads
    - A: not finalized yet - need some level of metadata in there
- Q: is the token-payload an ordered list? A: yes
- Q: The threat model makes sense (of not wanting to leak # of claims etc), but doesn't the token-payloads property do that?
    - A: yes - to the same degree that a particular kid at a particular issuer does



- When doing selective disclosure & reveal some and hide others - the proof value itself will include randomized proofs of each value whether or not it's revealed
- Q: What's the strategy for preventing a holder generating a JWP and handing it to another person who presents it on their behalf?
    - A: a bit out of scope. But it comes down to the binding at issuance. The JWP is created by the Issuer - to it's their level of assurance/binding - hardware bound? Software bound? If the issuer gets a hardware attestation, then there' stronger prevention for private key sharing. If private key in software there's not much to prevent.
    - A: could emit several VCs, some of which are strongly bound
- Q: most zkSnarks require a trusted third party - who is that in this case?
    - A: it will be part of the algo - e.g. if you use this algo, you need a 'trusted setup' - might be the trust framework.
- Q: if have zkSnarks, why support selective disclosure? SD just slows down the rate at which people find out your data. All the privacy attacks boil down to a verifier being able to arbitrarily choose the challenge. Sees no projects that define what a challenge is - and force a verifer to commit to what kind of challenge must be. Verifier could ue a "20 questions" attack. Selective disclosure allows fingerprinting holders so they can be tracked between presentations. Humans won't be able to monitor the challenge-responses fingerprinting. Need a commitment by a verifier in the form of a verifiable computation. So holder can check their verifiable computation in advance. Arbitrary challenges formed by the verifier is a chosen text attack on privacy.
    - A: Presentation exchange is the problem, not selective disclosure. However JWP is the container - not the policy of how the interaction works.
      @David Huseby: I 100% agree, and it's not been addressed anywhere yet: https://github.com/decentralized-identity/presentation-exchange/issues/204
- Q; interesting - if i codify my privacy policy about my need for specific data - is there a legal binding at the protocol level? Verifiers need to define their data requirement and and the data use policy - should we push this into the protocol? No. But verifiers should have to codify it into machine readable.
    - A:

- Q: Could I think JSON + JWP as a kind of simpler alternative of JSON-LD + LD-Proof?
  For me it looks like: JSON + JWP === JSON-LD + LD-Proof - LD*
  (*: data linking feature with complex RDF things...)
    - A: Dan: yes, that is a goal, both a simpler alternative but also one that supports a wider range of capabilities
- Q: Responding to statement that people are not aware of algo properties and consequences. Please all educate each other - we need to increase 'known' stuff.
    - In the work - we are working out the proper layering. There will be more situations that will need more knowledge about the choices implications/consequences to avoid problems.
- Q: strongly don't disagree ;-)
    - Highly encourage joining the Applied Crypto slack and mailing lists - good discussions
- Q; about binding, its an open research question - no final answers yet. Can use verifiable computations to do deciding functions to avoid having to share private data _ever_
    - Want's to hear about the research
    - There's a tacit assumption that for humans a biometric will be sent along with the selected disclosure - e.g. a photo along with covid certificate
    - We will need to tie the hands of the verifiers so that they must reveal their business logic
    - Huesby wrote an essay in the Applied Crypto chat :-)
    - **DIF Applied Crypto Slack: https://difdn.slack.com/archives/C021JUSRXC0**
- Q: isn't this the point of Presentation Exchange? RP telling Holders what they want to receive in the presentation? It's hard to get down to a single set of expressions due to the broad range of requirements. Eventually PE will include the ability to state that a presentation must conform to a specific trust framework or specification.
    - A: Yes - that's exactly the thing.
    - A: envision that a credential request could be the equivalent of a Swagger/OpenAPI document
- Q: Where is the use case for using the signature scheme- what's the added value to the existing schemes?
    - A: The approach combines the selective disclosure and the unlinkability - to ensure that nothing in the container makes it easy to introduce linkability. Also to easily drop in different signature algos. So they can all use the same container format - just like JOSE patterns do - same approach.
- Q: Was in the UProve TAG - experience with integrating it for application layer. Didn't need new specs/formats. What's the pitch/justification/need for a new format?
    - A: One objective is to support multi-use credentials. This allows the Holder to present multiple time to multiple audiences - without causing linkability by default.
    - Current view is that thi can't be achieved by existing JOSE specs.

CCG 101: Get Involved With Standards/Pre-Standards at the W3C

Thursday 20B
Convener: Heather Vescent
Notes-taker(s): Heather Vescent

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

Went over this CCG 101 presentation: Intro to the CCG v1.pptx

Limitations of technologist viewpoint, need for humanitarian viewpoints, for the future, for freedom.

Teach Me About MOSIP

Thursday 20C
Convener: Phil Windley
Notes-taker(s): Trent Larson

Tags for the session - technology discussed/ideas considered:

Federated identity, Aadhar

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

Modular Open Source Identity Platform (Source Code)

(Below is from 30 minutes into the discussion. I gather the context is: someone has discussed whether SSI could help or apply in MOSIP.)

Aiming at government organizations, so it's a federated system and the user doesn't have control of their own ID.
It's valid to have a government-issued & government-controlled ID.
However, to have a 30-minute timeout on all IDs doesn't match the issuer-holder-verifier system... the holder cannot present their credential elsewhere.

MOSIP - Privacy and Security by Design

The underlying encryption is a good step, but they could do better with credentials that match SSI and allows for innovation (eg. independent verifiability).

But we don't want to jump into the cryptography & technical.

They don't typically have edge devices so we'll want to introduce a guardianship model.

Aadhar has a reputation for serving residents rather than being a good national ID (eg. migrant issues).

Nicky:
Development community is moving from a focus on logistics to a focus on value, so that could help with the message.
EIDAS 2 & interoperability with EU/GDPR could be another selling point.

Phil:
Accounts & token-based systems are two different models of value.

Nicky:
1) Gov provides account for permissions (eg. ration cards)
2) There are experiments with government tokens to access services
3) Community currencies may provide value in a locale
Huge swaths of aid get gobbled up by government players, so if you can get the value directly to the people P2P, that's huge.

Phil:
Knowing how to build your account system doesn't translate into knowing how to build a token system.

Nicky:
The aid community is measured in many ways but data is critical. SSI can help the funding organizations track the real impact.
Talk to Peter Simpson.
Also Amit Sharma from Finclusive
Also Sovrin's The Rulebook

Phil:
Want to help with financial inclusion.
Morocco, Philippines, & one other have "adopted" MOSIP.

The Self Sovereign Identity Revolution will Not be B2B

Thursday 20D
Convener: Adrian Gropper
Notes-taker(s):

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

The Zoom chat for this session is really good. Look below the outline:

- **Public Blockchain Inspiration applied to SSI**
- A single name as a communication control handle
- Organizations are the gatekeepers of digital trust and we're stuck with the model they will accept - organizations first - Issuer / Holder / Verifier model first
- Wallets can be coercive as in ankle bracelets for every kind of credential
- **Communities can dominate instead of enterprises**
- Get a popular P2P tool first and then business will add on
- **SSI conversation has been 90% about companies and what they do**
- SSI has to work for individuals first - "I take one look and I want it"
- SSI fails as a marketing message - it's a social and societal problem - NGOs and popular orgs are our hope
- Incentives are a challenge - SSI is not in the interest of the sovereigns - social and political challenge
- Institutional (bank) fears that the wallet will go to the OS - the wallet is a touchpoint with the customer and the companies lose (Google Apple Exposure Notification example)
- Sign In with ETH as a race to the bottom for wallet user experience - no API for policy management
- Is this an adversarial issue (facebook? example)
- Does Trust over IP have to be reconstituted to have a broader base of participants
- What kind of "space" is the online space? It's overwhelmingly corporate (not like home or community)
- **SSI needs to be like cash - we all know how it works** - it's not complicated - can be good for enterprise
- Facial recognition with SSI?
- If we can be in a Person 2 Person way instead of the platform way - Rohan's Modern Markets - too much concentrated power -
- Need communities to connect with each other directly
- Standards are not that important
- But what about regulatory capture? Communities can't do much about that - use the farmers market model - local currencies
- **Can regulations help us?** - Is there a way for SSI to leverage government? Wingham Rowan identifies what "modern markets". are in this video. https://vimeo.com/showcase/8884996/video/620052773
- Coop examples as good regulation in credit unions, mutual insurance, some electric utilities
- Joyce's point about trying to build something on a community level rather than a global scale reminds me of the notion of SSI Assurance Communities as introduced in this article:
- https://www.researchgate.net/publication/348325716_Decentralized_SSI_Governance_the_missing_link_in_automating_business_decisions
- Medical regulation as a model - balance between FDA central and MD licensure distributed
- Is GDPR enough? No because federated learning is the real societal issue

- Can associations play a foundational role? Let's get the existing communities to build stuff in their own self-interest
- **How would the broader social justice community understand SSI** - values of self-determination - choice - step back form SSI - it's a pierce of a bigger issue
- Heinz vonFoerster's "Ethical Imperative"
- Control over trust - how?
- Need reputation work in the SSI community context
- How does reputation work in the real world? Gather information about the other… Figure out a way to do this at scale in the digital world? We're going the wrong way in the digital world

---

The chat for this session is really good:

ZOOM CHAT:

10:34:05 From Adrian Gropper to Everyone : https://docs.google.com/document/d/1TdpExrGc_98akMmKV3P1Ac5_DmX1EAlaOLdrpSP5VQc/edit
10:40:00 From @PrivacyCDN to Everyone : Is there a URL where the objections to the DID spec are written?
10:40:26 From Mike Parkhill to Everyone : I just found this news article: https://itega.org/2021/09/24/why-mozilla-is-opposing-user-control-over-identity-billionaire-kicks-off-effort-to-challenge-social-networks-with-distributed-identity/
10:41:01 From Steve Todd to Everyone : @PrivacyCDN see the notes from yesterday's session: https://docs.google.com/document/d/17nhNNImluaElKsCl9AMWixra5cfl1HDFOKgQVxsUt6I/edit
10:41:36 From dsearls to Everyone : To me SSI should be about self sovereignty. More than 90% of the conversation I hear about it, however, has been about what businesses do, or do with each other. Which is fine, as far as it goes. But to succeed it has to work for muggles in a way they understand. And I see relatively little talk about that.
10:47:46 From Mike Varley to Everyone : Here is the link to the forma DID objection: https://lists.w3.org/Archives/Public/public-new-work/2021Sep/0000.html
10:50:45 From @PrivacyCDN to Everyone : Thanks @Mike and @Steve
10:50:51 From dsearls to Everyone : To me saying SSI should start only with organizations is like saying personal computing should have started with mainframes, or browsers should have started with servers. If you leave personal things up to organizations, you have a different personal silo for every one of those organizations. That's what happened to CRM—customer relationship management. It was meant to be a way all orgs could relate to all customers. Instead it became, as a B2B thing, a way for every company to relate to customers in their own special way. And that ended up sucking.
10:51:17 From Marc Davis to Everyone : +1 Doc
10:51:40 From @PrivacyCDN to Everyone : Noting that we don't own software, including wallets.
10:52:11 From Marc Davis to Everyone : A wallet per organization seems a likely outcome of letting organizations control wallets.
10:52:40 From Timothy Ruff to Everyone : Reminds me of the early internet, when every organization thought they had to have their own browser, too...
10:53:00 From @PrivacyCDN to Everyone : I suspect that the best (?) we can hope for is a single wallet per device we carry.
10:54:27 From Chris Matichuk to Everyone : If wallet moves to single wallet, I could see this becoming an OS component, or part of the top authenticator apps. Doesn't the MS Authenticator already have support for VCs?
10:55:13 From Alan Karp to Everyone : I don't think that's viable. How would I interact with the same organization from two devices?

10:55:27 From Timothy Ruff to Everyone : Until there's a business model of giving to consumers what most of them will expect to be free, we are stuck with business models that incentivize organizations to move to an issue-hold-verify model, which plants the seeds for SSI
10:56:03 From Timothy Ruff to Everyone : Gotta run... thanks for the useful convo, all... :)
10:57:37 From Mike Ebert to Everyone : +1 to incentives, both for Bs and Cs
10:57:46 From Fraser Edwards to Everyone : +1
10:58:27 From Mike Ebert to Everyone : There will need to be political, social, AND economic incentives
10:59:47 From @PrivacyCDN to Everyone : Historical sidetone: When the British Empire outlawed slavery, II've seen estimates that this cost the Emprire 2% of GDP annuallly for decades. Sometimes doing the right thing can't depend on economic incentives.
11:00:19 From Marc Davis to Everyone : +1 @PrivacyCDN
11:01:06 From @PrivacyCDN to Adrian Gropper (Direct Message) : Noting that all the speakers so far have been male and white. Any chance of eliciting other points of view?
11:01:14 From Marc Davis to Everyone : @MikeEbert agreed, but economic incentives cannot be determinative of political and social freedoms or we live in a system fo digital feudalism.
11:01:39 From Mike Ebert to Everyone : True, you can't rely solely on economic incentives, but I think In this case there are some that can be used as a carrot (instead of just using sticks) to move businesses along
11:01:41 From dsearls to Everyone : I think calling self-sovereignty a social and political question is true, but it's not the only one. My pants, my car, the wallet in my pocket, are all personal things that I operate in a self-sovereign way. We need the way we present credentials to be simple and organic. Whether it's something which, like the touch feature of credit cards, works simply and seamlessly, that would be fine.
11:01:42 From Alan Karp to Everyone : But there are longer term benefits. There are big local economic losses when a military base closes, but a decade later the local economy is far better than it was when the base was open.
11:03:16 From Marc Davis to Everyone : @Mike and @Doc ultimately its is about power and control and the individual and groups vs. corporate and state power. The economy is a key and unavoidable element of that power struggle.
11:03:38 From TelegramSam to Everyone : I believe Timothy's view is a result of over focus on credentials (the *about*) instead of connection (the *with*)
11:04:09 From Joyce Searls to Everyone : Dave Husby is doing a session next on this topic that he just posted "We're building digital gates to keep people out" Breakout room I
11:04:28 From Mike Varley to Everyone : +1 Chris, totally understand that struggle.
11:05:32 From Joachim to Everyone : ENS Ethereum Naming System
11:05:48 From @PrivacyCDN to Everyone : Thanks for the convo. Doing the butterfly thing today.
11:06:07 From Alan Karp to Everyone : @TelegramSam: Can you elaborate?
11:09:50 From Steve Todd to Everyone : However, regulation generally just benefits the incumbents.
11:11:47 From TelegramSam to Everyone : Credentials are centered in orgs as the issuers
11:11:52 From dsearls to Everyone : I think some times and in some ways, the interests of businesses, large as well as small, are (or can be) aligned. By that I mean we all agree to speak the same language, drive on the right (or the left), and behave in polite ways with each other. This is not to say that large companies, or most of them, will abuse their powers. What I'm saying is that SSI, if it works well and simply, doesn't have to be about anybody screwing anybody else. And frankly, I think individual self-sovereignty does work for some companies. Trader Joe's, for example, succeeds by going out of its way to NOT do game-the-customer marketing as usual, and derives the benefit of minimized cognitive and operational overhead.
11:11:57 From TelegramSam to Everyone : But SSI can be about more than just what other say about us.
11:12:34 From TelegramSam to Everyone : we need to do better connecting people with people and people with businesses, not from a VC perspective, but from an interactive perspective.
11:12:44 From TelegramSam to Everyone : @Alan^

11:13:26 From Alan Karp to Everyone : @TelegramSam: Agree. That's why I try to bootstrap adoption with person to person.
11:13:32 From Mike Ebert to Everyone : ^^^ The interactions can be a way to show the organizations involved that this is good for them, too
11:13:47 From Alan Karp to Everyone : I haven't used cash in months.
11:13:47 From TelegramSam to Everyone : Funding is hard with that, but the spread can be quicker.
11:14:34 From Alan Karp to Everyone : Trying to show the business case to HP (where I was working) is what killed our project.
11:15:12 From Mike Ebert to Everyone : Meaning things were running along smoothly until you told them it made business sense?
11:15:46 From Alan Karp to Everyone : They wanted returns in the next quarter, not 2 or 3 years out.
11:17:37 From Mike Ebert to Everyone : Yeah, that's a problem with business incentives, isn't it... is there a next-quarter return to SSI?
11:20:33 From dsearls to Everyone : @Mike, until it becomes obvious to a business that SSI is just a better way to do things, it won't happen. It will be like we saw with PCs, LANs, the Internet, and smartphones. All were seen as costly threats, before they became obvious necessities.
11:20:36 From Marc Davis to Everyone : What if we looked both to peer to peer for individuals as Joyce and Sam are saying and NGOs, trade unions, and credit unions?
11:21:10 From TelegramSam to Everyone : I believe both work together Marc.
11:21:27 From TelegramSam to Everyone : The hard part is the economics of development.
11:21:44 From Marc Davis to Everyone : @Doc totally agree, but will most of these businesses support true self-sovereignty for individuals?
11:21:58 From Marc Davis to Everyone : @Sam agreed!
11:22:40 From Mike Ebert to Everyone : @dsearls Agreed, I would love to find a way to prove to orgs that SSI is better ASAP.
11:23:42 From Marc Davis to Everyone : If self-sovereignty is something we must first convince corporations to give us, I think we will not achieve true self-sovereignty. The lords of the manor don't give all their serfs freedom.
11:24:58 From Mike Ebert to Everyone : I don't think it's dependent solely on convincing businesses, but it could speed things up or smooth things over if we can in parallel to other efforts.
11:25:13 From dsearls to Everyone : @Marc, they will if there are tools for the job—on both sides, but especially on the individuals' side. I don't see that yet, or much work on it, frankly. I have a Trinsic wallet for my phone, and nothing to use it with. Meanwhile Triassic on its website says—to business, not to me—"share data safely and instantly authenticate participants in your ecosystem, network, or marketplace." That tells me it's selling silos to companies.
11:25:45 From Joyce Searls to Everyone : This guy Wingham Rowan identifies what "modern markets". are in this video. https://vimeo.com/showcase/8884996/video/620052773
11:28:16 From Marc Davis to Everyone : @Doc I actually believe in a virtuous economy of self-sovereigns based on your ideas Doc. The question I am asking is how we get there. My fear is that the current political and economic order has incentives that work directly against individual shaving self-sovereignty and that a purely corporate path for adoption is based on an inherent tension in our current political economy, which would agree for alternate adoption strategies for self-sovereigns to assert and gain power.
11:28:48 From Marc Davis to Everyone : Typo: which would argue for
11:29:33 From dsearls to Everyone : @Marc, it's the innovator's dilemma. No innovator (an incumbent market leader) wants to do anything that threatens to disrupt itself, even if it can see the logic of it. The job is up to the disruptors. Who is disrupting here, and how?
11:30:14 From Peter Langenkamp to Everyone : Joyce's point about trying to build something on a community level rather than a global scale reminds me of the notion of SSI Assurance Communities as introduced in this article:

https://www.researchgate.net/publication/348325716_Decentralized_SSI_Governance_the_missing_link_in_automating_business_decisions
11:31:22 From Alan Karp to Everyone : We got HP to disrupt itself by making the argument, “If we don’t do this, someone else will do it to us.” That got us funded and into the market. Unfortunately, they shut down the product group 3 years later.
11:31:29 From Marc Davis to Everyone : @Doc my question is if the innovation of SSI has to be in corporate space first, or if it requires other spaces in which to be nurtured and gain adoption and power (e.g., P2P, NGO, credit unions, alternate ecoomic and political structures, etc.).
11:32:35 From dsearls to Everyone : @Marc, I don't disagree with that. I do fear that something will be lost when that innovation is done. And it will be what makes the individual truly self-sovereign.
11:33:22 From Mike Ebert to Everyone : Is pitting some bigs against the bigs (like or similar to what Alan said) a good strategy?
11:34:55 From Marc Davis to Everyone : @Doc is that “something that will be lost” the ability of self-sovereigns to truly assert and exercise economic power aa individuals and groups?
11:34:58 From Joyce Searls to Everyone : If communities band together to use common infrastructure, the bigs will notice.
11:35:07 From Marc Davis to Everyone : +1 Joyce
11:39:18 From dsearls to Everyone : I submit that both the GDPR and the CCPA are bad regulations, and good examples of protecting yesterday from last Thursday. (GDPR protects 2015 from 2012.) What makes both bad is that it locates all significant agency on the corporate side. The GDPR assumes that the "natural person" is just a "data subject," and the processors and controllers of personal data are corporate entities. Also that privacy is a grace of those corporate entities' systems for providing privacy. It's totally fucked and has caused enormous inconvenience for everyone, with fatuous and insincere consent notices on websites that nudge visitors to "consent" to exactly what the regulation was meant to prevent. Plus a massive business in providing "GDPR compliance" that's all about screwing the spirit of the regulation while obeying its letter.
11:40:39 From Marc Davis to Everyone : I find it interesting that my question to the group of whether the interests of, and incentives for, self-sovereign individuals vs. corporations are aligned, or in conflict, in the current political-economic order has only been addressed by a few folks here. It seems to me to be a fundamental issue affecting the entire SSI effort.
11:40:41 From Brigitte Piniewski to Everyone : Thanks for the helpful details dsearls!
11:41:06 From Brigitte Piniewski to Everyone : Absolutely Marc
11:41:20 From dsearls to Everyone : The CCPA similarly demotes all of us to mere "consumers," who have rights only (or mostly) to insist that those who have stolen our data horses from our personal barns either return those horses, or not sell them in the horse market, in which we are not involved.
11:41:54 From dsearls to Everyone : Welcome, Brigitte.
11:42:20 From TelegramSam to Everyone : Marc, I'm not sure I know enough about it to say anything intelligent.
11:42:50 From Alan Karp to Everyone : People won’t adopt SSI just for itself. They will adopt a tool that can only or most easily be built with SSI. The trick is coming up with that killer app.
11:43:05 From TelegramSam to Everyone : Agree Alan.
11:43:06 From dsearls to Everyone : Agree, @alan
11:43:14 From Neil Bourgeois to Everyone : +1 @alan
11:43:54 From Joyce Searls to Everyone : +1 Margot
11:46:26 From Timothy Ruff to Everyone : GLEIF meeting ended early. What'd I miss? :)
11:46:46 From Adrian Gropper to Everyone : look at the agenda document -
11:47:02 From Adrian Gropper to Everyone : it’s a series of short bullets

11:47:25 From Marc Davis to Everyone : @TelegramSam, thank you for that Sam, but maybe you can think about this question: Do you believe that most corporations see their goals of profit and control as aligned with supporting the interests of individuals for self-sovereignty?
11:47:48 From Timothy Ruff to Everyone : @Adrian - Within this chat? Zoom erases all comments when people come into a meeting...
11:48:08 From Alan Karp to Everyone :
https://docs.google.com/document/d/1TdpExrGc_98akMmKV3P1Ac5_DmX1EAlaOLdrpSP5VQc/edit
11:48:30 From TelegramSam to Everyone : Session on Reputation on the schedule.
11:48:42 From Timothy Ruff to Everyone : Ah, of course. Thx!
11:51:15 From Timothy Ruff to Everyone : Can't have reliable reputation without first having secure attribution. Otherwise you end up with fake reviews, like what plagues Amazon. Also, negative reputation remains a thorny subject, as SSI holders have a negative incentive to share any negative info about them. This is why CRAs do what they do... someone has to capture the bad news.
11:52:23 From Marc Davis to Everyone : @TelegramSam, or in economic terms to use @Doc's excellent terminology and ideas, how many corporations in today's political economy truly believe that "free customers" will be more valuable to them than "captive customers"?
11:52:43 From Steve Todd to Everyone : Abuse of reputation is one of my biggest fears for the future.
11:52:47 From Mike Ebert to Everyone : We definitely want to be careful of unintended consequences.
11:53:11 From Mike Ebert to Everyone : Gotta run, thanks all!
11:54:33 From Marc Davis to Everyone : @TelegramSam I think my question can be framed another way: do you believe that asking corporations to grant individuals self-sovereignty is the best or right path to our achieving self-sovereignty?
11:55:26 From Timothy Ruff to Everyone : I do, by having corporations find a selfish reason to "give people their stuff". Incentives rule the world, we need to align them.
11:56:46 From TelegramSam to Everyone : BUT TRUST THE ALGORITHM!
11:57:39 From Marc Davis to Everyone : @TimothyRuff, I think this is the fundamental question. Strangely, I think in the case of self-sovereignty, too many companies are incentivized short term to act against their long term economic self-interest.

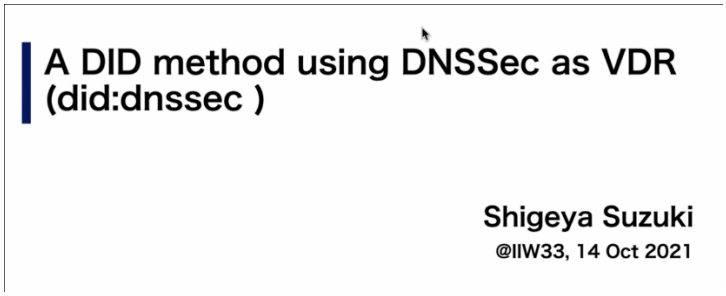
did:dns and did:dnssec

Thursday 20G

Convener: Markus Sabadello, Shigeya Suzuki
Notes-taker(s):

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

https://danubetech.github.io/did-method-dns/



Slides:
https://drive.google.com/file/d/1fdhpXsugdymH-2Jx62xBWIRMOq1430_r/view?usp=sharing

https://shigeya.github.io/did-dnssec-proposal/main/draft-suzuki-did-dnssec-proposal.html

Digital Identity with LEIs - Update on the Verifiable LEI (vLEI)

Thursday 20K
Convener: Karla McKenna, Christoph Schneider
Notes-taker(s): Christoph Schneider

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

The session will cover the use case for the verifiable LEI (vLEI) to provide decentralized identification and verification for organizations as well as the persons who represent their organizations either in official or functional roles, the vLEI Chain of Trust and vLEI Credentials as well as the approach to delivering the vLEI Ecosystem and Infrastructure using an interoperable and technically agnostic solution.

Slide deck: https://github.com/WebOfTrust/vLEI/blob/main/docs/2021-10-12_Update-vLEI-IIW_v1.1_final.pdf

Explainers Needed - Brainstorming The Explainers

Thursday 20N
Convener: Kaliya Young
Notes-taker(s): Kaliya Young

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

The starting premise for this is that there is a gap between community knowledge and what is available for folks entering/making sense of the space. What are the missing explainers that are needed.

- Kaliya wrote one that

Neil - the government trying to sell this as a "replacement" for what you have - digital Drivers licence and digital health card.

- Why privacy is important - what you are giving away that
- How do we arm ourselves and explain it.
- Easy to explain to parents is - privacy issues for children.
- What is in it for me relative to the current ecosystem.
- Dark Actors what can they do with the data.
- Ontario - pitching to the business community saying they will save a lot of money.
- Not reaching out to regular people - use-cases not concerned John Q public.
- SSO - is leaving a trail.

Sebastian - philosopher

- 4 Years in the blockchain space

- DIDs for media content
- Identifier ISO - international standard content code - (is a DID?)
- timestamp/claim rights - could do so with DID/wallet address.

Huge issue - address reach those who would come up with use-cases.

“I tried to read the specs” they are really hard to understand.
Either very superficial - or technical details that are incomprehensible.

Phil Wolff’s session on VC metaphors - important conversation we forget to have - how to break it down for folks outside the space.

How to make accessible to them - understandable but accurate.
Use different metaphor depending on who you are selling it to.

end -user
Business decision maker for investing in it.

Kent Bull-
Number of corporations working with - need to explain to principles and engineers. I want tow rite blog posts to fill in these gaps - I’m a teacher by nature.
Seems big and intractable.

Rob Aaron - career took turn away from this material - was a semantic web guy. Individual to providers of goods and services - schema’s and ontologies - no identity layer. OPen up the world - connections passwordless login through which data can flow.

Henk van Cann - Netherlands - trying to explain to sam smith everything about Keri - documenting it for ½ a year or more. Trying to bring it to a different level of people trying to understand it.

Dan Robertson - hear what folks thoughts - my own experience trying to get ramped up is slow.

So much going way back conceptually - framing what is the problem to be solved.
All the different branches to be explored. Trying to load that context is challenging.

Originally at IIW you could get up to speed - “at” IIW so many different technologies and parties at play.
Can’t get crash couse now.
Explain customers
Increase diversity in the community.

When I hear that it takes a long time to explain - challenge accepted. Can’t explain it simply we don’t know it well enough. Divergence learn and gather information - this is what is really going on.

The things that stick over time - they tend to be simple.
Need a PhD - to understand doesn't’ get adoption.

Some abstraction needed to make it simple.

Keri - paper building on 30 years of academic -

Charles - not in space full time - background
Liked my VC flavors explained.

Clarity for technical people to get distinctions.
Overview for policy makers to understand the choices that were made.
Needs more of that.
WHY are people doing these things
How do thy relate to each other.
People are making different choices based on the context that they are in.

Helpful for capital and business manager.

https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf

CONTEXT for ID Community - sort of pre-SSI
An
DIDComm - lift out of prose - secure point to point communication protocol.
SSI book has work flow - really exciting stuff

Didn't talk about DID resolvers.
Didn't talk about DIDComm - core things that are enabled.

Explanation for common people - why are we doing this?

Part 3 - Decentralization as a model for life
Vision and blue sky - inventory of topics.

Issue with SSI book - they don't resonate with people.
QR Code society <- dangers.

Would like to have artubments for them that resonate with them.

What draws me to SSI - Blockchain - we have a chance at digital control - in heaven - control identity and have true privacy - people can have a voice and can trust that voice being heard.
Voting route - local precinct voting.
Get burnt out - upper party leadership -
Mathematical veracity to local politics - believe they have a voice.

WHERE do we EXPECT the momentum?

- Governance states
- Public demand
- Commercial and economic interests.
- OS comes up with something impressive and convincing.

Selective communication of aspects.

Niel Thompson -
Ultimately we need to explain SSI to policy makers, who are non-technical.

I'm seeing papers from the Canadian Governments who clearly don't understand the current internet problems or what SSI solves and what role "jurisdictions" like themselves have to provide (e.g. governance and enforcement)

What is the role of Public Key Cryptography -
Change of paradigm comes with this.
What is a cryptographic signature and how to explainer.
Metaphor to explain - Can't take off the locks in a steel plant. When you need to lock out a turned off circuit for work or maintenance you put your lock on it. The next technician may come and place his lock on top of yours. Then, in order for power to flow all the locks must be removed.

The Laws of Identity -

What is going on NOW with database exchange - engagement of businesses to reduce risk.
SSI could create a worse world then we have now.

Painting the picture of the NEGATIVE picture well.
I have failed to convince them there is a problem.

https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf
https://ssimeetup.org/how-avoid-another-identity-tragedy-with-ssi-christopher-allen-webinar-53/

https://medium.com/berkman-klein-center/big-brother-a-critique-of-the-4th-industrial-revolution-in-africa-fdcd1a5fdddd
https://www.wired.co.uk/article/kaliya-young
https://github.com/henkvancann/keri/blob/master/docs/KERI-made-easy.md

Maybe also - benefits.
Those papers don't get
Slip privacy and anonymity in the back door.
Cryptographic tools are on peoples phone.

Andreas - Negative picture - experience when talk with developers and technical people - they think they don't need this "everything is solved" - coming from central mind. Not talking about blockchain - DECENTRALIZED ID/IT Architecture.

Why I need this stuff - I've solved this, it works.

2-3 of the key flips

- Privacy approach (they don't care about privacy)
- Operational Security - dont' have central service to run - operation easier - millions of people scalability -
- Scalability
- Openness to other - run digital infrastructure as a government - private sector can join.
- Open room for innovation - count more for governments
    - Give advantage for economy

Elimination of PII - you don't need to store - 'Toxic Data'

Elimination of risk
Reduce friction by eliminate login

KYC-CTF-AML
All you need to do is use a VC that meet your need.

Infinitely scalable low cost Federation

Governments already - issue - spit out VCs - everyone compatible.
RBAC - Strings (role-based access control) - alternative to json web token

Audience - who are we talking to.

Why Governments
Why Businesses
Why Technical people

Talking about drawbacks of

Number of papers
Charles Lanahan

- Different changes different people in SSI make -

More comparison papers

Crypto Curves Flavors Explained
ED22519 vs P256

Credential Exchange Mechanisms.

Governance Model Comparison
WHY people are doing it.

Phil Wolff

- Short form messaging. Where is SSI TikTok? 30 second audio/visual nuggets with high emotional content.
- Distil into one idea - people can pick up on and relate to and share.
- As long as we're in evangelism mode, learn from the best of issue advocates and political communicators. Greta Thunberg, The Lincoln Project
- Propaganda has layers: establishing beliefs and popular support for common values that connect to deeply held worldviews, identity (the old kind) and feelings.
- Public support

Videos like Store Wars
Podcast and video content
Kurzgesagt as channel that makes short explainer videos about science
https://studybreaks.com/tvfilm/kurzgesagt-is-the-youtube-channel-that-explains-science-simply/

Rob Aaron - semantic web - focus on machine-readable information, bottom-up approach
Machine readable receipt - hard road to get critical mass.

Start with something simple that can achieve critical mass - contact list / address book
Behind the scenes what is happening (VC issuance between peers, private channel communication) is transparent and doesn't need explaining - it just works.
Give everyone control of their contacts again - a contact list application - create peer to peer channels. - functionality of communicating - reaching out goods of services. Join and you can connect with the person this way. Then add providers of goods and services where it's key and essential to have real data transfer.

How do we get

Making Facebook Obsolete - the path using SSI

Origination paradigm - publish meme/post on your device and publish peer-to-peer via your new contact list/address book app (there is a scheme a for social media posts).
Publish to wherever. Peers in-boxes as well as all social media / professional networking sites that are participating.

Killer app - explanation after.

Judith - drummond said it just need to work.
Don't need to understand how it works.

We need these explainer documents for us - the masses will take because it works.
There are philosophical disagreements on how it gets built in that

People deploying and non-technical.

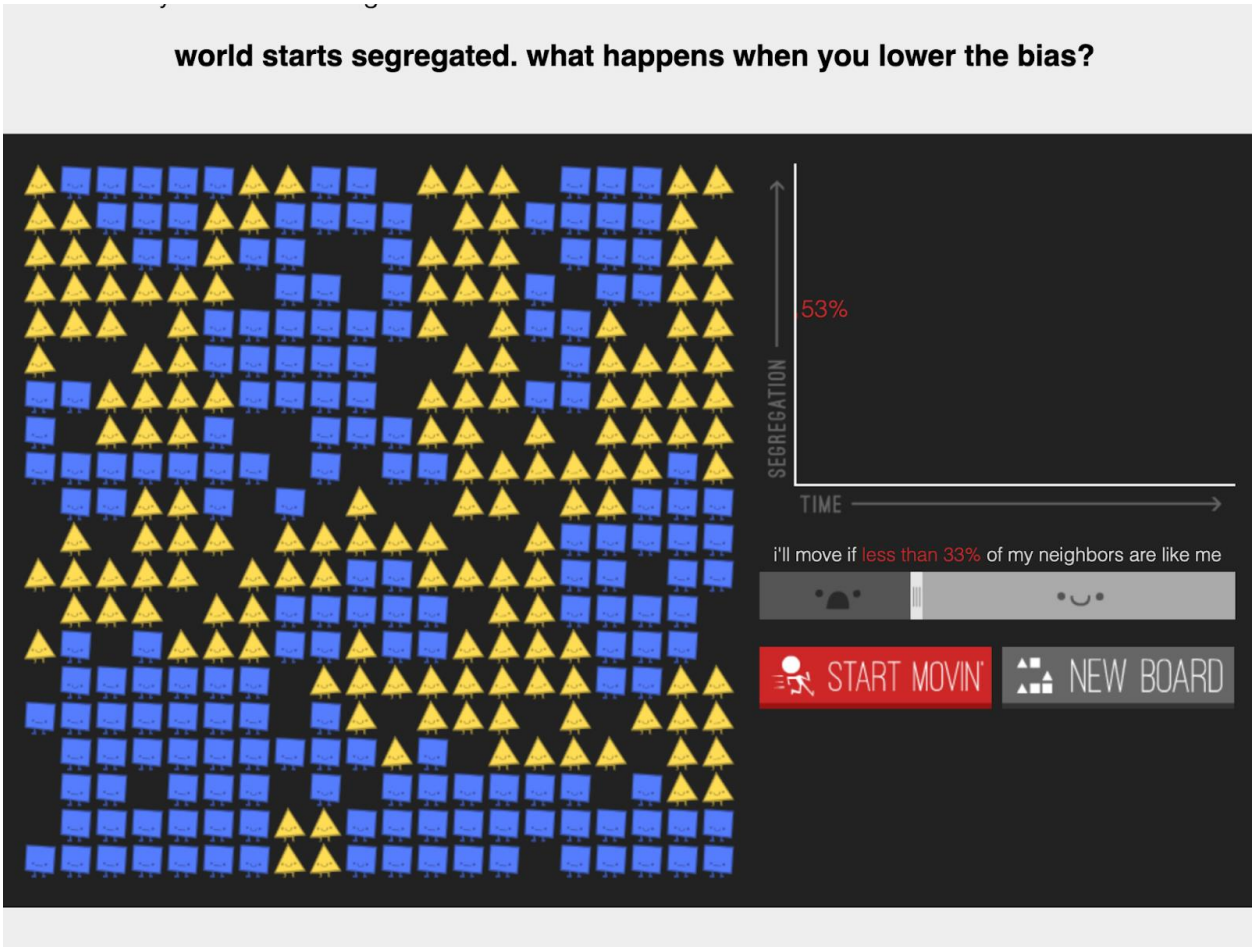
Business decisions makers not technical
Technical people - there is no way I'm ever going to know enough.

You know it's just working when…

The elephant is too big for each of us to see the whole.

Andy - is there a world where we are worried about resources about this - we can
Andy is an designer - UX person suggesting infographics

- Design system mapping is a great technique: https://medium.com/disruptive-design/tools-for-systems-thinkers-systems-mapping-2db5cf30ab3a
- It also allows for talking about societal systems and how ID tech will affect them
- Parable of The Polygons by Nicky Case: https://ncase.me/polygons/



Resourcing the communication effort:

- Employers paying for time to write papers
- NGO with evangelical goals raising funds to pay for creative and media.

MORE DIAGRAMS!!!

Like this - https://www.lfph.io/wp-content/uploads/2021/04/Verifiable-Credentials-Flavors-Explained-Infographic.pdf

Communications within companies about SSI - disconnect between comms and the engineering/tech
Enable comms to understand/equip them with resources to communicate effectively

https://medium.com/webcivics/inforgs-the-collective-info-sphere-67a660516cfd?source=friends_link&sk=29ba4752f9a2ef12b6d2895539b52725

Diagram creation corps - to get key points/differences articulated in visible form.

Why Quebec gov and large corporations decided privacy was important - EU cut them off from all electronic commerce where GDPR compliance was a requirement. Threat of being cut off for not being compliant.

Communicate to LAWYERS! - they are driving decisions inside corporations.

Phil - we need curriculum - organized sequenced
IDPro - put out a Body of Knowledge - not bad if you ignored lack of decentralized identity.
https://bok.idpro.org/

Chunked categorized - step by step mastered a field - Curriculum

Ways to teach people -
Parable of the polygons. Little simulations - segregation in neighborhoods.

What is identity -

Kent - needs more design.

Fibonacci story point in Agile - 1-3-5. Basically you grab a "story", a "task" you need to do, and then you give it a "size".

Narrative story structure.
Diagrams clean and simple - tufte - maximize information to ink ratio
Not be scared of alternatives

Popsicle sticks
Dance your PhD

Timothy - ontologies - understanding is needed. How to create them.

Explainer - crafty youtube video explaining SSI using popsicle sticks, foam figures and cards
https://youtu.be/81GkdBRmsbE

"What are you" video from Kurzgesagt https://www.youtube.com/watch?v=JQVmkDUkZT4

https://en.wikipedia.org/wiki/Internet_governance#/media/File:Who-Runs-the-Internet-graphic.png

UX section BC - covid passport folks - fundamental questions - am I safe private - is government on my back.
Accompanying set of communication - values and what we stand for and appeal to what other people's values are.

Static QR Code.

Lawful Intercept - eSafety.

https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf

Need a bridge (for each audience) from their initial knowledge base
You learn a new thing (most easily) if it can be related to what you already know

As we are talking about KERI as an example (no more than that) of complexity that needs to be tailored to common people. https://github.com/henkvancann/keri/blob/master/docs/KERI-made-easy.md

An approach - explaining SSI in current real-world pre-tech terms - perhaps in human interaction term - particularly how this works in today's online world (before) and after ssi (after)

I shared the article about me in WIRED UK: https://www.wired.co.uk/article/kaliya-young

Ultimately we need to explain SSI to policy makers, who are non-technical.

I'm seeing papers from the Canadian Governments who clearly don't understand the current internet problems or what SSI solves and what role "jurisdictions" like themselves have to provide (e.g. governance and enforcement)

I completely agree. Try explaining the value prop of SSI to volunteer lay people running neighborhood caucus elections of between 20 and 200 people.

Any significant complexity and the people run the opposite direction!
This _must_ be simple to be adopted.

Yes to a "how to get up to speed" reading list - including "principles of identity"

https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

Yes to a "how to get up to speed" reading list - including "principles of identity"

https://ssimeetup.org/how-avoid-another-identity-tragedy-with-ssi-christopher-allen-webinar-53/

https://medium.com/berkman-klein-center/big-brother-a-critique-of-the-4th-industrial-revolution-in-africa-fdcd1a5fdddd

https://docs.google.com/document/d/1K_LsCg2lba1nbjSMBQq69sCZ5PXZZAniUXJkfRJ8qQY/edit

Potential metaphor to explain crypto: “mixing paint colors” — where a private key is a set of paint colors, and the public key is the resulting color from mixing that set. If you can produce the mixed paint color, you’ve proven you are the person who knows the set of paint colors that mix to produce that one color
08:28:51 From Dima Postnikov to Everyone:
+1 there is a gap. And all sides including SSI folks seem to be blinded (“their way is the way”)
Two great points

"The lawyers will save us" - The most effective "convincer" of why corp and gov IT needs to care about privacy - GDPR compliance and legislation on privacy.

+ 1 to audience specific papers!

The Manning book about SSI was mentioned earlier, in the context of “what is missing about the WHY in that book’s explanation?” — but I think even if that book contained a perfect explanation of why SSI matters, it’s not enough… Someone who isn’t sold yet is not going to buy or even borrow a huge tech book to learn about why they should care about a thing they don’t care about.

I agree, that's why I believe we have to meet the market where they are at and improve processes they have current strong emotional connection to.
People who are buying the book are also already interested/invest/involved

This is why I'm targeting credentialing, meeting assembly, and voting processes for local county political parties.

It won't appeal to the generally curious

+1 - need to build knowledge bridges - from where people are to where they would like

I was also thinking that we need to make some short easy to understand communications. I want to know all these things, but don't have time to ready a bunch of long long papers. I'm sure others feel the same.
08:36:51 From ChrisKelly to Everyone:

Kurzgesagt is my favorite channel that makes videos about science
30 short communications win over 300 pages of deep technical text
+ anecdotes

What happens when you don't address privacy (example Canada/Quebec province ignoring GDPR)

Issues of speaking smae language

We also need (as we are all explainers or we would not be here) a set of "tools & methods" on how to explain - including by different audiences

A series of diagrams @ different levels of understanding and complexity

Sharing the first interactive infographic that ToIP has on our website: https://trustoverip.org/wp-content/toip-model/

https://www.lfph.io/wp-content/uploads/2021/04/Verifiable-Credentials-Flavors-Explained-Infographic.pdf

For different audiences - what are their motivators?
Craft udemy or other courses on Decentralized X?

here's some diagrams (in case their helpful); although not simply about DIDs / credentials - works have always involved them. https://medium.com/webcivics/inforgs-the-collective-info-sphere-67a660516cfd?source=friends_link&sk=29ba4752f9a2ef12b6d2895539b52725

INVITE MORE DESIGNERS TO YOUR SESSIONS WEEEE
We will illustrate things!

we have to have enough free content on YouTube and the like to get the ideas out. Advanced courses and deeply involved workflows are great for Udemy and other courseware.

I'm thinking we need curriculum. Organized and sequenced chunks of knowledge. Bodies of Knowledge try to define "what you need to know" without spelling everything out or getting into pedagogy.
https://bok.idpro.org/
Yes, absolutely. I agree. That's what I intend to create. This session is awesome for me.

If we're going to produce more diagrams (which I love) - then can we follow some simple rules (like those Edward Tufte proposes, maximise the information to ink ratio)
https://www.edwardtufte.com/bboard/q-and-a-fetch-msg?msg_id=0000yO

who wants to continue to engage with working on messaging - explainers. please put your e-mail in the doc (will take out before going in public notes).

ontology creation, production, what is an RDF ontology, whats the difference between RDBMS vs. Semantics (spraQl, etc.) https://www.youtube.com/playlist?list=PLCbmz0VSZ_vqZemkHpzb7-GWmzcUdGgfP
this might help too: https://www.youtube.com/c/KingsleyIdehen/search?query=virtuoso
yet generally, the problem is the materials to teach people about ontology related stuff, is too hard

Also, in case we run out of time... suggest we use story/narrative structures (since that's how we're wired to learn and remember stuff), and use alternative forms of explanation (like using popsicle sticks, foam figures and cards - I might have done that already...)

Andy - I was a film director for undergrad :D so if you need film students lmk too
Meaning, I did that as my major
Before my masters
Chris Kelly - I have a past as a video producer

Kamal Laungan - not sure if we covered this, but we likely have a dearth of learn2earn programs in the ssi space

"What are you" video from Kurzgesagt https://www.youtube.com/watch?v=JQVmkDUkZT4

re: governance of how the internet has traditionally worked, vs. the impacts of DIDs
https://en.wikipedia.org/wiki/Internet_governance
https://en.wikipedia.org/wiki/Internet_governance#/media/File:Who-Runs-the-Internet-graphic.png

ID Token as VP (OpenID Connect 4 Verifiable Presentations)

Thursday 21A
Convener: Kristina Yasuda, Torsten Lodderstedt
Notes-taker(s): David Waite

Tags for the session - technology discussed/ideas considered:

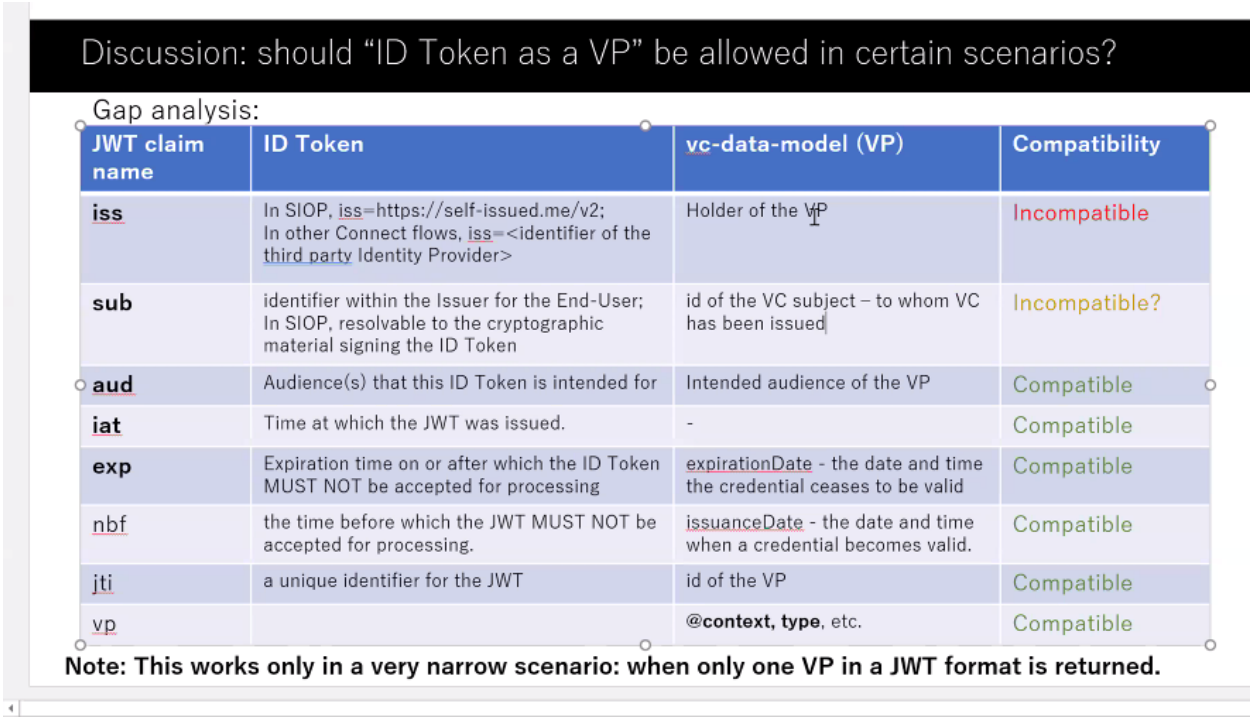
OpenID Connect, Verifiable Credentials, Verifiable Presentations

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

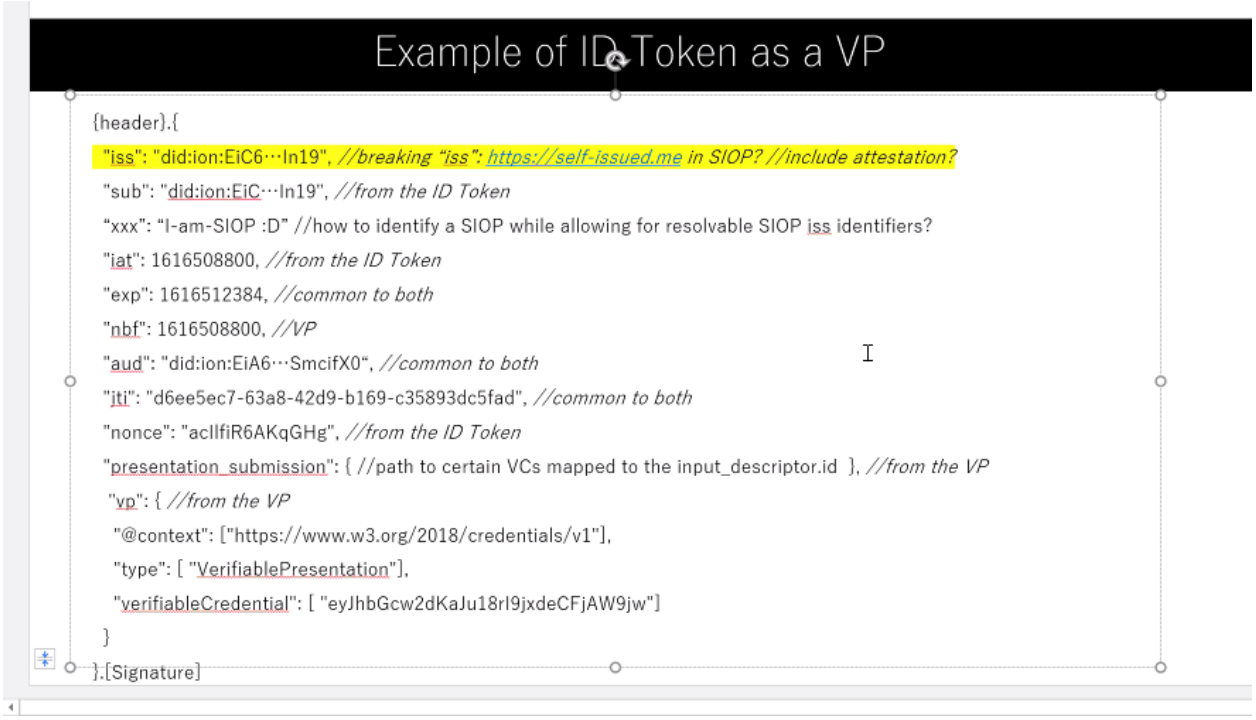
Today OIDC4VP allows presentations to be either conveyed inside an id_token or beside the id_token in a vp_token response parameter.

Question has come up whether the id_token can be a VP, e.g. contain credentials as long as they share a common proof.

Vittorio: If you conflate the id_token and presentation, you may create ramifications for existing infrastructure which expects an id_token as a trigger for authentication pieces, when you actually only want presentations and not sessions
Torsten: We will not have this as being the only option, you will still be able to have the id_token separate from the presentation



DW: Nonce and Audience is interesting because it isn't actually part of the VC data model, because these map to the protocol elements of presentation, and VC does not define protocols



DW: Changing the behavior of issuer has ramifications of how id_token validation fits into a traditional SIOP stack - a.k.a. a larger delta in policy changes between OP and SIOP communications

From SIOP call:

> Chadwick, not using id_token to identify the user directly, using the VC sub as identifier for user.
> Mike Jones, commented that this is not OpenID Connect behavior, (subject, issuer) pair is meant to be the identifier for the End-User for the relying party

DW: Issuer _could_ be the subject, idea of resolvable identifiers is that the OP is more of a statement of common metadata across multiple SIOP implementations/installs, but changing iss breaks the OIDC protocol

Vittorio: Changes implementations, would have millions of issuers

Torsten: how would you differentiate issuers if you do not use a hard coded value
DW: OP would not have a JWKS URI if the OP metadata represents a SIOP policy
Torsten: Is this a robust enough signal
DW: Likely should have additional metadata so a mere JWKS missing or not resolving
George: Prefer explicit signals since implicit signals can come back to bite you
DW: We can have it per OP or per id_token, id_token would increase the payload

Mike: SIOP in the general case don't have any way to host web infrastructure, not sure how to make the entity resolvable.

DW: Is it on the table to possibly new serialization other than VP-JWT that has our rules without changing claims?

Torsten: question is whether id_tokens can be consumed as presentations as-is

Impact on existing implementations pushes away from wanting to make changes to the issuer claim.

DW: One potential benefit is in having a VP that is part of a higher level abstract protocol across transports, but I don't believe this gets us all the way there even with issuer changes

DW: Should probably reach out to the VC WG with this possibility to get broader input, also see if a potential rechartering might change the equation of whether this can be supported.

The Seven Deadly Sins of Commercialised SSI

Thursday 21B
Convener: Ankur Banerjee, Alex Tweeddale
Notes-taker(s): Alex Tweeddale

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

Presentation link:
https://www.dropbox.com/s/y4a36uv9z3f1fx6/The%20Seven%20Deadly%20Sins%20of%20Commercialised%20SSI.pptx?dl=0

Session Summary:
Ankur used this presentation to deep dive into the most common red flags people raise on the question of commercialising SSI. He broke this down into '7 deadly sins', as follows:

1. The Price of ID checks is too high
2. Making it free as in beer, not as in speech
3. Payment correlation can cause privacy risks
4. Being fanatical about your ledger
5. Planet of the Apps
6. Utopian Vision clouding real Usability
7. On the internet, nobody knows your DID is a dog

Decentralized Reputation

Thursday 21D
Convener: Johannes Ernst
Notes-taker(s):

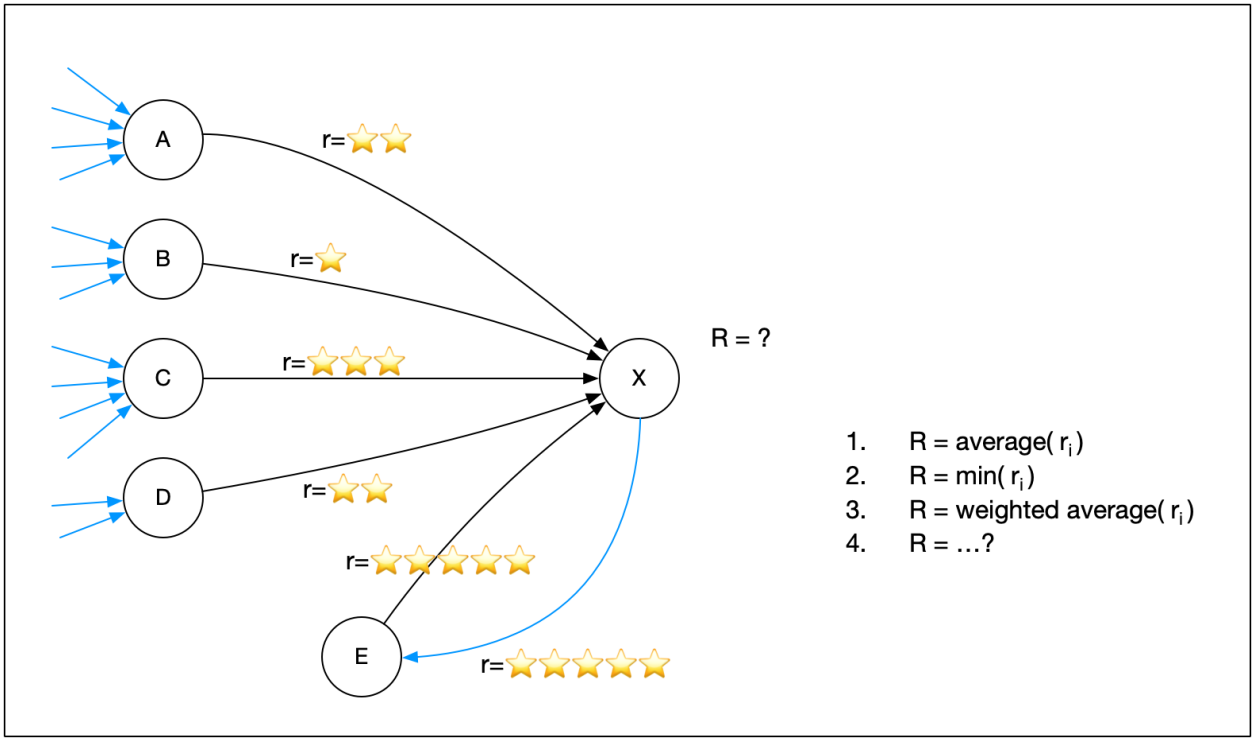
Tags for the session - technology discussed/ideas considered:

Reputation, authentic data, decentralization

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

Challenge: the motivated malicious user is willing to dedicate far more time and resources to manipulate the reputation systems then a normal user. This leads reputation systems to be dominated by those with the most extreme views.

In lieu of a whiteboard:

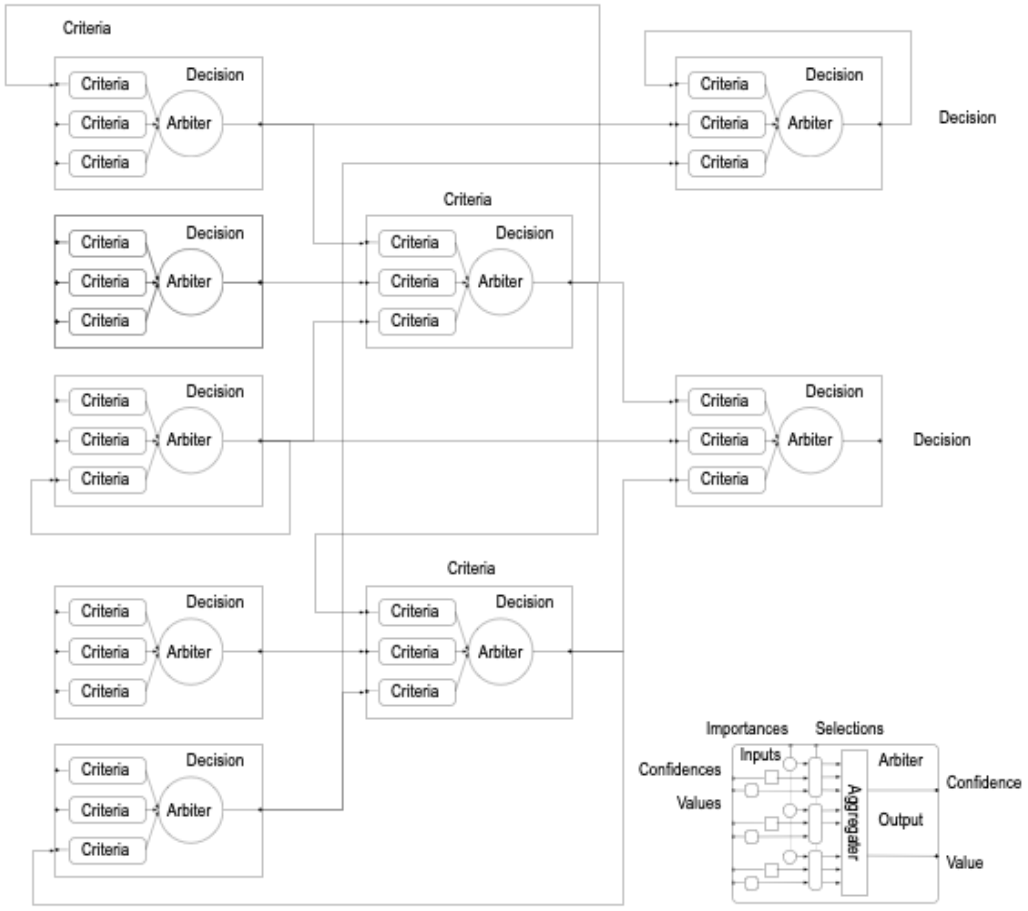


Links from the audience

- Sam Smith: presentation on a github pdf ; more papers on reputation are here
- Timothy Holborn: medium link
  - example about 'repetitional' related problems linked to 'identity' associated decision making (ie: associating DNA to birth certificates by default, rather than ancestry.com)
  - please decouple this comment from my identifier, for purposes of privacy / dignity protection
  - friend link
  - causality & social informatics implications. complex version

    - Notes about 'identity' (human agency / personhood, AI Ethics related considerations) - also this and this
- Juan Caballero: github pdf

- Not only algorithm, but the people who pick the algorithm
- Lots of money often equals high reputation because it can be paid for
- Open Federated Learning
- As soon as you allow non-transparency, people are tempted to introduce bias and cannot learn from others



Rouven Heck1 to Everyone (10:04)
recording?
Nader Helmy to Everyone (10:04)
This is one of the oldest problems in identity ☺ there's a lot of prior art
To put it lightly
Johannes Ernst (Indie Computing) to Everyone (10:05)
https://docs.google.com/document/d/1rDMMm2AB75nH4YhMDOpbLXUgRkgLIh1VWwhJJNzF71M/edit

Me to Everyone (10:05)
Nader Helmy to Everyone (10:07)
The reputation of “x” for what purpose? It’s not a universal score, there is presumably a specific context to which that claim is being made
Andy Morales to Everyone (10:07)
RottenTomatoes review bombing is a great example too
Steve to Everyone (10:08)
Can we record the meeting?
Juan from Spruce to Everyone (10:08)
are there slides?
TelegramSam to Everyone (10:08)
diagram in notes.
Andy Morales to Everyone (10:08)
We are in the notes, Johannes is diagramming there
Nader Helmy to Everyone (10:08)
No slides but here are Johannes’ notes:
https://docs.google.com/document/d/1rDMMm2AB75nH4YhMDOpbLXUgRkgLIh1VWwhJJNzF71M/edit
Juan from Spruce to Everyone (10:09)
nice thanks, qiqo bombed and was showing me a "request access" page somehow! 🤦
Timothy Holborn to Everyone (10:09)
question reference: https://miro.medium.com/max/3122/1*OD62QRiDXQd5mBdR_MiFpQ.png
Juan from Spruce to Everyone (10:10)
do people want to record?
John Phillips - Sezoo to Everyone (10:11)
my preference is yes (if only because I'm running on very little sleep so my ability to absorb new content is limited! ☺)
Juan from Spruce to Everyone (10:11)
^ +1
Michel Plante to Everyone (10:11)
recording preferred
Timothy Holborn to Everyone (10:12)
“the distinction between reality and our knowledge of reality, between reality and information, cannot be made” Anton Zeilinger
Juan from Spruce to Everyone (10:12)
can someone get the host-code and hit "record to cloud"?
hostcode = 232323
google founders :(
Andy Morales to Everyone (10:14)
But will the data EVER be securely attributed on the internet?
I just…don’t ever see that happening?
John Phillips - Sezoo to Everyone (10:14)
Do we really want this? Just because we can, does that mean we should? What problem are we solving for here? If we have concerns that "identity" is too often the table stakes for interactions, surely we should be more concerned if reputation becomes the table stake?
Juan from Spruce to Everyone (10:14)
huge +1 -- sam's papers on this are great reading, highly recommend on this.

@Andy, we're all dealing in probabilities between 0 and 100 that one or the other decentralized technology will get us close enough to that goal :D

Juan from Spruce to Everyone (10:15)
@John Philips, Dave Huseby has a session on that very question happening now in another room :D
Andy Morales to Everyone (10:15)
Love that, but there's a high high chance that actors that do NOT want to be recognized will do everything in their power to at least obfuscate the systems no?
Juan from Spruce to Everyone (10:15)
(I agree the social dangers are huge!)
Eric Weber to Everyone (10:16)
Don't you have to ask A,B,C,D for rating
Andy Morales to Everyone (10:20)
But this is a different situation because landlord has to abide by clear laws ruled by public organizations, person submitting a review anonymously on the internet does not have any potential compliance issues
John Phillips - Sezoo to Everyone (10:21)
Answering my own question further up in the chat (just because we can, doesn't mean we should)... if we assume that our reputation is being rated by others, whether we like that or not (think Equifax etc.), then having an understanding of how our reputation is measured, and having some control over how we present it, *could* be good. However there are way too many dystopian possibilities here. We could create a "rod for our own back".
- thanks @Juan, I'll try and clone myself!
Trev Harmon to Everyone (10:21)
@Andy, we'd like to believe that's the case, but it isn't everywhere. This renter example creates a very concerning extension of the power differential between tenant and landlord.
Dan Robertson (he/him) to Everyone (10:21)
But how do I know the landlord is not a synthetic entity, who has been made to appear reputable via a Sybil attack (i.e. many fake renters who have asserted they rented from the faux landlord)?
Andy Morales to Everyone (10:22)
@Trev fair.
But see, "they're a public legal entity"
This example depends on "public legal entity" as a core concept
Juan from Spruce to Everyone (10:23)
^^^^
Timothy Holborn to Everyone (10:23)
https://miro.medium.com/max/3122/1*OD62QRiDXQd5mBdR_MiFpQ.png
Brigitte Piniewski to Me (Direct Message) (10:24)
Do you have an example of when the system is in place, then people will work to give you better data?
Michel Plante to Everyone (10:25)
Landlord + tenant use case: https://domilabs.io/
Trev Harmon to Everyone (10:26)
I think that the landlord/renter example only really works with consistent regulation. However, this is just a hypothetical example.
Andy Morales to Everyone (10:26)
The problem with these things (decentralized reputation systems) is ALWAYS that we need a group of humans doing investigative work SOMEWHERE. Whether it is in a centralized public organization, or in a series of private organizations that build visualizations of the networks of reputation, or volunteers...
I'm more interested in how THAT labor will organize
Andy Morales to Everyone (10:27)
I think that's ultimately the most important thing
Juan from Spruce to Everyone (10:28)
there's a lot in glassdoor on SV employers

outside of california it's a graveyard
here in berlin it's almost worthless, <5 reviews for companies with >100 positions
Andy Morales to Everyone (10:28)
Blind is a better example imo
Because you need to have a company email to be able to submit a review
Andy Morales to Everyone (10:29)
But it anonymizes you
Rouven Heck1 to Everyone (10:29)
Before we have computation on top of encrypted data - can we really build privacy preserving reputation systems?
(decentralized)
Dan Robertson (he/him) to Everyone (10:29)
I think glassdoor is also better for larger companies than smaller. If you're at a three-person company, you probably don't feel safe to be honest in posting publicly about how you feel about your employer — since "…by a Product Manager at XYZ Co" may literally identify you uniquely.
👆Or Blind app, etc.
Timothy Holborn to Everyone (10:31)
causality & social informatics implications. complex version is https://medium.com/webcivics/theoretical-relationship-between-social-informatics-systems-and-quantum-physics-reality-check-6ce3781d1a29?source=friends_link&sk=f0d5323abc9355ad1edb7e15f1e60f41
Timothy Holborn to Everyone (10:31)
Notes about 'identity' (human agency / personhood, AI Ethics related considerations)
https://www.webizen.net.au/about/executive-summary/preserving-the-freedom-to-think/
https://www.webizen.net.au/about/references/social-informatics-design-concept-and-principles/
https://medium.com/webcivics/the-semantic-inforg-the-human-centric-web-reality-check-tech-50e2fa124ed4
mary104 to Everyone (10:31)
YES!!!
Trev Harmon to Everyone (10:32)
We also still have the issue with bias in AI.
Charles Lanahan to Everyone (10:32)
@Timothy I'm getting "oops that page can't be found"
Dan Robertson (he/him) to Everyone (10:32)
I say LET SAM DECIDE
Bart Suichies to Everyone (10:32)
What reputation are we talking about?
Mary to Everyone (10:33)
and who made the algorithms and what are their biases
Timothy Holborn to Everyone (10:33)
@charles - i've tried the links, perhaps someone else can confirm if there's a problem?
Charles Lanahan to Everyone (10:33)
oh wait, haha user error
Charles Lanahan to Everyone (10:33)
I copy/pasted both links as one link
Timothy Holborn to Everyone (10:33)
friend link to https://medium.com/webcivics/the-semantic-inforg-the-human-centric-web-reality-check-tech-50e2fa124ed4?source=friends_link&sk=27043bff446e23466b9bae786fa614e0
Trev Harmon to Everyone (10:33)
@Mary, exactly. We don't need AIs "inadvertently" disadvantaging certain groups because of those biases.

Mary to Everyone (10:34)
@Trev yes
TelegramSam to Everyone (10:37)
the discussion about the topic generally is excellent, but one point: we can make reputation 'portable' by issuing credentials. This is obviously limited, but also right in front of us.
we don't have to fully solve the issue to benefit from some 'portable' reputation usecases.
Juan from Spruce to Everyone (10:40)
^^^+1
Me to Everyone (10:40)
+1
Juan from Spruce to Everyone (10:40)
<3 non-rivalrous good
Timothy Holborn to Everyone (10:41)
example about 'repetitional' related problems linked to 'identity' associated decision making (ie: associating DNA to birth certificates by default, rather than ancestry.com)
https://www.dailymail.co.uk/news/article-9106197/Researchers-uncover-British-foreign-aid-workers-fathered-children-abroad.html
Timothy Holborn to Everyone (10:42)
please decouple this comment from my identifier, for purposes of privacy / dignity protection:
https://drive.google.com/file/d/1Vni97O6Pa1YETLE0S3NzV4CsWwDo5YLl/view?usp=sharing
(above it says repetition rather than reputation).
Andy Morales to Everyone (10:45)
Lol my computer shut down
Andy Morales to Everyone (10:45)
Didn't mean to mic drop and leave
Johannes Ernst (Indie Computing) to Everyone (10:46)
I wondered where you suddenly had gone!
Juan from Spruce to Everyone (10:47)
Plugging a colleague's session on this topic: 24I - Self-sovereign Applications on "Authorized P2P" Infrastructure: Kepler Design Progress Report (added after session generation this morning) - 1.45 PT/4.45 ET/Very late CET
Andy Morales to Everyone (10:47)
Someone catch me up! Did someone suplex my argument!?
Eric Weber to Everyone (10:49)
Is the objective reference the sum of a lot of subjective references?
Me to Everyone (10:50)
I call this "User Permissioned Trust"
Juan from Spruce to Everyone (10:54)
Do I have to plug my colleague's session again?
I think the ZCap/OCap people would say that granular and caveated delegation could get us most of the way, if not all the way, to those kinds of crawlers and discovery mechanisms and authorization languages...
Juan from Spruce to Everyone (10:55)
(I'm trying to bait Adrian to answer here ;D)
Zorigt Baz to Everyone (10:57)

Juan from Spruce to Everyone (10:57)
+1
Dan Robertson (he/him) to Everyone (10:58)
I think we have until 15 past the hour, no?

John Court to Everyone (10:59)
I am not convinced from any of this that reputation will become decentralized through current SSI technology. The centralised ecosystem can switch to issuing VCs and maintain their audience because word of mouth from individuals no matter what form is inherently untrusted when monetary lose could be involved. What seems to be needed is an ecosystem to build trust in individuals somehow.
Andy Morales to Everyone (11:00)
+1 to the above
I also want to mention “decentralized trust systems” have been built by women for YEARS. They were called “gossiping” and was never paid precisely because it was not backed by money or powerful institutions
Me to Everyone (11:01)
cryptographically authenticated but fully pseudonymous trust and be built over merely from behavior. This is the type of reputation that allows trust in the history of behavior. Similarly it allows rapid loss of trust given any variation in behavior. Think Victorian ear female authors with male pseudonyms
Andy Morales to Everyone (11:01)
You wanna design a dececnralized trust system? Just go to a hair salon.
Juan from Spruce to Everyone (11:01)
^^^
Aaron Goldman to Everyone (11:02) Gossip is a valuable protocol
Charles Lanahan to Everyone (11:02) haha
Zorigt Baz to Everyone (11:02) That’s social media
Juan from Spruce to Everyone (11:02)
I have a non-IIW meeting I have to run to. thanks all!
Andy Morales to Everyone (11:02)
No, social media has other weird incentives, like faking that your life is better than it is.
Trev Harmon to Everyone (11:02)
Thanks for the discussion everyone. Have another meeting to run to.
TelegramSam to Everyone (11:02) There is only IIW.
Andy Morales to Everyone (11:02) At the hair salon you are looking at your worst lol
Andy Morales to Everyone (11:03) Have to go :(bye everyone!
Eric Weber to Everyone (11:04)
There is certain chance that your reputation will de-anonymize your pseudonym
John Court to Everyone (11:05)
So a non-authenticated form of individual trust could be seen to be the current fad of `social media influencers`. Can we somehow build on how that has somehow happened ?
Dan Robertson (he/him) to Everyone (11:05)
Great point, Sam, re: not needing to be associated with a natural human individual
Timothy Holborn to Everyone (11:06)
https://medium.com/webcivics/comms-security-privacy-vs-dignity-8fe67c1669c0?source=friends_link&sk=c694d9ed735b167dcabb36720042c00e
Mary to Everyone (11:06)
same with scammers who steal financial payment artifacts like atm cards, etc
Me to Everyone (11:07) If you pseudonym is a cryptographic random string of sufficient entropy then there is no correlation to the string only from the body of work itself.
evanwolf to Everyone (11:08) IS THE CHAT WINDING UP IN THE SESSION NOTES?
Timothy Holborn to Everyone (11:08) probably important note: (noting therein also, wikidata)
https://youtu.be/l0P4Cf0UCwU

Mapping Verifiable Credentials to Hierarchical Identification and Declaration

Thursday 21G
Convener: Kevin Dean, GS1
Notes-taker(s):

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

Kevin Dean Summary from Opening Circle:
This session presents on mapping Verifiable Credentials to hierarchical identification and declaration. This session is less of a nuts and bolts discussion and more about the challenges of taking the Verifiable Credentials framework and applying it to an existing identification system and the data associated with those identifiers.

Presentation here: https://gs1go365-my.sharepoint.com/:b:/g/personal/kevin_dean_gs1_org/EbJGrFAo6DpNgBCXnheyZCoBpCMY7sAEK-UQQVdYiyo2zA?e=qYIWl3

We're Building Digital Gates to Keep People Out. Why Identity Cannot Be An Input To Verification

Thursday 21I
Convener: Dave Huseby
Notes-taker(s): N/A

Tags for the session - technology discussed/ideas considered:

#ssi #covidcredentials #freedom #liberty #cryptography

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

We are Building Digital Gates to Keep People Out

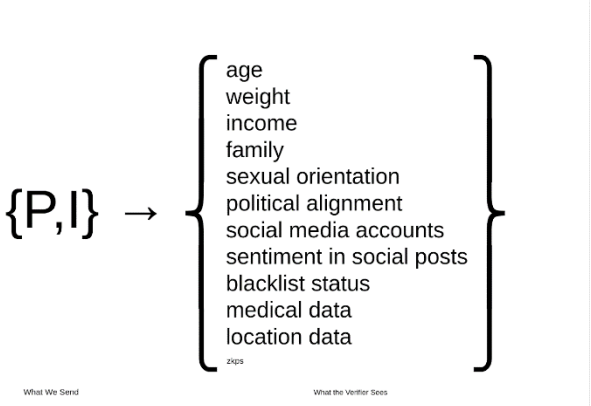


Figure 1 - Holders present zero-knowledge proofs (P) and leak identifying information (I). The verifier uses the identifying information to de-anonymize the holder and then applies policies based on the identity information instead of the provided proofs. The only way to prevent this is to entirely eliminate the identifying information (I) from the presentation.

- SSI originally promised user sovereignty and privacy and decentralization.
- The manifestation of that has materialized into digital gates designed to keep people out of everything.
- Up until very recently, access to resources (e.g. food, water, shelter) has been a concern of humans everywhere.
    - Large amounts of money and effort has been expended in the past to increase access and increase the stability of access to these resources.
    - Access to these resources has generally been considered a human right.
- Now that we have digital <whatever> passports, the idea is that we will have physical/digital gates that will block some people from accessing these resources.
    - This is a fundamental sea change in the "human community standards"
- WE are responsible for this. SSI is the way the passports and gates are being constructed.
- Right now, despite our best efforts, the implementation using the W3C standards does very little to protect privacy and what it does do, doesn't really preserve privacy.
- Theory: as long as the identity of the holder/presenter can be ascertained by the verifier—by any possible means—then the gating/verification function can, and probably will, expand it into all of the associated personal data available in online databases. This means that digital credential checks can, and will, operate on our identity despite all of the privacy preservation we employ.
- It is ***critical*** that it is impossible for the verifier to correlate and identify the presenter in all credential checks.
- What we have built is a tool that can be used to create real-world consequences—even violate our human rights by blocking access to basic needs—for having "incorrect" personal attributes (e.g. the wrong politics, the wrong skin color, the wrong social class, etc).
    - This is how political dissent will be punished.
    - This will eliminate all peaceful approaches to resolving our political differences.
    - History teaches us that individualized control and lack of peaceful political resolution always leads to violence.
- The information theory model for online de-anonymization is based on gathering enough observable traits during online interactions to uniquely identify the participants.
- Social media/Tech companies have been doing this for more than a decade and have used the observations to create empirical models that make de-anonymizing us extremely easy and are so accurate it is scary.
- "Perfect privacy" is when interaction happens but the identifiable information exchanged is absent or so little that de-anonymization is impossible.
- To achieve perfect privacy we need a system that allows for business logic to operate upon our private data but the data sent is so little that de-anonymization is impossible.
- One model for doing this is to combine authentic private data with a verifiable computation run by the holder of the authentic private data and combined into a 1-bit answer (e.g. yes or no) with proofs of authenticity of the inputs and the correctness of the computation. The combined result with proofs is called a Qualification (e.g. I am qualified to enter this grocery store).
- Conclusion: If the good health pass or other similar digital credential systems gate access to food/shelter/work/travel and are able to operate on our identities/biometrics then it will

immediately become a social credit system and we will descend into a collectivist dictatorship overnight, enforced by the digital gates we have built to keep people out.
- If we don't build for perfect privacy, posterity will blame us.
- The DIF Applied Crypto working group is the place to hang out if you want to talk about and/or work on this.

References / Reading
- Zero Architecture is the Way Forward
- DIDs are Dead
- Achieving Absolute Privacy
- Don't Use DIDs
- The Authentic Data Economy
- The Web was Never Decentralized
- A Unified Theory of Decentralization
- The Principles of User Sovereignty

Zoom Chat
10:03:37 From Alan Karp to Everyone: https://youtu.be/t-OKL7cKarA
10:10:17 From Vic Cooper to Everyone: Anyone have links to those articles?
10:12:20 From Mark Scott to Everyone: https://dwhuseby.medium.com/
10:13:09 From Mark Scott to Everyone: Nine articles going back to July, 2020.
10:13:10 From Vic Cooper to Everyone: thanks
10:22:11 From Shannon Wells to Everyone: fact
10:22:27 From Marc Davis to Everyone: +1 Shannon
10:23:39 From Alan Karp to Everyone: There's a Chrome extension that changes your browser fingerprint for each site. Someone showed that you cans till be identified with high probability.
10:24:07 From Marc Davis to Everyone: Home Zipcodes are used to predict a huge number of data points about the individuals that live in them
10:24:47 From Jeff O to Everyone: Indeed Marc!
10:26:32 From Zorigt Baz to Everyone: But you're right
10:26:33 From Jeff O to Everyone: Great optics David. Absolutely formative truths of the matter.
10:26:50 From Henk van Cann1 to Everyone: +1 Zorigt
10:27:28 From Shannon Wells to Everyone: But you also have to consider —all— the implications and there needs to be a recourse, no matter what you build
10:27:48 From Alan Karp to Everyone: Unintended consequences
10:28:14 From Shannon Wells to Everyone: ^^ there will always be these, you can't predict what they are, which is why there must be recourse for everything
10:28:57 From Vic Cooper to Everyone: I'm not sure the problem is access. The end result of surveillance capitalism is manipulation/behaviour modification based on how much more the algorithms knows about us compare to what we know
10:29:29 From Marc Davis to Everyone: +1 Vic
10:30:26 From Vic Cooper to Everyone: And if the algorithm knows what we are afraid of then it knows how to manipulate us
10:30:32 From Jeff O to Everyone: Social Scoring
10:31:27 From Jeff O to Everyone: Boundless level of metrics with boundless implications.
10:31:50 From Zorigt Baz to Everyone: So 1984 scenario is very real
10:31:53 From Marc Davis to Everyone:
Jeff Orgel:10:32:10 From Shannon Wells to Everyone: it's here already
10:32:14 From Marc Davis to Everyone: Sorry Jeff! Mistyped.

10:33:40 From Henk van Cann1 to Everyone:
@Zorigt What we already have today, was Orwell's worst nightmare?
10:34:19 From Trent Larson to Everyone:
Is there any controversy in his statements? FYI: I believe he's spot on, and it's driven by the simplistic desire to have "teeth" to chase down bad players for any governance problem proactively, as opposed to allowing nuance and even potential low-level threats to happen… all because of the false lure of enforceability.
10:35:48 From Brian Richter to Everyone: If we succeed in only sending 1 bit its almost impossible to create multi user interactive applications is it not?
10:36:12 From Jeff O to Everyone:Teeth well sunk into the "fabric" David. I'vve been watching & feeling "IT" for well over a decade.
10:36:37 From Shannon Wells to Everyone: it's not possible to be apolitical
10:36:38 From Steve McCown to Everyone: So we send the required 1-bit … and then sign it with a public DID (or key)?
10:36:51 From Shannon Wells to Everyone: you can just opt out of making a specific political statemnt
10:39:13 From NickyHickman to Everyone: context= moment
10:39:17 From Alan Karp to Everyone: How do I get personalization?
10:39:18 From Marc Davis to Everyone: +1 Shannon
10:39:20 From NickyHickman to Everyone: identity is a function of that context
10:39:38 From Vic Cooper to Everyone:
It's not 1984 it's Brave New World. Orwell vs Hexly. Big Brother vs Big Other
10:39:39 From Marc Davis to Everyone: @Shannon Architecture is politics.
10:39:41 From Kent Bull to Everyone: Jumping in a little late. What are the cryptographic primitives that support such privacy? I want to use them in my app.
10:40:26 From Shannon Wells to Everyone: human rights is political… but anyway, I don't see anything controversial just points I hadn't considered, but I"m not sure about a "simplistic" need for teeth to chase down bad players so much as a way to opt out of it and to establish technical protections
10:40:27 From Kent Bull to Everyone:
@Marc totally. This is because governments have defined themselves in a way that violates proper civilized boundaries. It's time to architect things in a way that rebalances power one internet packet at a time.
10:40:33 From Zorigt Baz to Everyone:
there are uses cases for personal verification and authorization. How do we do those with single use key?
10:43:06 From Steve McCown to Everyone:
This makes me think of "Strong Anonymity". (https://venturebeat.com/2016/10/08/how-strong-anonymity-will-finally-fix-the-privacy-problem/)
10:43:25 From Marc Davis to Everyone:
@KentBull Totally agree and I love your phrasing: "It's time to architect things in a way that rebalances power one internet packet at a time."
10:44:08 From Henk van Cann1 to Everyone:
@Vic: Huxley nails our present-day society on the head https://youtu.be/alasBxZsb40, he did this more than 60 yrs ago.
10:44:31 From NickyHickman to Everyone:
Your point about web vs internet is very important. We call it web 3.0 and that's a problem, because as you say it's not about the web it's about the sub-structure of the Internet. I think that Doc and Customer Commons Intentron plays directly to this
10:44:55 From Joyce Searls to Everyone: +1 Nicky
10:45:33 From Shannon Wells to Everyone:
Not everyone can "start a company" to solve their problems, that's not a good answer

10:46:11 From Alan Karp to Everyone:
Get a loan from your parents to start a business. — Mitt Romney
10:46:26 From Shannon Wells to Everyone: I mean I realize David was being a bit flippant
10:46:30 From Joyce Searls to Everyone: YES. Beyond the Web
10:47:31 From Alan Karp to Everyone: The authorization token system we built used a different key pair for each certificate.
10:47:32 From NickyHickman to Everyone: 🤼 for joyce
10:47:52 From David Huseby1 to Everyone: Ohhhh!
10:48:04 From David Huseby1 to Everyone: I always thought “buy” + “my way”
10:48:26 From Shannon Wells to Everyone: for people who don’t know though, “apps” often just are using a browser under the hood, aka “web view”
10:48:36 From David Huseby1 to Everyone: I was being flippant about “build it yourself”
10:49:04 From Alan Karp to Everyone: I know. Just poking you.
10:49:13 From Shannon Wells to Everyone: I suspected you weren’t serious, it’s just a common response
10:49:39 From Vic Cooper to Everyone: Isn’t a lot of this about moving the software we use over to our side of the fence?
10:49:41 From Jeff O to Everyone: @Alan - to your point of being able to do what you want to do, you likely may find that you simply have to things differently. Security is nice when it can be made convenient, yet look at how firemen, doctors, military, police, etc. wear to work. They probably would like to successfully do their thing less effortfully.
10:49:45 From Brent Zundel to Everyone: I love "intentron" but feel like it is demanding an additional number, a'la "Intentron 9000"
10:49:52 From NickyHickman to Everyone:
Even Tim BL says "“We demonstrated that the Web had failed instead of served humanity, as it was supposed to have done, and failed in many places,” he told me. The increasing centralization of the Web, he says, has “ended up producing—with no deliberate action of the people who designed the platform—a large-scale emergent phenomenon which is anti-human.” https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets
10:50:36 From Joyce Searls to Everyone: interesting, Nicky. Thanks for that quote.
10:52:00 From NickyHickman to Everyone: @Dave - can you speak to the idea of no individual identity, only 'dividual' identity - we are a number in a group.
10:52:24 From Trent Larson to Everyone:
I want to give a small ray of hope despite today’s toxic and totalitarian atmosphere: the web has connected people directly, to each other as well as to the real sources of information. It’s a stepping stone, and people are realizing their individual power & discerning abilities, and we’re having the right discussions for next steps. 👏
10:52:26 From Alan Karp to Everyone:
@JeffO: People will always choose the easy way. The trick is to make that the secure, privacy preserving way. Unfortunately, there’s no incentive for companies to make that so.
10:52:38 From Joyce Searls to Everyone: RIGHT Dave!
10:53:15 From Jeff O to Everyone:
People's past (yearbook pictures) are showing up from 40-50+ years ago from analog real world. The data scape of mining is leaking into digital implication - reputationally.
10:53:20 From Joyce Searls to Everyone: Human memory is designed to degrade. “Time heals all wounds”
10:53:39 From Jeff O to Everyone: That's the song...
10:53:50 From Joyce Searls to Everyone: But, digitally memory lives forever.
10:53:50 From NickyHickman to Everyone:
encoded often in models that predict a homogenous kind of behaviour framed w/ western and white models of expected behaviour and incentives … it's deeply wrong but not too late to pull back

10:56:58 From Jeff O to Everyone:
Tech centric cultural/governmental control are turning their societies into ants and bees. That is where this stuff works in nature - but not so common in human nature.
10:59:26 From Marc Davis to Everyone:
@Dave The very nature of the Sovereign is hat it has the power of permissible and necessary violence against its subjects. That is true in the US as well.
10:59:59 From NickyHickman to Everyone:
Yes @Jeff - it's always about power and politics, but understanding as a socio-technical system requiring a socio-technical solution - no tech is the full solution no matter how brilliant... create space play GO not chess
11:00:51 From Brent Zundel to Everyone: I've heard there's a CBDC effort that will be happening at the LF
11:01:39 From Kent Bull to Everyone:
@Brent That's awesome. I'd love to learn more about that.
11:01:58 From Marc Davis to Everyone: +1 @Nicky
11:02:25 From Jeff O to Everyone:
@Nicky: Yes. Giving breathing room for the HumanOS (human nature) to be in the sorts of real world communal space with near others is often bypassed. Tech is an important (more or less per person) side channel of hopefully respectful function.
11:03:10 From Marc Davis to Everyone: +1 @Vic
11:03:21 From NickyHickman to Everyone:
Read this to understand distorted realities https://en.wikipedia.org/wiki/The_Magus_(novel) +1 Vic
11:03:31 From Jeff O to Everyone: ya
11:03:33 From NickyHickman to Everyone: Completely agree
11:04:42 From Jeff O to Everyone:
We are well served to learn to stand, or move away from, this fire without burning away.
11:05:15 From Marc Davis to Everyone:
@Vic: "The best possible prediction is the ability to manipulate someone's behavior." Brilliant!
11:05:28 From David Huseby1 to Everyone: +1
11:07:22 From Kent Bull to Everyone: What is the expiration date of a part of a reputation?
11:07:35 From NickyHickman to Everyone:
You call for policy but that is governance - what does self-sovereign governance look like - self asserted terms and policies - community based - bottom up policies
11:07:36 From Kent Bull to Everyone:
In the words of Steve Jobs: "Death is the single best invention of life."
11:07:39 From Neil Thomson to Everyone: aka Twitter is trial and conviction by social media
11:07:51 From Joyce Searls to Everyone:
These are not technical problems, they are spiritual ones.
11:08:15 From Zorigt Baz to Everyone:
Policies on federal level is very bad, it's mostly dependent on who gets contract on policy enforcement like private prisons.
11:08:56 From Neil Thomson to Everyone:
Influence on behavior is directly related to the closeness of personal relationships.
11:09:27 From Neil Thomson to Everyone:
We - the usual suspects
11:09:59 From Henk van Cann1 to Everyone: +1 David
11:10:05 From Zorigt Baz to Everyone: My tv is 29 inches, I only use it for DVDs that I borrow from the library.
11:10:07 From NickyHickman to Everyone: +1 dave - group hug🤗
11:10:14 From Vic Cooper to Everyone: Hard to imagine Dave being boring at a party

11:10:33 From NickyHickman to Everyone: that's because we like the same kind of parties @ Vic
11:10:43 From Steve McCown to Everyone: Dang it, I just bought a TV…. ;-)
11:10:50 From Shannon Wells to Everyone: fwiw I don't use social media either
11:10:51 From Jeff O to Everyone: lol
11:10:59 From Zorigt Baz to Everyone: Steve, I hope you at least bought OLED
11:11:12 From Alan Karp to Everyone: I'm a twit who doesn't tweet.
11:11:14 From NickyHickman to Everyone: LOL Steve
11:11:56 From Jeff O to Everyone: Broomsticks
11:12:02 From Shannon Wells to Everyone: bananas!
11:15:58 From Alan Karp to Everyone:
Croquet decided to use capabilities to manage permissions.
11:16:04 From Henk van Cann1 to Everyone:
@shannon maybe we should not underestimate the effect of tv, radio and other #MSM and lastly the web on our behaviour. "They" are manipulation our subconscious, especially when it's done in a multichannel way?
11:16:30 From Shannon Wells to Everyone:
I think we should ensure that we accurately measure it, not estimate it.
11:16:32 From Zorigt Baz to Everyone:
Social media made "cancel" culture possible.
11:17:00 From NickyHickman to Everyone:
Interestingly in the history of the interplay between politics and religion, everything has always been about social control and organisation think about Calvin and the duty to resist, think about the adoption of Christianity by the Roman empire, think about the catholic city states in France post the angovian empire
11:17:33 From Alan Karp to Everyone:
There was panic a number of years ago about subliminal images influencing our behavior. It never came to pass. (I don't think, but how would I know?)
11:17:39 From Henk van Cann1 to Everyone: + 1 Dave
11:17:47 From Jeff O to Everyone: quiet nod
11:17:51 From Zorigt Baz to Everyone: Collective dictatorship
11:17:56 From Shannon Wells to Everyone:
I think it's an oversimplification to suggest that people can be controlled by "the media" in whatever instantiation you think that is. People's behavior is determined by a complex network of factors
11:17:58 From Trent Larson to Everyone:
Collectivism is OK. Totalitarian Collectivism is scary.
11:18:28 From NickyHickman to Everyone:
the bald tradeoff of freedoms for information
11:18:39 From Shannon Wells to Everyone:
Subliminal messaging's power to influence was way overstated but people can be primed to make subtle associations, and that's used experimentally all the time.
11:19:19 From NickyHickman to Everyone:
"hearts & minds" - at home as abroad
11:20:22 From Zorigt Baz to Everyone:
As tax paying citizen
11:21:10 From Zorigt Baz to Everyone:
maybe we should get tax rebates if we're denied services
11:21:33 From Joyce Searls to Everyone:
gotta' run. Thanks, Dave.
11:21:39 From Henk van Cann1 to Everyone:

@shannon I beg to differ. What I've seen happening in Europe with Govs politically controlling the MSM and censoring critics…
11:22:40 From Shannon Wells to Everyone:
@Henk I suspect we may actually agree more than you realize. Too difficult to work out in a Zoom chat ☺
11:23:11 From Henk van Cann1 to Everyone:
@Shannon true :-D
11:23:49 From Zorigt Baz to Everyone:
DID is started with United States Department of Homeland Security's (US DHS)
11:24:09 From NickyHickman to Everyone:
have to jump, thanks Dave
11:28:10 From Vic Cooper to Everyone:
I'm curious how the model works with shared data? Data about us when we are apart of a group.
11:28:28 From Marc Davis to Everyone:
+1 Vic
11:29:19 From Shannon Wells to Everyone:
Wow
11:31:08 From Shannon Wells to Everyone:
How very enlightening and my heart goes out to you for what you've gone through dude.
11:31:20 From Trent Larson to Everyone:
It's crazy that we're allowing the NSA to gather and store all communications. It's crazy that US feds are currently discussing forcing all banks to send all transactions (> $600) directly to the IRS.
11:32:35 From Shannon Wells to Everyone:
yep
11:33:19 From Laura Jaurequi to Everyone:
Thank you!
11:33:21 From Jeff O to Everyone:
agree David. Better and better...
11:33:23 From Shannon Wells to Everyone:
Thank you Ken for sharing your important experience
11:33:28 From Brent Zundel to Everyone:
You too Dave
11:33:52 From Neil Thomson to Everyone:
Gotta drop - next time.....
11:33:59 From David Huseby1 to Everyone:
Thanks for coming Neil!
11:34:14 From Shannon Wells to Everyone: ^Kent
11:34:27 From David Huseby1 to Everyone: Thank you Kent for your story
11:34:49 From Jeff O to Everyone: Well put Vic.
11:34:52 From Kent Bull to Everyone: I'm glad to share it. Let it serve as a lesson on the consequences of getting SSI wrong.
11:35:01 From David Huseby1 to Everyone: +1
11:36:09 From evanwolf to Everyone: SSI vs. deep fakes
11:36:21 From Marc Davis to Everyone: +1 @EvanWolf
11:37:47 From Mark Lizar2 to Everyone: Providence at the outset is 100% the point - what we are calling consent by default
11:38:06 From Zorigt Baz to Everyone: SSI could be used for making government more transparent and accountable? Or, de-construct the notion of having representatives in congress to make it less corruptible.
11:38:32 From Brent Zundel to Everyone:

Reminds me of this: https://englishwotd.wordpress.com/2014/02/17/artificial-inanity-systems/
11:39:24 From Jeff O to Everyone: The velocity of socio-politics over digital can be tectonic. Can be Fast and far too.
11:39:38 From Mark Lizar2 to Everyone: LOL
11:39:40 From evanwolf to Everyone: In a world of pervasive computing, where our bodies, our persons, the spaces around us, and the metaverse are one thing, the ability to trust your senses is everything.
11:41:11 From evanwolf to Everyone:
Provenance from the sensor/hardware on up is part of this.
11:42:01 From Brian Richter to Everyone: @David is there a link to the latest provenance log spec or somewhere to read more?
11:43:19 From Brent Zundel to Everyone: adding correlation is easy
11:44:27 From Jeff O to Everyone: A data version of "evergreen"?
11:44:43 From Vic Cooper to Everyone: Seems like this all points to a web of trust model but one that works
11:45:10 From Kent Bull to Everyone: Gotta make a call. Be back in a few
11:46:20 From Marc Davis to Everyone: @Brent cryptographically? Please elaborate…
11:47:09 From Brian Richter to Everyone:
Answering my own question it might be this PR? https://github.com/decentralized-identity/crypto-wg/pull/8/files
11:50:27 From Shannon Wells to Everyone: oh my god
11:51:35 From Marc Davis to Everyone: @MarkLizar, is it this:
https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx
11:52:29 From Shannon Wells to Everyone:
I wish we would eliminate all advertising in children's content entirely
11:55:04 From Jeff O to Everyone:Thx Dave!
11:56:35 From David Huseby1 to Everyone: You're welcome Jeff
11:56:41 From David Huseby1 to Everyone: I wan't to work with all of you BTW
11:56:55 From David Huseby1 to Everyone Dave@cryptid.tech
11:59:19 From Vic Cooper to Everyone: Thanks for the session Dave. Great work and discussion!
11:59:51 From David Huseby1 to Everyone: My pleasure. Thank you Vic for coming. I always love to hear your thoughts on things
12:06:05 From Kent Bull to Everyone:
Headed out to a meeting for a bit. I'll see you all in the other sessions. Really enjoyed the convo and thoughts here.
12:09:46 From Jeff O to Everyone: Yay for anti-fragile.
12:11:53 From Zorigt Baz to Everyone: Cartel = monopoly
12:11:54 From Marc Davis to Everyone: I have to head out, and thank you all so much for a fabulous, thought-provoking, and even hopeful session.
12:12:14 From Jeff O to Everyone: Throttling commodities - ugh...
12:14:03 From Jeff O to Everyone: Amazon is getting pretty stripped too...
12:14:13 From Vic Cooper to Everyone:
A fascinating book on economics is actually a SciFi book, "The Ministry of the Future" Kim Stanley Robinson. The is a concept of a carbon currency and a decentralized social network called U-lock. They finally come to fruition when the other systems fall apart. The revolution happens because these ideas were ready as a plan B when the shit hits the fan
12:14:42 From David Huseby1 to Everyone: The mars series from KSR is awesome too
12:14:43 From Jeff O to Everyone: Thx All!

Power, Politics, Hamlet & Harms

Thursday 22A
Convener: Nicky Hickman, Darrell O'Donnell (Sovrin 14A Council)
Notes-taker(s): Nicky Hickman

Tags for the session - technology discussed/ideas considered:

#inclusion #harms #identityforall #UNSDGs #datification

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

The session was a discussion on addressing challenges to digital identity with a particular focus on underserved, marginalized communities.

We took each slide as a discussion topic, I4A Council is also bringing together a discussion paper and this feedback is important for inclusion in the whole. All are invited to contribute.

Here is the link to the presentation.

https://docs.google.com/presentation/d/1oMBSx1B27aU7U1ecN_H3SgNE1sd_zl233oNkMGDVr1A/edit?usp=sharing

Here is a link to the discussion document:
https://docs.google.com/document/d/1rvj3PVRvKs8wnBAJfzu6OTWzc8g6djWYYXQsMYas_5k/edit

Key points that were made in the discussion:

- There is a genuine issue about misuse of the SSI term, of misunderstandings about the differences between identification and identity and genuine challenges to SSI in particular.
- In terms of next actions, no conclusions were reached from the list of options on the last slide, however writing a white paper, collaborating across the community and the importance of the role of governance were all highlighted as most likely points to start in terms of basic myth-busting and getting the conversation on the table.

A Useful ZKP Revocation Scheme for BBS+ VC

Thursday 22B
Convener: Stephen Curran / Andrew Whitehead, Government of British Columbia
Notes-taker(s): Sebastian Schmittner, EECC

Tags for the session - technology discussed/ideas considered: Revocation, BBS+, zk-SAM,

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

Presentation by Stephen Curran : **>> Slides <<**

Non revocation token using zk-SAM

- zk-SAM = zero knowledge Signed Accumulator Members
- Diskussion on Registry file size. Obviously linear in # credentials.
- Indy (Sovrin): Writing Registry to ledger -> $$ -> Business Decision
- Links
    - Basic approach: https://hackmd.io/kj223D1ZQN29WiusmnPFMA
    - The math: https://hackmd.io/vTyqrJc9QoKgThqQpVtP3g
    - Starter repo: https://github.com/andrewwhitehead/bbs-accum

Andrew's Idea:
(better look at the presentation than at these few additional points ;))

- Akkumulator = Product of primes, one for each non-revoked VC
    - Check if accumulator is divisible by VC prime to check whether it has been revoked
    - Accumulator blocks -> smae primes in every blocks (corresponding to different VCs of course)
    - ZKP: Do not expose block / index while proving that a VC is not revoked
- Similar to Indy AnonCreds Revocation with Tails files
- VC -> Block + Member Index (prime number) in the registry
    - Opaque signed + shared
- Registry state: set of fully revoked (0), fully non revoked (product of all primes- all the same) and interesting: partially revoked blocks
- Timo Glastra:
    - This is a really understandable explanation of witnesses and accumulators: https://hyperledger-indy.readthedocs.io/projects/hipe/en/latest/text/0011-cred-revocation/README.html
- [Metrics -> see slides]
- There is a proof of concept implementation
- Why this method? Others considered?
- Christian Panquin:
  For background, here is a white paper about various revocation approaches we prototyped a while back with U-Prove, including an accumulator scheme close to this one.
  https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/Privacy20and20accountability20-20best20of20both20worlds.pdf
- Andreas Freitag: Balancing various target functions, in particular efficiency
    - Working Group in DIF evaluating the options
        - Crypto security

        - Privacy (non correlatability)
        - Performance KPIs (metrics)
    - Need objective (empirical) comparison
    - Interested Cryptographers and Developers: Please join the DIF WG!
- Rouven: Revocation as a service? Trust implications?
    - Stephen: Issuer needs to sign the revocation registry state! - no good as a service (other than CDN)
    - Rouven: Multi Key?
    - Stephen: msgs in VC must be signed with same key as the revocation registry
    - Andreas: Needs to be part of the Issuing Service!
- Andreas: Are you using revocation, Stephen?
    - Indy. -> Small Use Case
    - 12k Lawyers in BC
    - But almost every use case needs to have revocation -> non-avaiable revocation blocks use cases
- Andreas/Christian: "I am valid today credentials"
    - VC with expirey date just saying: that other credential is still valid
    - Keep re-issuing still valid credentials
    - A lot of load on the issuer for issuing lots of still valid credentials often
- Need Options for how to do revocation/non-revoked proofs to choose from

VC Issuance with OpenID Connect (using Credential Manifest?) Part 2

Thursday 22C
Convener: Torsten Lodderstedt, Kristina Yasuda
Notes-taker(s):

Tags for the session - technology discussed/ideas considered: SSI, OIDC, Issuance

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

We discussed this hackMD https://hackmd.io/0k1e45a9Ru-cizD7Gp86ig?view

Two problems:

- Binding of the assertions to the Client/End-user that requested it
    - → defining a new `proof` parameter that client can pass to the Token Endpoint or Credential Endpoint (newly defined endpoint) to request binding of the returned credential to a cryptographic material in the `proof`. To accommodate various kind of proofs.
- A mechanism to request certain types of credentials.
    - → Claims parameter with DIF Presentation Exchange

Design advice to design credential req-res first
Suggestion to use `response_type` - id_token

Decentralized Identity for Financial Inclusion: Field Notes from Kenya

Thursday 22E
Convener: Johannes Ebert
Notes-taker(s): Neil Thomson

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

standard SSI use cases not the same as financial inclusion

Logging provides data to show success of roll-outs to convince prospective clients

Banks (and other financial institutions) only see data they exchange - e.g. rent may not be considered in credit score as the banks don't interact with the rent cash flow (payer/payee). They do not currently use data except from other major providers (e.g. data brokers) for which many transactions are invisible.

Major goal for banks - risk reduction

In 3rd world - small stores have no visibility - bank used a video to assess a noodle store.

Kiva - looking @ supply chain (Margo Johnson)
supply chain lending

Types of reliable information for lending?
- this is expanding as an alternate (supply chain financing their customers (intermediaries in the supply chain))
- Using smart phones for data collection and transaction capture
- Incremental (integral) building of credit score
- Loans for service/product being immediately applied by the lender to the merchant vs going to the end-customer (who is the service/product recipient)
- Attractive to suppliers (joining existing platform and customer base)
- Attractive for intermediaries in supply chain, and banks and end customers for the same reason - lower cost of financial, increase of customer base and revenue, lowering of risk
- pre-this approach, changing lenders was costly, now it's simpler, faster and cheaper
- Integrated, small vendor friendly. Filling a vacuum that first world financial approach doesn't service

Feedback (from others) is in some african countries, the payment systems are too fragmented with too many different workflows. Chaotic.

Kenya was a unique opportunity as they had only a single payment system (ripe for expanding on that base)

Provider to provider transactions not well supported in multi-payment scenarios as they are all trying to dominate the market, not cooperate.

Some communities are all cash, with only temp storage (of cash) on debit cards.

In some cases fund transactions, including lending - much of the data discarded (or not managed) historically

Tech Stack for credentials?

- In many cases only basic phones or no phones
- Use a sponsor, agent, guardian (person with a smarter phone) to do the digital transactions
    - Can generate QRcodes for identification person w smartphone or other connected device for the sponsored person
- Lots of “friction” to digital for basic phones
- Very hard to build for older, not very good smartphones
- Many smartphone users do not know how to use anything but basic features

Many Dig Id projects underfunded, hard to get momentum - would be easier if more of the stacks were complete via open source and no/low cost for non-profit or early stage roll-out

Africa - support, services scattered, non-homogenous. Timing (when sufficient infrastructure and demand exist) is everything (not easy).

Does Login = Identity?

Thursday 22G
Convener: Doc Searls
Notes-taker(s): Nader Helmy

Tags for the session - technology discussed/ideas considered:

Identity, Login, Digital identifiers, Personal data

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

3 major themes/takeaways:

1. Physical embodiment is what allows us to achieve recognition in the real world. Similarly digital embodiment allows us to achieve recognition in digital contexts and online. Who are you in the digital world and how does that manifest? Agents and AI but also Web3, avatars, metaverse, NFTs

2. Login is about relationships, it should be 2-way but we model it 1-way. Cryptographic relationships are not always a great proxy for real world relationships.

3. Some scenarios/contexts require you to reveal information that identifies you personally but many don’t. You should be able to manage and use identities that don’t link back to you as a person. You’re this digital person that can project yourself into different scenarios and contexts, sometimes anonymously, sometimes pseudonymous, and rarely fully doxxed.

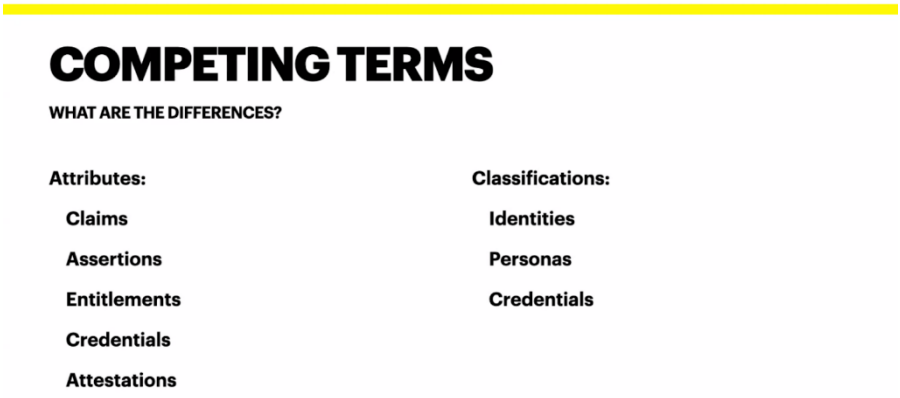
Person Schema Design - Doing it Wrong? @nytimes

Thursday 22I
Convener: David Wheeler
Notes-taker(s): Gaëlle Sharma

Tags for the session - technology discussed/ideas considered:

schema, schema design, person, user, credential, attribute, entitlement, claim, attestation, assertion, identity, persona

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



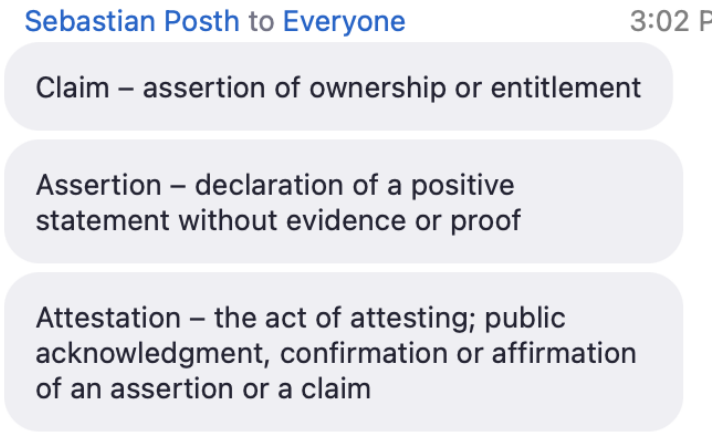
Johannes Ernst

- Do you have organizations?
- What is the target architecture?
    - Relational database?
    - DW: store JSON with a bunch of indexes / columns -- slightly fancy key value store
- Email addresses
    - How many authentication methods?
    - What is the user experience? Do users use multiple authentication methods?
- Github
    - Developers have two accounts -- one personal, and one corporate, to keep their two worlds separate
- Go and ask people about their schemas
    - Could be helpful. They may have some attributes you would never think of.
- I'm in California - CCPA
    - You may want to download the data
    - The better ones may show you structure
    - The higher profile of the company, the better they are organized
    - Might be useful to see how FB/Amazon represent marketing information
- Claim
    - As a programmer: claim is just a field
    - In an identity scenario: a claim is [something] stating that an entity has an attribute

        - A claim can be verifiable
        - Can verify who has made what claim
        - You can't verify that the claim is true, just verify who made the claim

Sebastian Posth

- Is there anything that relates a user to the content?
    - Claim that you own the right to that content
    - Attestation that you want to verify a claim
    - Attributing a piece of content to a rights holder
- A user with a specific credential, would have a credential to use a specific set of features
    - This is what I would associate with the relationship between the user and the content



OIDC specs

- Says that "names are specs" but I thought that was just an attribute of a person

Aaron Goldman

- OWASP - founded because people did use the same terminology
- Should have definitions for words

Safe Internet Use With KERI: Percolated Discovery OOBIS & Spanning Trust Layer

Thursday 22K
Convener: Sam Smith
Notes-taker(s): Henk van Cann

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

Session Presentation:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI_Percolation_OOBI.web.pdf

Notes are an addition to the slides in chronological order.

PERCOLATION
You don't need global lookup if you have invasion percolation.

Example: oil and water in a sponge, water will displace oil. We are talking about information flows. Metaphor: good information can drive out bad information. We are looking at authentic information. That's what we care about.

Not the veracity, that's a layer above KERI.

There are two controllers involved: the holder and the verifier. In KERI that means, controller of the key. Two moments in time: issuance and presentation.
The issuer is responsible for the registry. What could be problematic is that the state of the registry has changed between issuance and presentation. But it is still possible to get it. Percolation is multiple path. You can percolate information as well as the route; so the path doesn't matter.

We do not need a global registry with shared control.

Definition 'Information is…' in KERI :
Good => verifiable authentic attribution
Bad => not end-verifiable

In KERI 'Truth' is authenticity not veracity (veracity is more 'truthful, consistent')
'Spanning' means *available*

By having percolation and end-verifiability our problem is not **security** but just **availability**. Sam: "I'd rather have an availability problem than I have a security problem".
Security issue example: The most common attacks are (BGP) hijack attacks at certification authorities (middleman). They are complex and sophisticated nowadays.

Henk van Cann: KERI solves hijack attacks, because the binding between the controlling keypair (primary root-of-trust) and the identifier is strong, because it's cryptographically end-verifiable.

Participant: How about privacy with percolation?
Sam: very good question. It's being discussed in the PAC sessions (day 2 and day 3)

The discovery is not 'search', it's by already known connections, peerwise, on a *need-to-know* basis.
There is no global non permissioned search allowed in KERI.

Sidebar: In privacy, "Need to know" typically means that the entity wanting to know has a privacy - valid basis for wanting the information. As opposed to 'need to know' information about you for my business model.
In KERI *need-to-know* has a security base, pairwise.

KERI sits on top of the internet. Therefore our endpoints are URLs
All roles / all players in KERI have AIDs.

Sam's vision:
KERI needs to be **minimally sufficient** . Therefore it sometimes uses rather simple but reliable cryptography instead of the newest less tested stuff.
*Analogy Henk van Cann: You could use and build **spreadsheets** with the newest and most complex functions or solve the issue with just *,/,+ en -. The former might impose maintenance and backwards compatibility problems on us, the latter does the job too.*

Everything needs to be **end-verifiable** for trust, full stop. You can use it, but you can't trust it if it's not.

Pre-rotation and key management in KERI fixes a problem on the internet (verifiable attribution) that persists for 30 years.

From a security perspective Open ID connect (and OAuth and Fido2) are still subject to same attacks, it's harder, but still possible. Because it's not end-verifiable, conversely, KERI is.

KERI can't get rid of the attack vector *key management.* All the other security problems we've solved that's why we are trying to do key management as good as possible.

OOBI

Out of Band Introduction : https://hackmd.io/MxTAIBQTRkWU4-w140tNuA

A DHT is a welcome structure for availability in KERI, but it can't be a crucial part of the security mechanism.

KERI can't solve the problem of connecting a natural person to an identifier (primary root-of-trust). The good thing is: it only needs to be done once. After that everything is end-verifiable.

Passwordless Login: The Keys to Secure Logins

Thursday 23A
Convener: Mike Ebert, Sam Curren
Notes-taker(s): Mike Ebert

Tags for the session - technology discussed/ideas considered:

Passwordless login, authentication, authorization, DIDComm

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

Presentation slide deck:
https://hackmd.io/@TelegramSam/SJWpq3rSF#/

Login workflows:
Traditional account signup, VC presentation and link to account, VC presentation every login
Traditional account signup, VC presentation and link to account, use DID as authentication
Traditional account signup, link to DID, use DID as authentication

Connect with DID, VC presentation, create account linked to attributes of VC, VC presentation every login
Connect with DID, VC presentation, create account linked to attributes of VC, use DID as authentication
Connect with DID, create account linked to DID, use DID as authentication

Description of DID Login
Do we need to establish any new protocol for DID Logins?

Benefits of SSI-based passwordless login:

- So simple!
- More secure–avoid or eliminate password-based logins
- Avoids single point of failure
- Avoids phone home
- Avoids potential correlation
- Avoids provider lookup process

(Compare OIDC)

Recovery/Re-proving Ownership:
What is a good basis to re-prove account ownership if you don't have a traditional account setup?

Get a new matching VC (email, SMS, specialized). If the key attributes match, you're all set.
One-time passwords to unlock DID based accounts if the original agent/connection is lost

What Does Hybrid IIW Look Like?

Thursday 23C
Convener: Phil Windley
Notes-taker(s): Lisa R. Horwitch

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

Transcript from Discussion:

Phil: By way of introduction, we believe that by Spring we will be in a position where we can be face-to-face again. Over half of the participants in April were new to IIW. And we're faced with a large number who may not travel for an in person. For this IIW, we didn't know how the travel would be from last April to October. So uur thought and thinking was how to make hybrid work?

Phil: There are a few challenges we face with Hybrid:

1. WiFi in CHM is not great. They do have better WiFi, and are really proud of it, and charge a lot of money for it. If I remember right, they want something like $4-5,000 for the 3 day event (Heidi confirms - "at *least* that"). Which we just didn't have in the budget in terms of what it was going to do.

   (Heidi: And that "better WiFi" is with a company that CHM contracts out for it)

   Phil: so obviously if we're going to do Hybrid we probably need better WiFi, whether we have to pay for that or whether we can force CHM to do it because "it's a brave new world!"

2. The other challenge, of course, is that we need to have cameras in rooms, and probably not just people's laptop cameras.

   So Mike, I'm looking for something in between people just adhoc'ing it with their laptop cameras and something like what EIC had; and probably closer to people adhocing with their laptop cameras. But I'm thinking we could possibly buy some meeting owls or something like that and put in at least some of the rooms at CHM to make that happen.

Phil: So those are the kind of challenges from just a technical standpoint.

Phil: One thought we had after attending EIC, it helped a lot to have people in the room (moderators for every session); then as speakers changed there was someone to help manage the change over between the physical speakers and the virtual speakers. So Joyce was thinking we could have a requirement (sounds too stringent for IIW) or I'll say "strong request" - if you're going to have a virtual session we could have a "strong request" for the virtual session - where the presenter is virtual - that they also have a physical counterpart in the room who is "co-hosting" essentially with them. This person in the room can manage the session and logistics on site (e.g. virtual hand raising, etc).

Terry Hayes: At the very least, you probably need somebody that's managing the hand raising between the two environments.

Phil: Yeah, somebody has to moderate or facilitate that interaction. (Terry: Right)
Phil: Because one of my concerns has always been with hybrid is that the people who are remote/virtual are always like "second class citizens" and that's in some ways what Dick was saying about his experience speaking - it didn't feel like an "in room" experience at all.

Dick Hardt: What's the driver for it being hybrid? I think it makes things really complicated.

Phil: It does make things really complicated and my first position was - No, we won't go hybrid.
But unfortunately - well maybe fortunately - there's strong strong interest from many people in being hybrid - in terms of people who have never been to IIW before.

Phil: In the four times we've been virtual we've had not just a few, but strong group of people who have never been to IIW before and many of whom would never travel to go to a conference.
(**Heidi:** probably 50% easily)

Phil: And so in the spirit of inclusivity, we want to say….make this more accessible.

Dick Hardt: Those are two sort of different things. Because at every IIW it seems like there's 50% of the people who have never been before anyway.

Phil: Right, but these are people who won't ever come. Right...because they won't travel for one reason or another.

Dick Hardt: I get the lowering of the barrier. What about having virtual and live?. There's no hybrid. Just switch between the two formats. I think the hybrid's going to be problematic.

Phil: Yes, so that is an option - switching between them. So we do one face-to-face each year and one virtual.

Phil: There's a couple of things I think are tough with that. (1) As I said earlier, I think even if you don't do hybrid, people are going to do hybrid. They're just going to fire up zoom on their laptops and start, ya know, inviting people into their session. And now you've got hybrid but their really not part of the event. Their just there sometimes.

Dick Hardt: Sure, but that's been the case before, right. So who cares!

Phil: Yeah but we're much more use to it now, right. So I think it would just happen in lots of sessions.

Dick Hardt: Are we!?! Are we used to hybrid?

Phil: We're used to Zoom.

Dick Hardt: Right, we're used to it virtual. I mean, I'm speaking somewhat on my experience in sort of "quasi-remote" teams. You're either a remote first organization or not. And whenever it was kind of the "hybrid," everybody remote was really considered second class. You knew that you were going to be taking a back seat in a mixed meeting if you weren't there in person. And I know if I was trying to do something, I

was going to be in that meeting - in person - no matter what! Because, dialed in, I just was not going to be able to participate.

Phil: Yeah. And that IS one of my concerns. Like I said, I don't want the remote people to be "second class citizens (participants)."

Dick Hardt: And if I'm doing a presentation, I don't want to try and look after the remote people either - if I'm doing a session, I'm live and I'm there. I don't really want to have to deal with that (remote aspect), personally.

Other Participant: That even happened today, where the presenter is not paying attention to the raised hands and things. So even in the all virtual environment that happens.

Heidi: Speaking of which, I noticed Kyle that you've had your hand up for awhile and then you took it down. Do you have something to add...please?

Kyle den Hartog: Yeah, so there's two things: (1) the first time I raised my hand - the practical reality that I wanted to point out here -- My visia situation prevents me from being able to come - in a lot of cases. So if I go back to the United States - I'm a US Citizen but I'm living in New Zealand right now - I can't return back to New Zealand. Which means that I'm having to make a choice between attending an in person event or upending my life. And so, I'm going to choose to not attend the event, is the realistic scenario if that happens. **Phil:** Why does NZ hate you? :-)

Kyle den Hartog: They're closing their borders, is really what it comes down to. And even if I can get back in, I have to spend on the tune of about $7,000 to get back in, to pay for quarantine and stuff. [Phil: Wow] And so there's a cost prohibitive aspect that comes into play that, I mean, if I'm paying for myself, I'm likely not to do that. But, if my company's paying for it, that's their own decision. So that's one aspect that I think is going to come into play. Come next April, we're not going to have any guarantees of being able to come and go between countries for people outside the US.

Phil: Yup. Well, and that's why we didn't do it this time, exactly the reason.

Kyle den Hartog: Yeah, and I appreciate that. Because I was actually able to attend because of this.

Phil: Yeah. Okay. Other thoughts? Other thinking?

Lisa: Hang on one second - Kyle you said you had two things. Or was that two combined into one?
Kyle den Hartog: That was the first thing. I've forgotten the second, so no worries. **Lisa:** Okay, we're here when you remember.

Kyle den Hartog: It may have been, because I was just thinking about it - the facilitator aspect at play. What if we put a requirement to have a facilitator just like we have a requirement for a note-taker? It's an independent person, like the note-taker is rarely the convener. Well that's not true. I sometimes write my notes at the end.

Lisa: Right. And, for example, I'm taking notes now and different people take notes at different sessions. So while it's highly encouraged, and we do a strong follow-up to get notes, if we were going to do a facilitator for each session, it would be either a situation where we add to the "Facilitation Team" or try to limit the number of sessions/rooms that would have remote access/opportunity.

Phil: (referring to the Facilitator) I think they would just be assigned already.

Heidi: It would be along the lines of Joyce's idea, which is really the best if you're going to do it: there's someone in relationship to the remote person and the one who is live. And the two are doing it together. [**Phil:** yeah] So it's somebody that's actually involved in the session, not a person who doesn't know what's going on with that topic (not part of the IIW Facilitation Team).

Mike Jones: Yeah, and I think ITF kind of does that. But they try to do remote participation using their own custom tool. But, one of the things is …. they won't start until they have a note-taker and what they call a "jabber scribe" - which is somebody reading the online comments, who will then walk up to the microphone and ask questions for the remote people.

Phil: Yeah, that's interesting. And our rooms are probably not big enough that they need to walk up to the microphone, but it's the same idea. [Mike: Yeah]

Dick Hardt: Yeah, and it's a whole bunch of extra overhead. [Mike: it is] Having been chair in a number of meetings, and having to go and deal with remote people and having machine and looking at that, trying to manage all this stuff - it's just a lot.

Phi: It is overhead. And I guess it's the cost for the inclusivity if that's the direction you go. But yeah, it's overhead. And it's more cost, right. I mean running hybrid is definitely more expensive - just from a business standpoint - because you've got to have the CHM and we've got to have Qiqo Chat.

Now we've talked about how it might be interesting to have Qiqo Chat, just in general; but, that's a separate issue. But you've got to have both of them. It's a lot more overhead. A lot more work. Which is why Lisa, Heidi, and Dounia came and said "no, we're going to protect ourselves from all the extra work that Phil's going to agree to." [Heidi/Lisa: chuckles]

Dick Hardt: It's not just the cost to you running the event, it's the cost to everybody attending.

Phil: Yeah, yeah! I'm acknowledging that, and saying there's other costs as well.

Dick Hardt: Yeah. And as I mentioned to you Phil, I don't find the virtual ones nearly as useful as the in person.

Nathan George: Well, one of the things we have to acknowledge is that the virtual plus in person does create kind of a tiered access approach. I mean especially when we talk about a scribe who might read out a question. Someone in person has an easier time speaking up or interrupting, than someone who's over the video conferencing tool (or whatever happens to be). It's important we set whatever the expectations we need to set around that before we do it. Because in my experience, in the past, those who are online feel like they get to be observers, but they don't necessarily get to participate fully - in the same sense as those who are there in person.

Heidi: Also, given the nature of IIW and the type of conversations that happens, it's very different than an event that's hybrid - where it's a speaker, and an audience, and maybe there's Q&A. Because most of IIW - with the exception of someone who may share their slide deck at the beginning of a session and then we're going to talk - are active conversations. Which is a different thing to try and encompass, in my mind, than

Dick showing up and speaking to a room that's just receiving the speech or talk, and maybe there's Q&A. That's the piece I've wondered, just from being around IIW for so long. There's something that happens in the chemistry and with the people all sitting in the same room. That would be hard to create virtually/hybrid - unless you had those little robot things that people's faces showed up.

Dick Hardt: Unless somebody is going into the meeting or in a conference room that has the audio and everything set up to really capture everybody. Otherwise the people remote aren't going to hear the questions, aren't going to be able to participate in the dialogue or…. Like what happens in ITF, everybody goes up to the mic. So the remote people hear it. So you have to set up a mic. Here in a virtual world we all have our setup, so we can all participate in a way. But the sitting around in a room, it's really hard to envision how that's gonna work hybrid.

Mike Jones: Let me just say, especially after being at EMC last month, and I've talked to Phil about it - in person. In person is so completely richer than what we are doing now. Particularly for the kind of interactions we try to do at IIW, where it's multi-participatory….it's just crippled this way. If you're in the room you can look around the room and read people's body language. You can know what they are thinking. You can know if they're even paying attention.

Phil: Yeah, so like Dick always turns his camera off in these virtual settings and then it's his smiling Avatar. So I look at him/Avatar, and think "oh, Dick's really happy with what Mike's saying!" But he might hate what you're saying! I don't know….right! :-)

Mike Jones: I'm fine making accommodations for people who choose to be or have to be remote. But there is no substitute for being in the same place, where I can choose the bull room or I can choose any other room and actually see people. If we just admit that people are going to turn on their laptop camera sometimes, that may be ok. If we want to be more structured we could experiment with that. But there's a lot of back channel. The energy is really low at this IIW. And I think it's people are tired of all these Zoom calls.

Phil: I agree.

Mike Jones: I can't wait to be back in person and maybe we find a way to include people like Kyle who might not be able to come otherwise.

Phil: Yeah, and to be clear, I don't care if people turn on their laptops and have a session on Zoom with other people. That's not really the point. It's just that if we're going to be doing that with lots of people who are forced to be remote for whatever reason, can we make that situation better? I think that's the question. Or should we just say "no, it's face-to-face" and that's what you get.

Heidi: And then the next time it's online.

Phil: Or we do the interstitial events like we did this summer, that are online. That's something else we've done.

Kyle den Hartog: As somebody who would likely not be able to attend all of them, I know for next year, I probably will because I have to be back there for a wedding, and my residency aspect is changing as well…. So as somebody who'd like to be able to attend all of them, I'd much rather see in person events with king of intermediary catch ups online. Than what we've had here with Zoom. And that's recognizing that my situation at hand here would probably be one of the more affected ones. Because, as other people have

pointed out here, it's difficult to do the Zoom. Half the time I'm listening to the conversation at hand. And then the other half the time I'm working on stuff for like writing code or stuff like that. I don't put my full presence in, when I'm just on a Zoom call. And that's just out of natural habit of having things available to me that I don't think I encounter when I'm in person. Which forces me to focus on only the event and whatever session I'm physically sitting in.

Mike Jones: I was going to say, if I have any input at all….we should not have anymore virtual events unless we're forced to by health circumstances. A lot of people probably just won't come, and that might include me. They're so much worse. And you guys do the best job of virtual events of anybody, and I tell people that. But it's so much worse. It's not easy to make the case that it's a good use of my time.

Phil: You know, it's funny because I went home yesterday, and I was just beat. I'm sure you all felt the same way. And my wife said "well, so did you enjoy IIW?" And I said, you know, I don't know! (chuckles a bit) There were some parts of it that were really good; but man, it was hard. And so I acknowledge what you're saying Mike. I think you're exactly right.

Heidi: There's also a difference - Kaliya, Dounia and I did the one day, focused topic events. And it's very different because it's five hours and that's it. There's an opening. There's three sessions. And then there's a closing. And there's notes and everything that at IIW; but it's not even a full day. And if it's, you know we had 50-60 people Kaliya (?) or 40-55...that was a good number. You have plenty of sessions. A lot of different sessions on the same topic. And….it wasn't as tiring. And work got done in teh same format that happens at IIW - it was open space. In terms of considering interim events that people could broadly attend, 1 day is way different than 3 days. Now you don't get that great thing that happens over 3 consecutive days, where topics evolve and stuff.

Nathan George: As someone who has a team - and I have a bunch of people who want to go to these events - when there's a lot of those special purpose 1 day events, we often can't afford the time to send everybody to all of them. So when they're very purpose driven, or have a very narrow focus where I can say "this is the person on the team that gets to go to that one," it helps bring that energy of IIW into kind of a more regular process without having to be like - "we're going to shut everything down for 3 days" because everybody wants to go. Now, I don't want to lose that kind of cross functional/cross pollination that happens in the in person IIW - where I go to a philosophical discussion, followed by a deep crypto discussion, followed by the more user business case discussion. I think that's part of the value of what we get out of the in person IIW. But I feel like virtually, that happens a lot less than it happened in person.

And I don't know that I can explain why. But I feel like I end up in more thematic sessions. And I get less of the hallway track of… "oh, Doc's doing a session on this, and you really need to be there!" type thing... than I would get in an in person IIW.

Mike Jones: I can say why! Because in the Computer History Museum we have all these tables in the middle where people find each other. And they talk about stuff out of session. And then they'll sometimes say, "well, do you want to call a session on this thing we've been talking about?" or… "Did you know that this think Kaliya is doing is actually really pertinent, and we should go to that now" or… etc. It's the cross talk that in a scheduled set of or sequence of zoom calls there's no cross talk occurring at all. (Phil: Yeah). (Heidi: Even with the unsession - I'm making a joke. We've tried hard but it just doesn't work)

Kyle den Hartog: The interesting thing about it, I used to say this joke when we would actually have to fly to in person IIW events. The joke was - my day job doesn't start until I hit the bar when I go to IIW. And what I was actually implying was this: I have much better success of hearing out somebody's position, or

convincing somebody of my position, when sitting in a conversation at the bar with them to move a standard forward; than I do with the actual in person events in a lot of cases. Because that's where the one-on-one conversations are occurring. The other side of it is being able to sit down at the table. And that's all lost with this Zoom aspect at play. We don't have the dinners. And we don't have the sidebar conversations that occur. Because it's pick which place you want to be. And I think, as Mike points out, the those are the important points that we were trying to emphasize by way of doing the unconference. It was facilitating a space where it's possible to have more of those conversations. The Zoom has really kind of disabled that capability and made it almost like back to a conference style system of sorts.

Another Participant: And that's even with the spaces that you've created that are supposedly not presentations or discussions. Right? They're supposed to be just community. But I would wager nobody goes there. I certainly don't.

Phil: Very few people. I popped into one yesterday that had a couple of people - it was the coffee cart chat. And I thought "oh!, it looks like it might be interesting. I popped in, we had a nice little conversation. But yeah...it doesn't happen like the tables (at the CHM). It's definitely not the same thing.

Heidi: No (it's not). And at the end of the event, where you can gather energy to go and have your drink and dinner together, we're all so sick of Zoom we don't want to hang out in another Zoom room even with our drink. I know I'm tired. (Other Participant: same!)

Chris Kelly: I think, on a practical level, I haven't ever been to an in person IIW. Hopefully one day. But it's the practicalities of going to get a coffee or going to have lunch you can bring someone with you and continue the conversation. Where as here, I know I could put on bluetooth headphones and stay in a session and keep listening; while I go make a sandwich. But I need a break. I need to walk away from the formalized sessions. But it's tough to try and take someone on a conversation with me on a one-on-one basis for that.

Lisa: I think Chris is also adding to what you just said. One of the challenges I think that everyone has faced in the last two years, being online, is part of the culture of IIW...right. Culturally, we break bread with each other. When you think about it, around the world that's really where a lot of connections are made - is breaking bread with people. And I can't remember who it was yesterday that was saying - maybe Sam Smith - was saying there's parts of Asia where if you're not having a meal together and you start to have a business conversation it's considered rude. You need to bring food to the situation so that you can have that human dynamic. So it's definitely a challenge.

Phil: Yes. Food has always been an important part of IIW
Terry Hayes: No business until the third cup of tea.

Phil: Are there other thoughts or have we exhausted this and we should all go to different sessions?

Lisa: I will say this, Phil...Oh, I'm sorry, go ahead Kyle.

Kyle den Hartog: I was going to say that I feel like I'm convinced that in person is just irreplaceable. You guys have done an excellent job of facilitating; but, in person just remains irreplaceable. I get some of the IIW magic (virtually). But I feel energized when I'm done with an in person event. Whereas when I'm done with the virtual one, I just feel tired. I feel like I need to take a nap.

Dick Hardt: Yeah, I was wondering what/how you guys are going to summarize what you took away from this? I was interested in hearing.

Phil (smiling/joking): "Dick hates all of the remote people and doesn't want us to accommodate them." That's basically my report out. (everyone laughs) **Phil Continues:** No, no…. I think my report-out would be: We had a good discussion about this. And the strong feeling is - face-to-face is so much superior to remote. And hybrid introduces enough friction that it may not be worth the effort or the cost in terms of both people and other things. Now I'm sure that what will happen after that report is I'll get lots of email from people saying "Oh, I can't come please, please, please, please, please…", so…

Dick Hardt: I think there is some value in…. The hybrid one is the one I am concerned about. The remote can work for people who want to work remote; but trying to mix the two is problematic.

Phil: Yeah, that's a good point.

Nathan George: I was going to say, the remote does work for certain things. And it works quite well for certain things. And the in person is also kind of a necessity. We're seeing across the open source contribution side, that the communities work a lot better when they have touch points of being in person. It helps reduce a lot of the friction, a lot of tension, between personalities when there is an in person touch point. So as we consider doing an in person event, one thing to consider is how can we make sure and bring some of those communities in? Because a lot of the normal, in person, events that those communities naturally have on their own - like the different block chain conventions or conferences; or the different W3C events - a lot of those have gone a lot more virtual. And if we can bring some of those folks (some of those communities) in to have some kind of a touch point as subsets of our community, I think they would find and see IIW as more important to them. If they felt like they had place for that or if we could convince them to prioritize that.

Lisa: I'd just like to add a couple of things: (1) in the last two years, the notes forms, keeping the notes form online and having people access and complete on their laptops, even if they're in person, that has jumped exponentially in people contributing/completing notes from sessions. That's been a real positive; and it can still happen even with an in person event. But it would require improved/boosted WiFi. (2) the other notion is this - rather than calling it a hybrid event - you focus in for the Spring and attempt to do a few things well. So maybe you have 3 sessions or a few that are sprinkled throughout that are specific topics which can be accessed both live and remote - rather than trying to do it bigger chunk. Test it out with just a few and see if it can work and be successful.

Kaliya: One of the nuggets that I'm taking away is - face-to-face is super important and hybrid is very hard. I basically totally agree with what Dick said. I also think that there's a shift to more remote for several of the things that used to only be in person. Like I think W3C Tags and other people are naming things that are sort of within things that people attend within our community. So, IIW has always been a cross pollination place. And if we hold that, then we sort of invite key people from all these key constituencies, that we want to cross pollinate, to come to the in person IIW; but, we also perhaps think about what Kyle and others have suggested - these special topic events in between which are virtual. And we try to balance it out between the two, for the sake of cohesion in the community. And, potentially also work with…. You know, DIF used to hots its face-to-face meetings the day before IIW. Well maybe they keep hosting those virtually instead of…. What's our relationship to other things that are within our community but also their own entities? And so that's something I think we should talk more explicitly about. Because if DIF also pushes it's in person thing, only to IIW, then it's losing that connection to the virtual, right. So there's some things to balance out. That's kind of my takeaway.

Kyle den Hartog: Yeah, I'm glad you mentioned that Kaliya. Because that's sort of the idea I wanted to put forth too. I don't want to lose the two in person events. But I wanted to ask the question to the Facilitation team: Is it too much to add a third interim virtual event - such as like in July, where we do one of these virtual IIW's? And that's kind of an interim event that allows us to be able to allow more people to be brought in. Kind of to pick it up. And maybe make it like a 2 day event instead. And then use that as a kind of jumping off/springboard point to bring new people into the in person events. And catch the quality that exists in those.

Phil: We did a little bit, this past summer. Kaliya and Heidi ran these two interstitial events. One on business processes; and the other on UX - user experience. And I think that did help. Heidi was mentioning yesterday that some of those people, who'd never come before, came and ran sessions on business processes. They were just 1 day events, as Heidi was saying earlier. But yeah, that's an option for bringing remote people in.

Heidi: And doing a 1 day, in terms of getting it organized, is way less involved than the 3 day IIW for sure. Because we weren't soliciting sponsors, what needed to be tended to was much smaller. We were creating a good event space and doing notes and that part of IIW and doing open space. So, it's much less work for a 1 day event. Easy enough to show up and do it.

Kyle den Hartog: That's quite interesting because I knew about those two events, but I didn't attend them. What I find very interesting about that is they were almost diversity events, of sorts. There are ways for us to target specific targeted markets and say - here's what we do at IIW; and then to be able to use them as springboard things to bring the cross pollination that occurs there. Because I'm already convinced I want to attend IIW. But what's interesting about it, maybe these UX developers, or maybe these business people who are just finding out about the identity stuff, it's a good way for us to be able to target these things. So maybe we do something like, IIW for Asia Day. Or something like that where somebody who is in the Asia region is facilitating that; and it's an interim event to be able to try and get more people from Asia regions to come to the actual in person IIW events.

Heidi: I know for me, handling the schedule etc, one of the hardest things about the online event is dealing with all the time zones. And when I think about going back to CHM, and only needing to worry about the people that are there, and in one time zone; and, that we're only having five sessions a day and 15 sessions total not 24...even with all the other stuff that has to be dealt with - does Rich still have a coffee cart? And all those things - the span of what I'm holding immediately feels easier. Because when we're virtual, you want to attend to all the people in different time zones and make sure that you're communicating that correctly etc. So the interim events, having them be okay, Kaliya and I have talked about whether we orient them towards the East coast or West coast? Because whatever side of the US, then people from those other countries could come. But we weren't trying to be inclusive of the whole globe (for these interim events). And that made it easier too.

Dick Hardt: One of my thoughts was, maybe there'a a virtual session scheduled during the live one that's like a one hour session that virtual people can sign up for. Something like that. That's then configured for it just to be virtual. Although, it's hard to think about how you're going to have that at any kind of scale with a bunch of different presenters. So as I thought about that suggestion, it didn't seem like such a great suggestion anymore. And then, the other idea….I find that 3 days of virtual is like Wow! That's a huge amount of time for the value I get out of it. Whereas, a half day….
I think there's a huge value that you guys have found in being able to tap into people that normally couldn't go. But, maybe just making it a small time frame, and having that maybe on a quarterly basis? or, maybe

it's only half a day? Or something like that. So it gives people a taste of it. And then they say "Hey, I got a lot of value out of that, and I want to go to the in person one." Just tossing ideas out there.

Heidi: My imagination too is that - from some of the conversations of this event - for people who've been to the live event, that when we finally get to be in person again, everybody's going to want to be in person. All of our attention is going to be running in person again (from the IIW team to all the participants). And so the focus will be there. Even if the note taking is set up in QiqoChat and they can go get their pre-set notes forms and stuff like that. It's not trying to communicate virtually, in addition to being with people. Personally, as the main Producer with great helpers, to be there in person and then to also need to be attending to the logistics of "is the equipment working? And how many people registered today? And are the people who are remote having a good time?" I would find that challenging, at least initially.

Dounia: Yes, what you're saying is resonating. In the sense that...at first I was so adamant about hybrid being a good idea. And I'm realizing that there's also something about honoring being back in person, after two years. And so, I can't imagine how having virtual components to be a net positive. Especially if there is those satellite events that are designed for welcoming broader community. And then how these two weave in I think is something that we learn as it happens. Because some of these people might want to go to an in person IIW, but might never be able to. But I think it's too premature to think that through at this point. What I'm trying to say - perhaps serving people who want to attend but aren't able to, or looking at how to welcome more people into the community is not best done by having a hybrid element at the in person IIW without compromising the importance of being back together in person.

Mike Jones: I like the thought of honoring being back in person.

Kyle den Hartog:: Yeah, I found myself nodding my head when you put it in that way. I'd much rather miss an IIW because it's in person and I can't attend, than to lose the quality of having to consider all the other aspects when I'm trying to host something and trying to go find Heidi because the webcam isn't working; or because I couldn't find a facilitator. That just sounds like a logistical nightmare for you guys. You've already got enough to do as is with facilitating in a place like CHM and trying to deal with WiFi problems there. Adding more doesn't sound like fun, if I were putting myself in your shoes.

Michel Plante: I just want to bring up the fact that I have been attending IIW for the past 3 or 4 times, since the beginning of the pandemic. Because, for me, I'm based in Montreal. So taking a plane and going to CA plus hotels, restaurants, plust travel time plus everything...adds up quite fast. And at the same time, I realize fully that in person must be totally different. And on line I can do 20 things at a time. I can attend or not sessions. And when I don't attend sessions, I can go back to my real day job. I just don't know how I will be able to manage if it goes back to in person. On top of the fact that it's 10x the amount of money. I will have to make a difficult choice of actually not going or maybe going only once every two or three IIW's because of that. So in terms of diversity, I am diversity for the group. I'm also assuming that people from Europe, from India, from Brazil...all those guys that have been connecting online, won't find it as easy to go in person as it is to go online. So I would even be prepared to pay my entry ticket, a higher price point, let's say $1000 instead of $450. It would still cost me a lot less money than to take a plane and go there. So with the extra money from online only people like me, maybe we can higher a firm or somebody else to help out in the overall organization in logistics of hosting a hybrid environment?

Heidi: One thing, and I know it's not a huge cost Michel, but one thing just to be aware, is that the cost of the ticket for the in person event includes breakfast and lunch all 3 days; and, two dinners. And the most expensive ticket for the in person, that we have right now, is like the late corporate ticket. And that's not

even $600 or something. So the structure of the event does include meals. I know that's not hotels and that's not the plane. But that's our in person way of trying to make sure that everybody who comes can earth together, etc. I know you haven't been to an in person IIW, so I just wanted to share that piece with you.

Michel Plante: I'm not that far away. Montreal is not that far away from California. But it's still close to a six hour flight, plus a 3 hour time zone difference. So I have to fly in a day early; adn fly out a day later. So for me, it's minimum 4 nights at a hotel. [**Phil:** Yeah, as for me. **Heidi**: Yeah, and our European people, and those from Japan…]

Michel Plante: Yes, and for those from Europe it's even worse. It's probably 2 days, maybe not. So it all adds up very quickly. And if I go there physically, I have to take 4 days off my job to attend. But I do want to attend. For me, this is invaluable. So invaluable. Everything that I'm learning is just incredible. And I"m now being an advocate within the company that I consult for, about everything digital identity and with everything that I've learned about.

Chris Kelly: Yeah, I just want to +1 on this. I am based in Germany. It would be an undertaking to make the trip over to attend in person. Something I would love to do one day. But also, just to pull it out of the chat, Kaliya also mentioned, trying to liaise with some organizations like the Engine Room to make in person events more accessible for people who maybe could not afford participation. In the name of inclusion and diversity, I think Kaliya's idea of cost saving guide is also a really great tip. Particularly for out of towners - where is cheap to stay, or how to reduce the general costs of your trip. I think digital events are a really accessible way for people to get involved. Not only in terms of geographical diversity, but also smaller businesses, freelancers who don't necessarily have the financial resources to dedicate to buying a ticket or travel costs.

Kaliya: I have a couple of thoughts that are arising. One thought is about perhaps we're reaching a stage collectively that, across the board, we need to communicate better outwardly. So folks like Michel and those who are remote, have better access to the educational materials that would be helpful to them. I think our communities have been weak on that. It doesn't solve the richness of the learning in these groups, but we also can't just have that it's the only place you got rich learning from our community. I also think we could be better at explaining where different work activities happen on an ongoing basis. There's probably 15 working groups a week that meet within this community. And I can barely keep track of it, and I'm like super primed! And so, how do we support folks like you, Michel? Whether you come to an in person IIW, I'm just kind of curious where you participate when you're not at an IIW, if anywhere? And then I had another thought, which is like a possibility of….we've taken feedback early on from folks like Mike Jones and others who gave us very strong feedback that we needed to keep IIW, "IIW," and not dilute it with having satellite events. We have had a few in person events that are not main IIW and it was made very clear to us - early on - we had to label them as satellites and explain that they were "like IIW" but not the "real IIW" that was in Mountain View. And I hear that.
And I also think that there may be a bridging place. Our universe of people participating is growing. So are there other things?

Like I've had this idea of hosting "identity camp" in the summer. We'd say "we're all going to fun place x. If you're in the community, come hang out for a week." And maybe we do 2 sessions a day, but the rest of the time we're being social and hanging out. But those could happen on different continents. Like there could be a Europe one - like Chaos Computing Camp happened - or there could be….you know how do we support…

There is a super value for in person. But if we say the only way you get in person is to come to IIW, that may be hurting ourselves. Those were just some thoughts that arose from that. But Michel would you be willing to answer my question about where else you participate?

Michel Plante: Yeah, I'm involved in Sovereign, in Trust over IP in the States. And, in Canada, I'm involved in CIO Strategy Council, and DIACC. So I'm already spending a lot of my time, like 12 months of the year on those events. And now, obviously, like IdentityNorth and DIACC, we used to be in. We used to have in person meetings and that all stopped when the pandemic started. And they are starting, as well, to think just like you are - about going in person again. But at some point, there's only 24 hours in a day. So I'm sure I'm not the only one in this situation. But it's not going to be feasible for me to go to Vancouver, Toronto, and Halifax to attend DIACC, or CIO Strategy Council. So I'm going to have to drop out from a couple of events, if all those go back to being only in person. And I'm with you, Kaliya, when you say there's so much going on! Just for Trust over IP, I think there's 65 or 68 working groups! I'm only observing in about 3 or 4 of them. I just can't keep up. (**Kaliya:** Thanks.)

So what about if the decision is to go back to in person only, is there a way that you can systematically record all sessions? Because right now we're always asking, our participants if their comfortable with recording sessions. And I've never heard anyone say "no, I don't want this to be recorded." So why don't we take the default position that we record everything. No?

Kyle Den Hartog (shared an example of a conversation/session at a recent IIW with a group of people who did not want to be "on the record" because of the affect their comments might have on how they represent their clients, etc. in other settings.): This is a perfect example of, we wouldn't have had those conversations and had good crossroads with that group if we had to require the recording.

Heidi: And you use a good word, Kyle. Most of IIW are conversations. They're not presentations. Recording a presentation is different than a group of people getting together and jumping into the mosh pit of "how do we really think this should work?" And there are Books of Proceedings going back all the way to IIW 7, when I showed up to start people to take notes.

Kaliya: You can actually find notes from IIW 1 & 2 on the Internet Archive Wikis.

Heidi: I also think it's the nature of IIW and that it's Open Space. It's meant for the people that are participating, mostly. And it has generously, since the 7th IIW, generated notes which it shares publicly to the world. Anybody can go find them. And we do let people know "these notes are going out into the world, so don't put anything in them that you don't want out in public." It's kind of a fine line. But as a non-identity person, but a person who's been co-producing and facilitating, it's people like it. It's not the standard event format.

Kaliya: I was going to ask - what thoughts do people have about the idea of supporting regional in person things, perhaps in collaboration with other organizations, to meet in person needs for people who can't travel very far?

Phil: So the prototype of that was probably the London event that you did Kaliya, years ago. And then we went and did India. **Kaliya:** Right, we did do India. **Heidi:** We did 2 in D.C.

Phil: And it is interesting. You do get a different group of people when you move around. CHM is our home and we love it. But it does bias the conversation in certain ways. When we were in DC there were a lot more policy discussions, for example.

Kyle den Hartog: Yeah, who attend the events makes a big difference. And like where I was trying to go with the previous statement I said about "my work gets done at the bar" - the in person events, they fill the gap that aren't filled already by working group calls that we have weekly. Like the DID Com working group as an example - we discuss what we're going to discuss at IIW, the same way as we discussed what we are going to discuss next week on the working group call. Whereas like the in person event allows for you to breakdown the tension that builds up - in between the events - because you get to see the human side of people. You don't have to focus on the work side only and keep it bound to a 1 hr call or something. I think that's where the experience in person is priceless. That's why I'm willing to justify it. But then again, I have to acknowledge my bias that I don't have to pay for my plane tickets, I don't have to pay for my hotel. Whereas many consultants who offer different opinions do have to take those things into consideration. And that's where it changes the conversation in a way, because we lose them.

Heidi: The group of people talking here today, 16 years after this thing started, is absolutely because it's been meeting in person. And you've had the drinks, and dinners, and coffees etc. The personal relationships have been developed.

Dick Hardt: I agree. And that's why I go. A lot of work happened on a lot of Standards at IIWs. OAuth2, Open ID...less now that the world is moving to DID. Maybe all the DID people are doing stuff and I'm not tracking all of that. So I'm sure there's a lot of DID work going. One thought, one of the things that ITF does, is they have 3 events a year. And each of them is in a different geography. So there's one in North or South America, and one in Asia, and one in Europe for a year. This lowers the barrier for people who can't travel, as well. So there's one that's easier for them to get to. It spreads the effort around as opposed to everybody having to go to the CHM.

And while I'm throwing out crazy ideas - what if you were to tie one of the IIW to being saved before or after EIC? Where you've got a number of identity people in Europe already. And now, people can make one trip and make it a bit longer if they want to for both of those things. There are a number of things that tie into IIW, right. There's Open ID Foundation has a kickoff the day before. Like a number of other people tie things around. So IIW could tie to other identity related events at other times.

Kaliya: We did do those… we called them "Identity Open Space" things, one day pre…. This was even before there was IIW - there was a formal identity conference and the day before we hosted an open space in association with them. So I like that you're resurfacing this as a potential path to support in person connections across the community using open space. It's an interesting thought to reach out to EIC and sort of explicitly talk with them about maybe doing a day of open space next door.

Phil: This was very very useful. It's good to hear all that. So thanks everyone.

SESSION ZOOM CHAT:

From Kyle Den Hartog to Everyone: Could we pay for a few prepaid broadband hotspots to solve that wifi problem?
From Scott Mace to Everyone: Would CHM allow that?
From Windley to Everyone:
CHM is pretty flexible (especially with us)From Dick Hardt to Everyone: I LOVE MIKE!
From Kyle Den Hartog to Everyone: Stone wall name over here :)
From Scott Mace to Everyone:
The audio capture situation for remote attendees is untenable for those breakout spaces that don't have their own physical room (the tented-off spaces in the big room)

From Kaliya Identity Woman to Everyone: A day being 5 hours
From Dick Hardt to Lisa Horwitch (Facilitation Team)(Direct Message):
You are now the host :)
From Scott Mace to Everyone:
What about having a couple of time slots for virtual-friendly sessions, maybe one near the start and one at the end? Or sprinkled throughout the conference? Might need to survey remote-only folks to see if they would still participate.
From Scott Mace to Everyone: Must run, good luck all
From Nathan_George to Everyone:
While we appreciate the opportunity to express our opinions. This summary of "what has worked well" and "which improvements should we never give up" are probably the most important learnings from the session. (We need ways to make this work better over time if we are going to help the community get more globally inclusive)
From Kaliya Identity Woman to Everyone: like a 2 day? Business of SSI & UX and SSI
From ChrisKelly to Everyone: +1 for smaller online satellite events
From Kaliya Identity Woman to Everyone:
have the interim virtual event not be on pacific time.
From ChrisKelly to Everyone: +1 :D
From Kyle Den Hartog to Everyone: +1 A major factor I rarely wake up in time on the 3rd day when virtual
From Michel Plante to Everyone: sorry I just got in so I missed the start
From Kyle Den Hartog to Everyone: Absolutely! That's what I'm most looking forward to
From Kaliya Identity Woman to Everyone:
On a different thread of focusing on inclusion - building more relationships with organizations who do work on identity in the global south and getting funding from funders to support them being able to attend in person - I'm thinking of the folks at an organization like The Engine Room
From Michel Plante to Everyone:
Money problem. Online = $500, In-Person = $5000 (airfare, hotel, restaurants, travel time, etc.
From ChrisKelly to Everyone: +1 kaliyah
From Kaliya Identity Woman to Everyone:
I also think we need to work on writing up more about how to reduce costs when attending - like renting a bike :)
From Kaliya Identity Woman to Everyone: or renting a camper van and staying in the hotel parking lot
From Dounia (Facilitation Team) to Everyone: @michel - would you go to a 1 day event on more focused topics?
From Dounia (Facilitation Team) to Everyone: online*
From Kyle Den Hartog to Everyone: It's worth acknowledging my bias may come from the fact much of my costs are typically
covered by my company
From Scott Mace to Everyone: #SickBurn
From Michael Jones to Everyone: I need to run. Thanks for having this discussion.
From Windley to Everyone: Thanks Mike
From Kyle Den Hartog to Everyone: Thanks!
From Dick Hardt to Everyone: It was I did yep Working for me!

Have We Forgotten to Design for Consent, While We've Been Building for SSI (Round 2 - Participant Request)

Thursday 23F
Convener: John Phillips
Notes-taker(s): John Phillips

Tags for the session - technology discussed/ideas considered:
Consent Models, Mental Models, SSI, ToIP.

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

Session not recorded and chat notes not captured. My bad. I pressed end meeting without thinking… blame it on 8 hours sleep over the last 72...

Deck used to frame discussion is here (this is a separate deck to the one used yesterday to incorporate some of yesterday's comments).
https://docs.google.com/presentation/d/1JEKgLKNRXgZz-YxgWD74LJElIG0GTU4ZM17_nz_XrmI/edit?usp=sharing
Premise
[from the presentation deck]
In general terms, within the SSI world, we illustrate trust frameworks using diagrams like the trust diamond from ToIP. We spend a lot of time on the roles of the actors, the nature of the data that traverses these links, and how and when the data traverses them.

But what about the "why"?

For example, why is the Holder presenting a proof to the Verifier? Because they received a proof request? Why did they trigger the proof request? Why did the Verifier make the request?

My hypothesis on one of the Why's: before any issuing, requesting, and proving interactions, some form of exploration and bargaining has occurred.

We might say that "consent", in some form, has been agreed, a bargain has been struck, whether fair or Faustian.
(and yes I'm watching the emerging Schrems v Facebook news from Ireland with interest… some people are gaming the difference between contract and consent…, let's ignore that for now)

Yes we 'kinda' have consent in SSI wallet interactions. We might consider this useful, necessary even, but not sufficient.

These SSI wallet interactions aren't "consents" in the normally accepted sense. Here are just 3 examples of definitions of consent in a digital context (there are so, so many):

1. Consent of the data subject means any **freely given, specific, informed and unambiguous** indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
   GDPR

2. The use of personal information by companies should be permitted only in those instances where consent was **specific, express, and voluntary**
   "Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent", Nancy S. Kim, D. A. Jeremy Telman, 2015, Missouri Law Review

3. ...consent given by a consumer is **voluntary, express, informed, specific as to purpose, time limited and easily withdrawn**.
   Australian Consumer Data Right

In fact, while there are some elements that are common, there seems to be no generally accepted 'pattern' for consent, a.k.a "Where's my mental model of consent? [To the tune of "Dear Science" (the Hoverboard song)]

Here are some brief notes on the papers I've reviewed so far:

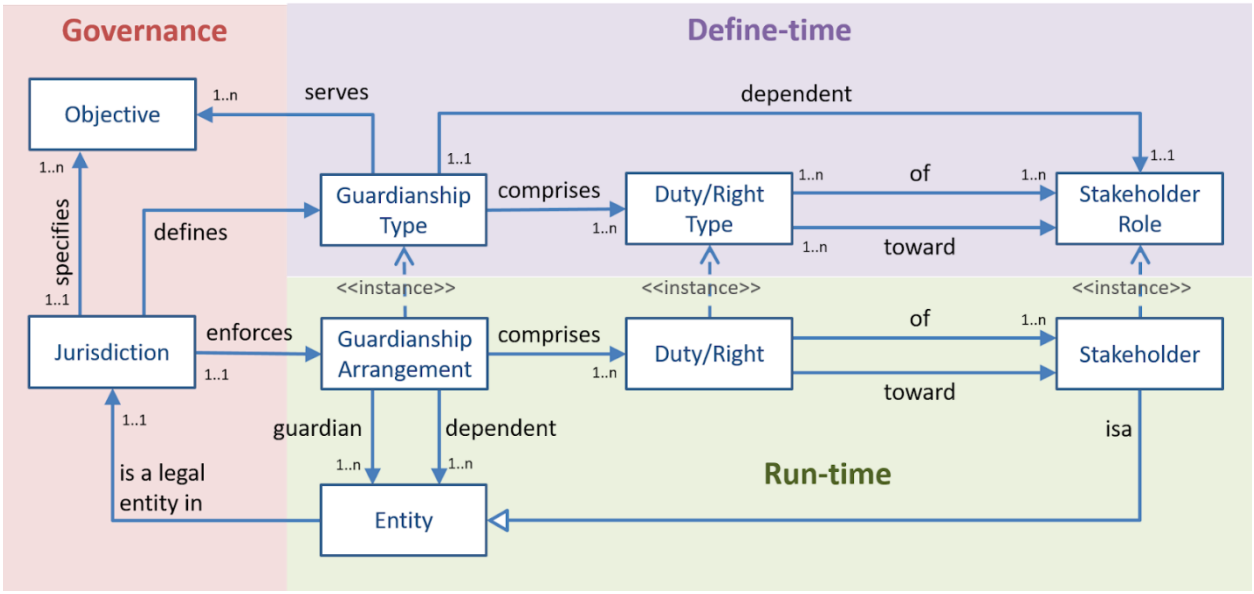
Title	**Comments. Useful?**	**Priority 1 high 10 low**
World Economic Forum. 2020. "Redesigning Data Privacy: Reimagining Notice & Consent for human-technology interaction", https://www.weforum.org/reports/redesigning-data-privacy-reimagining-notice-consent-for-humantechnology-interaction	Very useful. Very well written	1
Jenkins, Georgia. 2021. "An Extended Doctrine of Implied Consent – A Digital Mediator?", https://link.springer.com/article/10.1007/s40319-021-01024-2	Not useful	8
"FAIR Digital Objects for Science: From Data Pieces to Actionable Knowledge Units", https://bora.uib.no/bora-xmlui/bitstream/handle/11250/2737212/publications-08-00021.pdf?sequence=2&isAllowed=y	Interesting, but not directly relevant to consent models	8
Teare, H.J.A. Prictor, Megan. Kaye, Jane.2021: "Reflections on dynamic consent in biomedical research: the story so far", https://www.nature.com/articles/s41431-020-00771-z	Discussion on Dynamic Consent. Relatively useful.	3
Kim, Nancy S. Telman, D.A.J. 2015: "Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent", https://scholarship.law.missouri.edu/mlr/vol80/iss3/7/	Some useful content, includes a suggestion of "Specific, Express and Voluntary" as required attributes of consent.	3
Solove, Daniel J. 2015. "Introduction: Privacy Self-Management and the Consent Dilemma": https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf	This one is not bad. Legally based but an interesting explanation of Privacy Self Management and Consent	2

Neil Richards and Woodrow Hartzog, "The Pathologies of Digital Consent", 96 WASH. U. L. REV. 1461 (2019). Available at: https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/11	Useful and well written. Four key contributions: - vocabulary of pathologies of consent - ideal circumstances for consent - arguing against/explaining the privacy paradox - theory of consumer trust	1
Matilda A. Haas. Harriet Teare. Megan Prictor. Gabi Ceregra. Miranda E. Vidgen. David Bunker. Jane Kaye. Tiffany Boughtwood. 2020. "'CTRL': an online, Dynamic Consent and participant engagement platform working towards solving the complexities of consent in genomic research", https://www.nature.com/articles/s41431-020-00782-w	Yes in the context of NAGIM. Describes experience and lessons learnt in building of CTRL which uses online forms to generate DUO compliant statements about the constraints / use of the data about the patient for research.	2
W. Nicholson Price II, JD, PhD and I. Glenn Cohen, JD. 2019. "Privacy in the age of Medical Big Data", https://www.nature.com/articles/s41591-018-0272-7	Not bad, but not very useful	4
"Contracting Around Privacy - The (Behavioral) Law and Economics of Consent and Big Data", https://www.jipitec.eu/issues/jipitec-8-1-2017/4529	Slightly useful. Argues for the use of behavioural and "traditional" interventions in privacy law.	3
MEF Whitepaper: Understanding Digital Consent, 2017 (I think), https://mobileecosystemforum.com/programmes/personal-data/whitepaper-understanding-digital-consent/	"Mobile Ecosystem Forum" -	6
DUO - the Data Use Ontology - the essentials https://github.com/EBISPOT/DUO	The (GA4GH) Data Use Ontology (DUO) includes terms describing data use conditions, particularly for research data in the health/clinical/biomedical domain.	5
#### PLEASE ADD MORE TO THIS LIST IF YOU HAVE THEM		

I'm not researching this (just?) for fun, there is a real use case underpinning this exploration...We're (Sezoo) looking at SSI as a potentially better way to provide consent management for genomic data research being performed in Australia under NAGIM. This is a pro-bono piece of research/pilot work that, along with the other pilots, will receive a review in December this year from the world's most prestigious medical research centres - and then the follow up work may get grant funding.

This could be important, an SSI approach might become an adopted model for medical research consent patterns. That could be good...

So… I want a “mental model’, a simple but meaningful representation that helps reason about consent. Any type of consent, for any purpose. I’m thinking of a mental model like this from the eSSIF-LAB and Sovrin Guardianship Working Group:



[But this is a mental model for Guardianship, what would a mental model for consent look like?]

Summary:

Before: Mostly we’ve been thinking hard about the technology that underpins trust (which we must, it is evolving, enabling, constraining and essential)

Now: We’ve begun to think about how this must work with governance in human trust frameworks. Equally essential

Next: we should think more about consent, it’s human, important, and critical to sustainable trust.

Challenge:
So have we been forgetting Consent? Is consent a missing piece of our trust framework?

Discuss….

Premeditated notes organisation - only use if it helps

Additional Research to consider	Existing Implementations / Standards	Legal frameworks	Attributes/Qualities of Consent
List of ideas. Add them here please…	List of sources. Add them here please… Yoma?	List of sources. Add them here please…	All ideas welcome, can be themed later…

Discussion: John | Nicky H | Mark L | Vanu

Scrappy real time notes by John

Nicky H: Separate intent and consent. Model of rituals and tights

Mark L: Consent as a valid legal state

ToIP: Notice and Consent task force privacy controller credential. Privacy Broadcasting (Privacy as expected)

Making standards to make a record of that state.

Permission and consent confusion

Started at the do not track working group. Data Privacy Vocabulary Controls W3C

Council of Europe 108+ Trying to be bigger than the GDPR
https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108

IAB

Consent Record Information Structure

Dynamic
Broken into 4 parts:

1. Prefix (GDPR….)
2. Purpose specification (legal justification, legitimate interest, covid etc.)
3. Data treatment and rights (frequency, withdrawal process)

What rights you have
Purpose management rather than consent management
Consent “Grant” - Open Banking
Data Receipt is Contract
Consent scales in the EU, not in the US where contract scales (Terms and Conditions)
ISO SE27
Privacy Assurance the ability to benchmark privacy according to context and then measure the performance of their response.
2014 Consent Receipt Team led to Me2B

Privacy Broadcasting.
Privacy Policy Log as a minimum
Intent Data - School Education Record

Four (five) terms to manage in the mental model
Purpose
Intent
Consent / Permission
Preference

The Byway

Thursday 23G
Convener: Doc Searls
Notes-taker(s): Doc Searls

Tags for the session - technology discussed/ideas considered:

#Byway #VRM #VRMCRM #IntentionEconomy #CustomerCommons

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

We discussed Customer Commons' pioneering work on a new market model that can grow outside of Big Tech and customer-trapping silos.

The model is called *the Byway*. Here are four links that explain where it stands so far.

A New Way https://customercommons.org/a-new-way/

Byway https://customercommons.org/solutions/tools/byway/

Byway FAQ https://customercommons.org/solutions/tools/byway/byway-faq/

Paving the Byway https://customercommons.org/paving-the-byway/

A summary from one of those::

In the Byway model, intention signaling between buyers and sellers is maximized by providing a way for anyone to signal anyone, outside any company's private system. The best model we have for that is email. Like the Internet it runs on, email is NEA:

- Nobody owns it
- Everybody can use it
- Anybody can improve it

None of today's hundreds of different commercial messaging, texting, and chat systems are NEA. Even the biggest ones: (e.g. WeChat, WhatsApp, Facebook Messenger are closed and proprietary. This means the Byway is free to be bigger than any of them. As is email already.

Doc and Joyce Searls, both of whom are founders and board members of Customer Commons, are currently embedded in Bloomington, Indiana, to work with the Ostrom Workshop at Indiana University on rolling out and researching the Byway with local communities of interest.

This strategy and some of the target communities were discussed. We also reported on progress since the last IIW.

Wendy Gilch, of Selling Later, joined by Bill Wendel of RealEstateCafe, led a discussion of how the Byway could work for the real estate business.

Adrienne Meisels showed how a tool built by her company, MyPlanIt, is the "personal dashboard" Joyce and others have wanted for a long time.

Trust Taize - Time to Breathe and Trust (Quotes & Music)

Thursday 23H
Convener: Judith Fleenor
Notes-taker(s):

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

Judith Fleenor Opening Circle Explanation: *By Day 3 of IIW, our brains may be so full we just need some time to think about everything that has been presented.*

This session - Trust Taize - was created for a time to breathe and trust.

A Taize service has readings, music or chanting, and time of silence.
For this session Judith created a 12 minute loop containing music and quotes about Trust. Three is time in between to think about those posts (quotes).

The session was offered mid-day when participants might have needed a break.
This was the type of session participants could pop in for the 12 minutes and then jet off to another session. Or come at the end of a session to enjoy a little "space."

The loop ran for the entirety of this session ~ Come Breathe and Trust!

Credential Chaining - Verification of VCs In Non-Trivial Trust Networks (Open Discussion)

Thursday 23J
Conveners: Sebastian Schmittner <sebastian.schmittner@eecc.de> ,
Robin Klemens <klemens@internet-sicherheit.de>
Notes-taker(s): Robin Klemens

Tags for the session - technology discussed/ideas considered:
Credential Chaining, Credential Delegation, Provenance Proof

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

- **Slides:** 201014_Credential_Chaining_SIG_IDunion
- State of the art of chaining implemented in x.509 certificates
- Differentiation in credential chaining:
    - Provenance
    - Delegation

Second part: Example of GS1 system in different flavors of credential chaining

- Established system that is in production for many years
    - Hierarchical system
    - GS1 Global at the top, breaks down into national offices

PAC Theorem Reprise: Economic Incentives For Privacy. PAC Layering

Thursday 23K
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:

Sam Smith… *"We had some requests to reprise the PAC Theorem talk as we didn't cover all the discussions. In this session we start with the economic incentives for privacy and also talk in more detail about how we layer the PAC layers."*

Presentation Link Provided by Sam Smith:
https://github.com/SmithSamuelM/Papers/blob/master/presentations/CensorshipResistance_IIW_2019_B.pdf

Verifiable Credentials For The Workforce - A PoC

Thursday 23L
Convener: Mike Parkhill - Dock
Notes-taker(s):

Tags for the session - technology discussed/ideas considered: VCs

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

Session Slides: https://docs.google.com/presentation/d/1luzoregW3xjOB-P0vJT7tTwj_gCtzFJejfCWzTAXXew/edit?usp=sharing

- https://console.api.dock.io/ - Sign up and management console
- https://docs.api.dock.io - API Docs

Considerations and Trends in Children's Data Governance and Age Appropriate Design

Thursday 23M
Convener: Moira Patterson
Notes-taker(s): Moira Patterson

Tags for the session - technology discussed/ideas considered:

Children's Data – Age Appropriate Design – Respectful Technology

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

Thanks to the small but inspired team that joined the session.

The context for the discussion is the challenges around helping children and parents manage in an increasingly connected world, where the online/offline environment poses new challenges to children's ability to develop on their own terms and in line with their developmental needs. While there are important benefits and opportunities, the discussion focused around risks and how to address them - especially ones around privacy, safety, security, and ultimately the mental and physical wellbeing of children. We see this in education to the gamification of the play and recreational space and through connected toys or social networking services, there is an increasing merging of online and offline spheres.

We discussed personal strategies that people use to support their children, and what changes in the landscape could help address challenges. Even where parents are knowledgeable, the environment (peer pressure, network effects) is stacked against the judicious and measured use of tech, and there is a strong desire by kids to use technology applications, and sometimes ones that their parents do not agree with.

Resources:
IEEE has various activities in this space, including:

- P2089 - Standard for Age Appropriate Digital Services Framework
- P7004 - Standard for Child and Student Data Governance
- P7004.1 - Recommended Practices for Virtual Classroom Security, Privacy and Data Governance

Other ideas that were suggested:
-Check the Me2B white papers, as there are detailed analyses of children's and education apps
-Certification models that can help build consumer trust in products following good practices
-In VR environments, ensure that risks are known to users (incl. parents who may buy them for kids), and that the onboarding experience includes components that communicate benefits and risks and also VR literacy
-To raise awareness and understanding of these important issues, we need good analogies that connect with people -- "A story is data with a soul"

We discussed this in the context of increasing awareness of the issues, including legislative and regulatory developments, as well as increasing media coverage, and technology standards, best practices and other approaches are critical to furthering positive outcomes in this space

Scuttlebutt - The Gossiping Protocol

Thursday 23O
Convener: zelf (Zenna)
Notes-taker(s): Charles E. Lehner

Tags for the session - technology discussed/ideas considered:

Data Sovereignty, Distributed Systems, Community, Trust, Applications, Fun, Standards

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

Zelf (Zenna), Project manager for Scuttlebutt NGI - developing on the backend of Scuttlebutt

Scuttlebutt is a gossipping protocol, in both the technical and social sense. It is a protocol born of the IRC chat "mad scientists" that D. Tarr was part of. D. Tarr is a wild mad genius who lives in New Zealand on the boat. That is the origin of its creation - to be able to offline compatibly communicate with friends. It took off and grew rapidly into a larger social network. Now as far as we know about 25000(?) nodes/people…

[Presentation slides unable to be presented because of technical difficulties]

Offline-first social protocol based on social trust between people and nodes. Some of the reasons why the re-design of an internet architecture is needed is Data Sovereignty - people need to own their own data - and that goes for Communities as well. Maori communities using Scuttlebutt… culture…

Internet "centralized"... We don't own our data but need a continuous upstream to access it. Cumbersome and unnecessary for access to our own data - and our friends'.

Scuttlebutt is as p2p as we can imagine without NAT punching(?). Development in the past year: "Rooms" (?).

Rise of cyber warfare… Google services down for one hour… November(?) 2020… People couldn't even turn on lights in their own home because they relied on the connectivity.

Last week, Facebook and Whatsapp and Instagram were down for 6 hours, which is also due to a large extent to the Internet architecture design… continuous upstream, energy use…

Current Internet Infrastucture is quite exclusive, requires people to have high-tech devices to be able to access, they way we are used to in the Western World… 48% of the world does not have Internet access… easy to forget [when we have] open space technology online…

Climate crisis… 20 years collapse of society left?

Aaron: We're good at patching things…

Z: We're trying…

Our solution: open source trust-based(?) protocol…

Humans trusting humans with their communications… offline access to data (Data Sovereingy), open source (developed for and by the community)...
Illustrations....

Aaron: What's your relationship to the project?

Z: Project manager for recent core development of the protocol. I've been doing that for the past year through NGI pointer. A team of 6-20 people working on it in various ways (core group of 6 people).

What is Scuttlebutt? How does it radically change the pattern of communication and Internet as we know it?
… It's a combination of 3 different elements:
Version control (like GitHub)
Torrent-based sharing (kindof - sharing small packages of data)
Ledger-based storage.
These three, together with the format of how the data spreads - which starts with you, having a subjective perspective… We're each in our world… We have friends… You choose your friends, and they choose you… effectively establishing a data transfer agreement.
You store data on your computer… Each node acts as a server.
Your friends' friends - you also share their data and
Your friends' friends' friends' you see their data but do not store it.
Subjective view of the network: what you receive you have access to even offline - or over Mesh networks.

Aaron: Sounds like a lot of copies of any particular message…
Z: Yes…
A: Is the data explosion a problem?
Z: It could be if very large files are uploaded… That was a problem in the early versions of the protocol… Media files ("blobs") take up a lot of space. "Messages" (text-based) do not take up a lot of space.
Another solution developed in past year ("partial replication")...

If someone out of your social proximity, you don't know they are on the network, and they don't know you are… no way to know unless there is some social path of trust…

Aaron: Is there a concept that smells like a retweet? Reshares… may be 5 steps away… deliberate action, chain…

Z: Could be. So far none of the applications have that functionality, but hypothetically it would be possible. You can also have separate network keys - that is completely private unless you have access to that key. Highly private if you want it to be.

That's the basic outline of how Scuttlebutt functions.. Above mentioned 3 points, and the pattern of social trust of spreading data

Radical new way of having a social network… Also meant that there are many "hacky", "messy" aspects - very different from usual user experience… no passwords, for example. There's a hack called "pubs" - an automated node/peer in the network to act as a constantly online peer… to enable spreading data… Rooms developed to address that in part… a relay server that does not share any data… just connects peers.

Aaron: Like a Torrent tracker?

Z: Yes

Also implemented “partial replication”. Problem: have log you can’t change or delete data, might continue together, people continue talking for 30 years… that’s going to be a lot of data, even if it’s text messages. So we implemented partial replication. That means you can have multiple logs of identity - and can choose which logs should be replicated… which kind of media it is you replicate… you can put a max cap on the data replication, can make ephemeral logs… that was a big redesign of Scuttlebutt from the protocol perspective. Also a new indexing format… 10x faster. If you tried joining Scuttlebutt you might have seen it took an hour to do the initial sync… Now we have it down to about 8 minutes.

Aaron: is there a process for discovery? How to find peers?
Z: Yes, that’s what Rooms and Pubs are for.
Rooms are quite new, just finished last week(?)
Some rooms are running, but you may need an invite.

Aaron: like with Git… if I want to do a “shallow clone” I can limit by directories or by number of commits… is it all different channels and I pick some, or go back 100 MBs…?
Z: Everything possible, depends on UX perspective. From protocol perspective you can do both - but it depends on how it’s implemented.

Aaron: what does the protocol look like? Do I have to follow messages back to the beginning of time?

Charles: traditional replication…

Synchronization

Sync from log id and byte...

Security audit of new protocol
15 people designing the protocol together, trying to see what would be possible to build within the time frame, and what is important to build right now.
Went for partial replication but also made “fusion identity” - still a bit out there but has something to do with “tangles”... to link two identities basically. The identities can then share a log. Design is finalized but not developed yet.
We’re not an organization or company… just doing it as an interested [community], we’re decentralized… next phase: “P2Panda”

Aaron: … Fusion identity…?
Z: A difficulty for Scuttlebutt because it’s traditionaly based on [device keys].

Solved [many problems]. At this point pretty much starting to wrap up the package for our goals for offline-first trust-based communication protocol.

A: Ephemerality solved? Deleting data in distributed systems quite a thorny problem. If many nodes replicate, how do you know they deleted it?
Z: My understanding is that when you create a new branch you have to decide if it’s ephemeral. If you decide that it has a timer on it…
C: Could be based on trust?
A: Could be… need to ask [...], doing security audit… quite critical. But yes, social trust is important.

A: Need to be careful who your peers are…
Z: Also it is now possible to be incognito on the network so that only some peers see you and replicate, to avoid unwanted interactions.

A: Solution for large blobs?
Z: Long-time conversation... one is to offline to another distributed protocol (such as hypercore) - another is to limit your local storage.

A: IPFS? Content centric.. Scuttlebutt message-centric…
Z: Scuttlebutt is more community-oriented. IPFS more similar to hypercore in my understanding… a very different way of distributing the data… Different individuals choose to distribute certain data. IPFS used more for business backend solutions. Different communities. Scuttlebutt doesn't do VC funding(?)

A: Thanks!

Brent: Thanks. Could you add slides to the notes when they become available?

Z: Yes.

A: Links to protocol specifications?
Z: Many links… trying to clean that up.

https://dev.scuttlebutt.nz/
A "treasure map"

Scuttlebutt developed in a distributed fashion, different values, different ways of working…

[Discussion about Twitter BlueSky]

Aaron: Value of network control
… Dimensionality of trust… e.g. speech mostly commercial - do you want to see it or not?
… Closed systems causing a lot of problems that opens sems can solved… could be the future of platforms. Hard to get things off the ground, could gain learnings…
… like Windows NT was an experimental kernel but now it's "the kernel" - but they also had a … drawbridge kernel… then they killed that project and moved the learnings into the main product.

Scuttlebutt compared to git?
Z: Subjective sharing of knowledge…
A: Necessary for distributed system. One global truth means need consensus algorithm, means need to connect to Internet…

Enddy: Can identity cease to exist? If people decide not to store it…
Z: No, it always exists at least for yourself.
… One person once failed to get online, started using it as just a diary… Then they connected with someone and their "diary" went public!
… If you have friends, it exists with them too.

Dmitri: Huge fan of Scuttlebutt… tried it last year… but lost key…
… Is there movement towards more like DIDs…?
Z: Yes…. good to write down in notebook… (I lost my first one too…)
A: Key generated randomly?
Z: Yes… can use [mnemonic] words
… Dark Crystal project, developed a beautiful way of sharing your key and getting back through social trust…. But unfortunately couldn't figure out to send it back without something like email…
… DID part: scoped out of current R&D in past year… now handing it over to the next team of developers ("P2Panda")... Scuttlebutt is as distributed in organizing as it is in protocol…

Domain name owners?
… Individuals, no foundation

Fusion identity? Can't say how specifically it's designed, but can say by linking identities together you can have the same messages go to different devices.

A: What do you use for NAT traversal? STUN and TURN servers?
Z: Not doing firewall bypass… we're doing services that don't store…
C: Room servers are like TURN servers…
End-to-end encryption

A: HTTPS?
Z: Need to send you the documentation.

A: Most projects using distributed hash tables…

Dmitri: do you have an ask for us? As developers or standards community?
Z: So many ways… but hard to say…
A: Standards people tend to be good at writing a spec.
Z: We've covered as much as we need at this point… Next would like to have mesh networks (not proprietarily). From a Scuttlebutt perspective, we are getting to a point where… documentation needs to be organized. Needs to be a larger security audit of the protocol…
Some parts have been audited - but not as a whole.
From a standards perspective - I'm new to that, would love guidance on that, personally.
Next steps: fusion identity - ready to go

[Dmitri, Aaron and Balazs talking about standards]

Aaron: … groups not having best practices on standards… how do you start?
Balazs: Hard… some standards written and not used… some broadly used but never received formal specification…
… "We made a new organization for this standard"
… Multiple approaches for standards… Every organization that works on them ends up having their own format, usually. Big boring background, political…

Audit Report: Secure Scuttlebutt Partial Replication and Fusion Identity

https://ssb-ngi-pointer.github.io/Audit%20Report_%20Secure%20Scuttlebutt%20Partial%20Replication%20and%20Fusion%20Identity.html
Fusion identity ^ (Not yet built) - Does not cover Rooms or the new indexing format.

Z: Standards…?
Dmitri: depends on how much time you have. Easiest way: join conferences like this. Then, join working groups or interest groups… like the DIF Interop WG (https://identity.foundation/interop/)… Many have bi-weekly calls. Getting in touch with community leaders [...] is good too..

Z: Great!

Balazs: https://identity.foundation/faq/ - educational page for going from new to decentralized identity to understanding why it gets complicated… with different layers and considerations, building up a stack, to be helpful for certain stages. From this you can get an understanding of the DID framework - without too specific/technical (hard to write…)

[Talking about Berlin]

[Talking about Boston]

E: Open Source?
Z: Yes.
A: Then you get bought by Oracle...
Z: But what is there to buy…?

Best way to engage with Scuttlebutt is to go on it.
People flow in and out depending on energy levels. It's a very fluid community.
Best way to engage is with your friends.
Because of the decentralization… one must feel their way around the parts and pieces to see what to engage with… One thing always desired is documentation. (D: That sounds familiar!) Specifically, organizing the docs… it's everywhere… including the repos themselves.

The primary thing is to fun.

One way to have fun: we recently built a demo app, where you can build whatever apps you want - and it runs over Scuttlebutt. A distributed application sharer.

E: I'd like to join...
Z: Just join and ask "stupid questions"...
A: I've got plenty of those…

Enddy: Big apps in production?
Z: Most maintained one currently is Manyverse - also building a desktop app. Patchwork has been "tombstoned" - not being continuously developed… beyond that there are many… Oasis (still maintained?), Patchfox, browser-based applications (popular when you can't download whole applications), patchbay still used but not maintained.

Microledger Hands-On: Tools & Libs Where to Start & How To Use It

Thursday 24A
Convener: Robert Mitwicki
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

Microledger, Data Provenance log, SAI, SAID, SCID, KERI

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

We looked on the implementation of Microledger - a way to achieve integrity and authenticity which gives us data provenance log.

Human Colossus Foundation already developed already couple of tools/libraries based on specifications created in few communities like DIF, and Web of Trust:

Microledger specification:
https://github.com/the-human-colossus-foundation/microledger-spec

SAID

Self-Addressing Identifier (SAI) provides a compact text representation of digests of data. It supports multiple hash algorithms.

- SPEC: https://datatracker.ietf.org/doc/html/draft-ssmith-said
- CODE: https://github.com/THCLab/sai

SCID

https://github.com/THCLab/scid

Machine Readable Governance: Theory, Code, and the Future

Thursday 24C
Convener: Mike Ebert, Simon Nazarenko
Notes-taker(s): Mike Ebert

Tags for the session - technology discussed/ideas considered:

Machine readable governance, trust registries, roots of trust, workflows

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

Presentation slide deck: https://hackmd.io/@mikekebert/HyjBmusEF#/

Machine Readable Governance Definitions

Goals of Machine Readable Governance

- Provide information about roots of trust
- Organize the ecosystem by codifying rules, conventions, and standards
- Decouple (some) business logic from code
- Provide flexibility to accommodate change and avoid having to frequently re-release or update agents

Start with defining the ecosystem's assets, actions, and authorizations.

Components of Machine Readable Governance

- Governance files
- Schemas
- Presentation definitions
- Interaction documents

Governance Files

- Allow a jurisdiction to act with sovereignty
- Can be cached to improve offline operations
- Can be hand edited or generated
- We have written code that responds to governance when present but functions with it
- Agents can utilize governance but aren't bound to it (but caveat emptor!)

Meta Data
Schemas
Participants
Roles
Permissions
Actions
Privileges

Presentation Definitions
Used for verification (cryptographic) and validation (business logic)

Demo
Future: Workflows
Future: Composability
Future: Discoverability
Future: Trust Registries and Machine Readable Governance

Privacy Broadcasting #3 Consent By Default - with A Privacy Controller Credential

Thursday 24D
Convener: Mark Lizar & Sal D'Agostino
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:

Starting new threads under Privacy Broadcasting -

- Consent By Default -
  - For Consented Surveillance - with proof of notice and evidence of consent
- OPN - Privacy Broadcasting
  - Privacy Broadcasting Policy
  - Must have a privacy policy providence log for changes to state

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

This session will be recorded and shared with the Trust over IP
Notice and Consent Task Force - https://trustoverip.slack.com/archives/C018C813D5X

Killer Whale Jello Salad - (WACI-PEx Update)

Thursday 24E
Convener: Rolson Quadras and Brent Zundel
Notes-taker(s):

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

We gave a summary of the problem we tried to address during the Killer Whale Jello Salad sessions last IIW, i.e., a protocol for requesting and submitting a verifiable presentation.

After IIW, the work continued at DIF: https://identity.foundation/waci-presentation-exchange/

Currently the v0.1 spec is in DRAFT status, which means it is ready (we hope) for implementations.
Brian Richter demoed his (nearly complete) implementation (small issues with BBS+)

Rolson Quadras demoed SecureKey's (nearly finished) implementation (Still using DIDComm v1)

Where do we go from here?
We should have a way to do issuance using equivalent components
Issuance is (arguably) the same as presentation. Issuer:Holder::Prover:Verifier
There are some nuances that make them difference, but perhaps those nuances can be addressed by the pieces that are passed back and forth.
OIDC model also collapses issuance and verification
Andrew Hughes is writing a blog post related to this

Implementation experience has shown that WACI-PEx has been an "interoperability nexus"

Moving forward, it may help to be more detailed. What restrictions need to be put in place to address specific use cases? Further conversations along those lines will help us to address more of the wedge issues. E.g, key rotation and revocation - should rotated keys stay in the spec?

Maybe issuance and presentation are just cases of delegation . . .
doesn't quite feel right. Each of the actions has different constraints.

Another useful link: https://identity.foundation/arewewaciyet/

The goal is interoperable wallets with portable credentials for issuance and presentation.

Achieving Full Global Decentralization with the KERI Protocol

Thursday 24G
Convener: Timothy Ruff
Notes-taker(s): Mark Scott

Tags for the session - technology discussed/ideas considered:

KERI, blockchain, decentralization, discovery

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

Timothy Ruff (Opening Circle Summary): *This session will discuss achieving full global decentralization with the KERI protocol. I believe the era of blockchain based identity and blockchain based authentic data is waning. I believe that we will be able to realize something that a lot of us have had as a goal for a long time - and that is full global decentralization of identity systems.*

IIW 33	Session 24G	Achieving Full Global Decentralization with the KERI Protocol
Time	**Name**	**Sessions Comments (interwoven with time-stamped comments from Chat)**
	Timothy Ruff	**Introductory comments**: Timothy spent several years building SSI with a blockchain-based primary root-of-trust, but now believes that approach is detrimental to achieving the goals of SSI. Evernym went to great lengths to create and establish an open-sourced network for managing and discovering SSI components/solutions by giving away control to the repository. Initially this was done via the Sovrin Foundation, and later moved to the Linux Foundation as part of the Hyperledger project (Hyperledger Indy, Aries, and Ursla). What emerged in the intervening years, however, was a network-of-networks, many non-interoperable DID Methods, and too much complexity to be feasible in support of viable business models. Essentially, in the Identity space, everyone ended up using blockchain as a platform; balkanized, captive platforms with identifiers locked in. By comparison, what is needed, is a protocol-based approach to interoperable SSI solutions. For examples of the advantages of protocols over platforms, consider: 1) SMTP vs. proprietary email; 2) SMS vs. carrier-based messaging. KERI (Key Event Receipt Infrastructure) is a protocol, not a platform. It publishes a Key Event Log (KEL), has no proscribed place or network, and replaces platforms. With KERI, you control your own identifiers and can communicate across any domains.
		Some discussion ensued regarding Timothy's definition of decentralized.
	Timothy Ruff	We can't achieve the original vision of SSI without decentralization.

14:00	Neil Thomson	Agree - just look at the COVID Certificate Initiative (based on existing blockchain DIDS) and their trust networks-of-networks that are being proposed. Essentially a multi-centralized system with lots of friction to set up and manage.
	Neil Thomson	Multi-centralized efforts are not decentralized.
	Timothy Ruff	Agreed. I like that term, multi-centralized.
14:04	Aaron Goldman	https://docs.google.com/presentation/d/1r9O8cBPCqyT2Kx1uYYF7IVs0HRD1BfjjC3m_dJYGZHE/edit#slide=id.p
	Timothy Ruff	Timothy showed the table: Relative Decentralization of Identifier Systems
14:05	Timothy Ruff	https://docs.google.com/document/d/165Y_1a8THF23rbuTz6dbwhVcXvjn69ff1hG1-Fn17zg/edit#
14:07	David Wheeler	There is a short list of trusted root authorities for DNS.
	Phil Windley	Let's not bring DIDs into this discussion. Having 117 different DIDs is a good thing at this stage. A small number will prevail.
	Todd Snyder	Along with mention of centralized in the table, can also characterize as proprietary or closed systems.
	Drummond Reed	Decentralized is complex and hard to describe. A 40-page paper has been written defining it. [Reference?]
	Wenjing Chu	What about the unique processes for obtaining a business license in each of the 50 US states? Is that decentralized?
	Timothy Ruff	I choose what I put in my wallet. How do we get there with any centralized identity systems? How does KERI enable full decentralization?
	Sam Smith	Thirty years ago, PKI was proposed as the security solution to the Internet (see reference below).
14:09	Sam Smith	https://www.rfc-editor.org/rfc/rfc2693.txt

	Sam Smith	It consisted of PKI, signing, certificates, Diffie-Hellman, etc. The problem: managing private keys. PGP came along, implementing the concept of a web-of-trust, but didn't solve the key rotation problem. With an upgrade to algorithms, one had to reestablish key pairs, which with even only 40 PGP peer connections, became unmanageable. With KERI, it's just PKI and key management, without shared governance (which would make it harder). Industrialized countries know how to manage keys now (better than in the 1990's).
	Sam Smith	The PKI of DIDs is centered on method-specific identifiers. We can use KERI to prove control of identifier in a particular name space. Each DID Method is its own trust domain. KERI allows for one trust domain.
14:13	Zorigt Baz	I understand KERI is for key rotation. Can you give an example of how KERI could be like SMTP to which different platforms connect?
14:13	Vic Cooper	Is Global decentralization an end in itself or is there a greater goal?
14:16	Phil Windley	I think we're spending too much time debating what decentralized means.
14:16	Zorigt Baz	+1
14:17	Michael Shea	Is KERI a standard?
14:17	Henk van Cann	Not yet.
14:17	Kevin Griffin	@Michael it's on track for IETF.
14:17	David Wheeler	+1 Phil Windley
14:17	Michael Shea	Then technically, KERI is not Standardized.
	Stephen Curran	We can't use KERI today, correct?
	Sam Smith	Correct. We should use whatever is available today.

	Timothy Ruff	I see a dead end to identifier systems based on blockchain ledgers, as they don't have sustainable business models.
	Michel Plante	How far away are we on KERI?
	Philip Feairheller	Beta today. Pilot on 15 Oct 2021. Witness networks are available.
	Sam Smith	Production in Q1 2022. GLEIF will be offering vLEIs.
	Timothy Ruff	KERI will initially be used for communication, corporate filings, then transactions.
14:18	Sam Smith	KERI is about establishing provable control via cryptography of an identifier such that any statement made in the name of that identifier can be securely attributed to the controller of that identifier. Key rotation is how you maintain persistent control over an identifier in spite of key compromise.
14:18	Phil Windley	https://www.windley.com/archives/2015/01/re-imagining_decentralized_and_distributed.shtml
14:18	Phil Windley	Re-imagining Decentralized and Distributed. We're missing an axis: hierarchy vs heterarchy.
14:20	Sam Smith	Control is established by cryptographically binding an identifier to one or more (public, private) digital signing key pairs. This means control is established via non-repudiable signatures.
14:21	Stephen Curran	I can have a KERI identifier. Now I need to share it and others have to be able to resolve it. How is it easier to use than a DID with a given DID method?
14:21	Cam Parra	How would that world work in places where smartphones are scarce?
14:22	Sam Smith	There is a did:keri method. KERI identifiers are independent of name space. DID is a name space protocol. The method-specific identifier in a DID is the cryptographic identifier; everything else in a DID is part of the name space, but control of that name space is only cryptographically established versus.
14:24	Stephen Curran	So to use KERI, we need a 118th DID Method. It's not that I'm against — I just don't see how it is used on its own. Thus, comparing it to DNS or blockchains seems like apples and oranges.

14:26	Philip Feairheller	KERI doesn't need a DID Method, but can be used to back one. If a wallet supports the KERI protocol it can verify any KERI identifier with anything being on a ledger. If someone "gives" you an identifier, they have given you the KEL too, which is end-verifiable.
14:27	Phil Windley	I think calling DID a namespace protocol does it a disservice. If you give me a did:keri:…, then I should know I can use it in DIDComm, I can resolve it, etc. That's more than namespacing.
	Phil Windley	In a different way, Mike Jones said: Encourages everyone he knows to not use DIDComm because he doesn't trust the security features of a messaging system.
14:27	Philip Feairheller	And if they are using witnesses, then you can verify that there has been no duplicty for that KEL.
14:27	Phil Windley	@Philip, same is true of did:peer:... (your first comment)
14:27	Philip Feairheller	Not the last part, correct? Jinx
14:27	Phil Windley	:)
14:28	Cam Parra	Will KERI include that layer? To work for custodial wallets?
14:29	Philip Feairheller	It will be part of the specification and is currently available in the python implementation.
14:30	Rouven Heck	Where do you host the other DID doc/metadata for KERI DIDs?
14:30	Philip Feairheller	https://github.com/WebOfTrust/keripy
	Sam Smith	We need an independent audit of KERI code.
	Stephen Curran	There need to be layers on top of KERI to get us to the place of other more mature solutions.

	Timothy Ruff	Yes, we need trust frameworks, legal, etc. A chicken-egg problem.
14:34	Rouven Heck	That's why we have public chains with tokens 😄
14:34	Rouven Heck	@Timothy - how do you incentivize the witness & watcher networks?
14:36	Timothy Ruff	A controller pays them.
14:37	Henk van Cann	And verifiers could pay the watchers.
14:37	Rouven Heck	+1 Stephen - I think we compare different things.
	Timothy Ruff	Banks would do witness & watcher networks. KERI doesn't proscribe best practice.
	Stephen Curran	Wouldn't it make more sense to weave KERI into DIDs so you can find KEL? did:web is ideal for what a KEL would do.
	Sam Smith	Agree. If I could get them to adopt KERI, great. The design of KERI is such that it could be a trust-spanning layer of the Internet, across domains.
	Timothy Ruff	One sticking point. [?]
14:39	Phil Windley	You're going to be part of a governance framework, and different frameworks will have different requirements.
	Phil Windley	Do we need blockchain? We need discovery for public identifiers. Block chain provides that. How else do we do that without blockchain?
	Rouven Heck	There are three layers of separation with blockchain: 1) High layer [description?]; 2) Execution engine; 3) Logical layer of where to find things.
14:45	Nader Helmy	KERI needs some organized way to build advocacy and incentives structures on top of it. A DAO perhaps? In other words, one way to formalize a community of KERI users and adopters.

14:48	Rob Aaron	I'm confused by the word "discovery". Is this search-ability?
14:49	Dan Robertson	+1, same question as Rob 🤔
14:49	Zorigt Baz	I think it means resolving DID. Maybe.
14:49	Phil Windley	I give you a DID, you need to resolve it. It's not my DID, it's a public DID. How do you resolve that? You need to discover it.
14:50	Vic Cooper	One meaning is how can you find me if all of our connections are peer-to-peer with no centralized directory.
14:50	Timothy Ruff	That. :)
14:50	Dan Robertson	☑ Thanks for expounding, Phil. 🙏
14:50	Rob Aaron	Got it!
	Sam Smith	Regarding discovery: Agree blockchains are useful. KERI has primary root-of-trust that is irreplaceable (the KEL). Using blockchain as a (replaceable) secondary root-of-trust could be the best use of blockchain (in identifier systems). We want to find approaches with better performance, cost, latency, governance (as in less governance), which is what KERI provides (with, for example, Percolated Discovery and Verifiable Data Registry (VDR)).
14:52	Enddy Dumbrique	Nooo! This was so good. I wish that I had not walked in a little late.
14:52	Rouven Heck	Timestamping in discovery is helpful. How do I know it's the latest state?
14:53	Michael Shea	+1 Phil Windley
	Phil Windley	We're years away from KERI being implemented and available.

	Timothy Ruff	We can talk about blockchain as a dead end for identity systems and authentication.
	Phil Windley	One could take a more tactful approach.
	Timothy Ruff	Yes.
14:54	Rouven Heck	Would you take a bet? ☺
14:54	Timothy Ruff	Yep. A big one.
14:54	Rouven Heck	Ok - let's do it.
	Timothy Ruff	Within 3 years, no one in the identity community will be using blockchain as a primary root-of-trust.
		[missed the final few comments in the chat]

Self-sovereign Applications on "Authorized P2P" Infrastructure: Kepler Design Progress Report

Thursday 24I
Convener: Charles Cunningham
Notes-taker(s): You!

Tags for the session - technology discussed/ideas considered:

Storage, P2P architectures, authorization, control plane, deep nerd stuff

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

- Slides (<-- ***LATE-COMERS START HERE***)
- Demo video of Kepler used from demo front-end
- Other Spruce links: Website, Discord, Developer Portal, and a demo video of a project that relies on Kepler for per-user self-sovereign storage

Notes

- Presentation
- Q&A

How to Make SSI Systems That Inspire People To Act Rather Than Be Acted upon?

Thursday 24L
Convener: Bruce Conrad
Notes-taker(s):

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

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

Transcript of the session:
Bruce Conrad: So let me just start out by saying that I am by nature an educator, and I love everything about computer science, have since I was 14 or 15. I went to the library in the small town near the farm I grew up on and I checked out *all* of their books on computers, and I read both of them from cover to cover. And ever since then, I've been talking about computers and computer science and this kind of ideas to anyone who would listen. And I must say the biggest surprise was that most people weren't interested at all, in any of it. And so it's, it's been kind of a lifetime challenge for decades now, more than five decades, of getting people to listen, trying to figure out how to explain it to them. And one of the frustrations is that most people don't seem to want to take control of anything about themselves on the web. They're happy

to obtain a car, and take control of the car, or obtain other things and take control of that. But very few people are willing or interested even in acting on the web.

Most people that I know want to just sit in front of their devices, and be entertained by content provided by others. And so the question I'm asking all of you and I hope you have some answers, is how can we get people to choose to act on the web, rather than just be acted upon by the web.

So take it away. That's the question.

Jeff Orgel: Let them know it's possible. A lot of people have lost hope because it's so complex and it's been so trust-broken for a long time.

BC: Well, that's definitely the first step.

Marc Davis: There's some traditional answers, one is game dynamics. Right, so you gamify user interfaces people love, and leaderboard scoreboards, incentives, levels, easter eggs, like all the lessons from game design that people have applied to user interfaces is that if you can gamify the interaction people will get involved and do it. The other is to not think of it as an individual, but think about it as a network of people, and think about incentives that are not just individual but or social and that inspire people to work together as opposed to alone.

You know that basically if you increase engagement and connection that's going to those are kind of all this is about what are fundamental human needs and drives. Right, and feeling connected to others is one of the big ones, just why social networking is so powerful, and then the gamification is really, there's you know deep cognitive and the motive machinery around our reactions to this.

And so much of SSI, is emotionless right it's really it just doesn't have any juice. And it's not positioned in a way that is. And then, I think you do have to entertain to the point where you want people's emotions to be elicited, and they want to have a stake in what happens. Right? And I think there's a lot of fear of looking at it that way but I think it's essential to gain adoption.

BC: That's cool thank you thank you so much, Marc. The informal survey that I mentioned when I introduced the session was to 90 some students in a class that I'm teaching this Fall semester. And I was very surprised and shocked that so few of them even owned a domain name. And one way that I could gamify it would be to give them 10 points towards their final grade to demonstrate that they own a domain name.

Joyce Searls: I feel like this goes *way* back. Actually the age of television taught all of us to just sit there with our hands folded and be entertained. And frankly, public education doesn't do a very good job of showing people how they have their own agency and how they can do things. So I think we have this problem that you put your finger on, and that we find ourselves in is long seated, you know like, probably, 50, or more years of being taught to stand in line and fold your hands and, you know, go along, And so the populace in general doesn't have, they never got that, that juice of, you know, making that thing that that did whatever I mean, even, even in, in kindergarten now it's like they give you the, the picture with the lines in it and you color it in; you don't even like make your own picture to start with; it's like so sad.

So, I just want to start by acknowledging that were you, it can't be shocking that people want it done for them, we have made infants out of people. And so when we asked them to like take agency and make something cool and do something for themselves, the best you can come up with is like, oh, we're going to

go play this game, you know, so anyway, that's just my way of saying why we're here, but it doesn't give you a solution.

BC: Oh, those are great comments Joyce. When we started watching TV indeed we sat with our hands folded, we've since learned to get a snack and be eating while we're watching TV.

JS: Even worse.

Trev Harmon: I do want to push back on some of this just a little bit, and want us to explore it a little bit more, so a couple questions, so one, Bruce (not just you but anyone), what is the behavior you would like to see because you can have owning a domain name -- now I own a whole bunch of them. But I don't necessarily see that as an analog of whether or not people want to be engaged. And I also think that those of us that are sitting around, they come to this unconference, they come because this is something that we care passionately about. But we can't necessarily assume, nor should we assume that that means everyone else is going to be caring about it and we're basically asking ourselves, “Well, why doesn't everyone else care about this as much as I do?”, where I would forget there's plenty of things that those people care about that were like yeah I don't care at all. Yeah. I love sports and sports is great and all but I don't really care to follow it because I don't have a passion in that thing.

And I wouldn't want them coming to me and saying, “You aren't feeling passionate about this the same way I am,” and I understand that that's a little bit of apples and oranges comparison between some of the outcomes that we get from whether or not we are passionate about certain things or trying to fix certain underlying systemic issues.

But really bringing that back to the question of what is the engagement, what are the things that you would like to see in terms of actions of people taking that would help us get to where we would want to be. What is the behavior that we would like to see people doing because once we know that, then we can focus more on helping have that type of behavior for that. So, anyway, that's the question for you Bruce, and the question for everyone else.

BC: Yeah, thank you very much Trev. That's a good question and one that I probably should have asked myself in preparation for the session to be a little bit more detailed. And so I'm a little bit at a loss, and I think you've put your finger on it on my own feelings, in a way, “I'm passionate about this, why aren't other people passionate about it?”

Just as other people ask me about the football game last night and what did I think about it and I'm going like, “I don't know, because boys playing with a ball, I'm not interested in that.” So if someone has a more detailed answer to this question about what behaviors we would hope people would be doing. Please speak up.

MD: So, I mean your question relates to some discussions we had earlier in the day and prior sessions is that you have to kind of ask the question first is what is it when you say make SSI systems and inspire people to act rather than be acted upon. Well, act in what way and for what reasons? Right, so, and I'll just give a couple quick examples, like, I think there's one camp of folks here and I probably put myself on that where I see SSI, not just as a technological innovation, but as a path towards alternative political and economic relations among people based on self sovereignty. And so if you see SSI, as a path towards changing the nature of society and economy towards greater self sovereignty for individuals and non government, and non corporate groups, then you have a whole different set of things that you want people to do.

And if you think about ends and means too, what do you want them to do now versus what's the end state you're trying to achieve. If you think that society is just a great way for companies to optimize supply and demand and increase profits. Then, which is a legitimate way of seeing it as well. Then you have a whole different question so I think there's a question before yours, which is what's the model of SSI in terms of ends and means like where you are trying to get to and why. And then you can figure out what it is you want people to do. And I think in the community, there's a variety of answers to those questions. So in others I don't think there's one answer to your question, I think it depends on, you know, what is SSI as far as you're concerned in terms of what's it for, what are trying to achieve, what are the ends. And once you know the ends, then you can think of the means. So I hope that's helpful for clarifying the discussion, because I was thinking.

Do you mind answering it for yourself, I'd be curious to, like, what do you think SSI is for, what are the goals you have for it. What are the ends you're trying to achieve?

BC: Thank you, Marc. Yes. What one of the ends that I've been working towards, for all of the years I've been coming to IIW, four and a half or so, has been to be able to be recognized when I reach a website. So that, my account is known to the website without having to deal with user IDs and passwords. And for that to happen, the companies that host websites have to change. And for that to happen we as consumers have to be made aware that there are other alternatives and begin demanding them. I don't know. Does that answer the question that you're asking me?

MD: Yeah, and I think in an interesting way so that's in a camp about efficiency of economic transactions, but not necessarily self sovereignty, as a kind of political domain. I think that's an important distinction, right?, so people think SSI is about, hey, I want single sign-on to websites that don't involve passwords. Basically, and where my profile information is available to the vendor I'm interacting with, so that I can reduce friction in transactions, so reducing transaction costs, which could be achieved in ways that don't necessarily increase the overall self sovereignty of individuals in our political system.

Right. Those are orthogonal goals, and really important points. So, I would say for your goal for SSI, in terms of getting people to act, I would use incentives, like discounts, right?, you know gamification, discounts, loyalty programs that kind of typical ways, because you're looking at economic incentives and reducing frictions and transaction costs. And so then the mechanisms that come to play in those types of interaction designs are about, you know, incentification, gamification, and reducing the friction.

And one could argue that Facebook and Google and Amazon and Apple are all trying to solve your problem. In other words, a monopolistic so another hazard is that a monopolistic Single Sign On solves your problem, but you don't need SSI to achieve the end you just stated, you would need a winner in the war of single sign on. And one monopoly and you'd solve your problem. So that's why I think it's important to tease these out, right?

BC: Yeah. Very important. Yeah.

MD: And that SSI, from a political point of view, that would be a terrible outcome.

BC: Yes, it would. I was rather horrified by that, that one of the silos becomes so big and so efficient that it edges out all of the others, and we have almost *zero* sovereignty.

MD: Right, but as stated your goal would be achieved by that means.

James Ebert: Just to build off of that, one of the things that I would mention here is that you can also achieve that by incentivizing the business side when you think about doing a better kind of login mechanism with SSI and agents that we have, that can actually reduce the risk and liability of the business and improve the connection between you and that business. And that's value from that angle and if done correctly, that's a protocol or a transport like a mechanism, not a platform that is enabling that as well.

So you're not you're not creating another Facebook, you're creating a mechanism that people can interact with businesses. And you may need to get some businesses to kick that off, but there's that other angle as well; it doesn't necessarily have to come from the consumer, at least initially.

BC: Yeah that's a great point James. I like that; businesses do take on a liability when they store our information because then they're required to to treat it correctly. So that could be an incentive; thank you for that.

JO: Yeah, I like that idea. In terms of businesses sort of delivering the same to their customers, guess what we can do for you. Now that there's this architecture in place. I think your first question is you know, "How do you incent people to care about this sort of thing?'' and I gave kind of a hand wavy answer by giving them hope and letting them know it's possible.

And I guess, you know, how do you do the hand waving in the other direction? How do you build a hunger in the beneficiary community which are your, your folks who are going to have their data protected, what's the what's the 30 second movie trailer of the ideal world that they exist in, and how do you how do you impart the possibility, beautifully to somebody so they say I want that? Is it too fraught now like I remember lovingly not yelling at people but saying, you guys are talking about technology and you say how you're always chasing security. And yet this is like putting people on a roller coaster and you just said you really don't know what bolts hold it together so how do you get people excited, you know, to go hey get on this we think we've got the right bolts, man?

So yeah, I'm wondering what that story might be for SSI that would really encourage people to jump on and go for a hell of a ride you know and I know that's a squishy comment but yeah, leave it at that.

BC: I like the analogy very much, essentially, we think we've got the engineering problem solved, get on our roller coaster. That is wonderful.

JE: Something that I would add in to use your own thought from the last session, Jeff, if you can tell a story that's really powerful. When you think like here's an example is if you have to talk to your phone company, you have to talk to AT&T, and you have to sort out your billing or such. You have to verify who you are, you have to, like, every time you talk to them, and also do you have assurance that they are who they say they are? Like I feel like there's a really good story of simplifying what that relationship, looks like with your phone company, with your credit card company, with all these relationships we have, there's a lot of power of making people's lives easier and better and I feel like that is a story that end users are would be interested in.

BC: Cool. Yeah, Thank you, James.

MD: Yeah, so this is a response to Jeff's comment. I think there are two pairs of stories going back to my point about like what your end goal is. So if you're trying to appeal to people who don't care about the politics of self sovereignty, and they just want cool stuff cheaper, better quicker, you know, I think the story there is, is somewhere, you know, Bruce, what you're saying at the beginning is that if you have all of your

data connected together and under your control and you have delegates that can do it, the answer is, you can get the stuff you want more, you know when you want it for cheaper, like it's a faster, better, cheaper argument around consumption.

And I've made this argument to folks in the industry and they believe it too right it's like, well, if I had my purchase records and my location logs and my search queries and my browser history and transcripts of every phone call and every email and I can analyze all of that, I can build a better predictor of what I want to buy tomorrow than Amazon can, right? So there's a consumer argument of saying, you know, faster, better, cheaper to get you the stuff that you want that you want to consume. So that's the SSI, as an age of consumption within the economic frame.

There's a whole different argument if you're talking about people who believe in self sovereignty because they want to change the dominant social and political order. They would say that you want to adopt SSI because this is the way that you don't get surveilled. And this is the way that you turn our economy and society away from corporate domination and control. And so this is you know people that's what people are using Signal for today, right, you know people that are organizing protests are so you go after protest groups, people on the left, trade unions, credit unions, people that want to create alternate forms of social and economic and political organization. So the answer to the question, the story you tell depends radically different on which community, for which ends you're talking to.

There is no one story; that depends, who it's for, what ends, and so I've just given examples of two very different stories, both of which could be SSI stories.

I hope that helps.

BC: Yeah. Yeah, it really does Marc, thank you. And, and so Jeff we've got two very different movie trailers to put together.

JO: Yeah great points. Absolutely, it's very contextual, especially to the locale.

BC: Yeah. Trev, and then I have a question for Trenton, and one for Mike.

TH: Okay, so just building on this discussion on storytelling I'm here to tell a story so I can talk about storytelling.

So, when I was doing some work with the university and one of the courses we put together was human computer interfaces, and also a course I helped teach; now as part of that we made the IT students design an interface for a, a communications device, which they all thought every single group thought they were absolutely brilliant app; made them go out and do actual user testing, you know, post it note testing, specifically saying you may not talk to anyone for this testing that is anything like you. So no one that's in computer science, no one who's in kind of this whole thing, must be a quote unquote normal person.

And pretty much all of them every single time came back deflated because all of a sudden they found out that their great interface that they completely understood and and loved was not usable by anyone other than them.

And I think that the SSI community, with our storytelling, we have a bit of that problem: almost every story that we tell, and Marc gave some really good examples and some really good stories to tell, but I think almost all the stories that we tell are infused with the things that we know, understand and care about. And

again are trying to put that on to other people, and then we're surprised when it doesn't resonate the way that we think it should or would like it to.

So, anyway, just some thoughts.

BC: Thank you, Trev. That's excellent. I also have experience many decades ago with teaching a course on computing for humanities students and it is very interesting how differently people view the world.

Trent, would you just tell us a little bit about your experience, observing your wife, using applications.

Trent Larson: So, you know, as you were talking and asking this question, you know I love computers as well but I, it's hard for me to find my community. And the way I do it is with conferences like this. And I think the same thing applies in a lot of our lives where there's no way for me to get my wife excited, or my neighbors who like to play games that they're not going to be excited in these things. And, so I I just have to, I've come to the point where I'm comfortable just saying, Okay, I will just keep reaching out until I find the people that are interested, so that's my first comment is like, I'm never going to get her excited. I'll just keep finding people who are.

And then, my, my second is, I love the words that have come out about usability. Beautiful comes to mind, you know, of my designer at work says you know games are just for entertainment and they have the best user interfaces; here at work we're dealing with serious things that happen you know we need to get done and and make the world a better place but we have terrible user interfaces.

So, yeah, we just got to get better if we want to get those other users, and then we've got to understand how they see the savings, what's beautiful to them, even maybe the little Asana unicorns that fly off the screen and maybe those keeps us engaged for just a little bit longer than we need and those are kind of interfaces that we've got to… if we want a broader audience. That's what we have to use.

BC: Thank you so much, Trent, for elaborating, and Mike, will you tell us a little bit about the savings that could be realized by call centers?

Mike Parkhill: Actually, I have no idea; I don't work call centers, but I can just imagine. When I think about every time I talk to the telephone provider or TV provider or whatever and I spend five minutes proving who I am, while they have their purposes, I call them. That's at least five minutes of my day that's wasted and if they are doing 100 calls a day that's 500 minutes, easily lost right there and time is money and not to mention the frustration factor of repeating everything so I think there's a whole value prop there from my non-expert perspective of call centers, that could be saved by a better way of doing that.

MD: Talk to Vic Cooper about that.

BC: Yeah, I was going to mention Vic Cooper as well. Yes, he worries about this professionally. His job is to get call centers to use this kind of technology and others.

MP: Yeah, Vic just sent me his name on chat, and is looking at that; totally does seem like the right fit.

Brian: I just wanted to share with you something that echoes some of the themes that I've seen a lot of talks and discussion that are anchored very much on privacy, security. And while I personally or strongly behind all of that Mike, in agreement. Flows like account recovery, when somebody gets a lost broken device stolen. How do you adapt?

Those are moments of crisis where users really really care, and they're deeply invested and to me are opportunities to drive adoption.

And you'll get some uptake from privacy, security, but at the end of the day, when it becomes easier to recover from crisis. It's going to help people.

And just a general statement, I haven't seen a lot of emphasis on those kind of negative transactions.

It's more, let's build the base infrastructure, but when we start discussing adoption and rollout, it really to me becomes, how are you going to smooth out the known rough edges and do the systems in place, address those directly?

BC: Yes, thank you, Brian that's, that's a great point. And that's kind of inspiring people in a different way.

JO: Yeah, my day job is supporting computers; I looked after about 200 plus users and machines and all different scopes of people-ness, from medical through military to single retired women living on their own.

What you just brought up, the urgency factor, is wildly astute. How the human animal deals with stress and to what degree that particular human animal is invested in that relationship with that device. The tear out is pretty astounding, and I don't know if you've lived through that.

You seem to talk about it as though it's familiar to you. [Brian and Jeff realize they both work on technical and end-user support] Oh wow, we might be the only two! I don't know; I meant to have a session asking that question because, nice to meet you, Brian.

I self-certified my thing in this thing I called emotional rescue. And it's no joke that you know, data trauma based on loss and data loss and reputational loss, it's very real, so I appreciate that you brought that up, it got my attention promptly.

BC: Great. Well, I'm glad, glad that this session has introduced the two of you. I will just as an interlude tell another personal story. Many, many years ago, after having been frustrated many times trying to find someone interested in computers. As soon as personal computers became available, and people started purchasing them, they didn't know what to do with them. And so now suddenly not only were people interested in hearing what I had to say, but they would actually *pay* me to come and say it to them.

And I remember one group in particular was a group of farmers from far away from the city. And I traveled to their town, a town of about two or 300 people. One night every week for four weeks. And I talked to them about word processors and they were pretty content with that. And I talked to them about spreadsheets, and most of them got that. And then when, when the lesson on databases came along, it was just deer in the headlights.

And then as I was talking through the vocabulary. I happen to use the word “attributes,” database “records,” still deer in the headlights, and then I mentioned that database records had “fields.” And all of a sudden, every head popped up, and the eyebrows raised, and people said, “Fields. We know all about fields; we're standing in fields every day all day long.” And it was really hard to break it to them that I wasn't talking about the same kinds of fields.

So yeah, to Marc's point: nerds are excited about means; non nerds are excited about ends and the end they desired was to be able to use this computer they had just spent a couple of thousand dollars on to do something useful in their farming activities. And I wish I could have helped them more than I did. [Mike in chat: Most computer science students' eyes glaze over when databases come up too]

Thank you, Mike. That's funny.

MD: Yeah, I just wanted to say that I consider my, I'm a nerd as well so I don't want to have that be a blaming of anyone. This for good reason, especially in SSI as an emerging technology. We're deeply concerned with means, right?, we're really focused on how do we get it to work.

But we rarely asked about what's it for, what are the ends of the technology. And, you know, consumers, for the most part, and you know who aren't involved in the building of the technology, all they care about is what does it do for them.

Right? They don't care about means they care about ends. And that's, it's a whole different community and discipline, you know from UX designers and qualitative researchers and product developers that are focused on that question.

And I'd say by and large in the SSI community it's mostly, not completely, but it's mostly engineering folks, looking at means not product and and front end folks thinking about consumers are really just care about what are the ends.

And as I pointed out before, different groups of people care about different ends.

And that's that finding that alignment is really crucial.

BC: Great. Thank you, Marc. So we need to expand our horizons and imagine what some of the ends might be. And then think of stories and figure out how to make film trailers to demonstrate those ends to people. And then at some point we can break the news to them. Oh by the way, you're going to have to execute a bit of publicly available code, which will produce a public and private key pair etc etc.

MD: And you can Trojan-horse things too right yes, it's really important, this came up in a session with [Dave] Huseby earlier today. He's Trojan-horsing, his whole approach, and others. His ends are different than the people he's selling to, and he's undermining their interests. Ultimately, I mean, I don't mean to accuse it but in other words, there are rhetorical strategies involved in selling where you may have a different end than the people that you're selling to or you may have an end that you think you *want* them to adopt that they don't see yet, but you're Trojan-horsing based on meeting an end that they have now in order to get them to a different place; so there's a whole you know set of questions about what you believe and what you're trying to get people to believe.

And it's. And I think that's a discussion that hasn't happened enough in the community, some of it did happen today, but I really do see this divide between the kind of political economic view of self sovereignty as an ideological frame for SSI and SSI as a business optimization tool, which is a very different, you know framework.

BC: Now that's, that's great. And if you don't mind, Trev, I'm just going to ask Joyce, if you're still here -- [I am] -- your rectangle is present. Would you prepare, after Trev, a brief statement of how, how you get people to get excited about the byways.

TH: Okay. Yeah, I just like to build a little bit more off what Marc was saying, as well. I think one of the tensions that we have -- and this is in the UX designers and the, the selling all of those things -- is that SSI, as we are, as we currently do it is about, you know, individual user control for whatever types of ends you want, that tends to be one of the foundational things that we all build off of. At the same time, that individual control means that the individuals have a lot more responsibility.

And a lot of our approaches add a large amount of new cognitive weight to what it is that we're asking and expecting users to do. So we're basically saying, okay, like Marc was saying, you're going to have to have these keys; now maybe we can hide the fact that they have those keys that are being generated, but then we're saying okay, you're now responsible for knowing who it is that you're going to connect to. And you're responsible for verifying that and you're responsible for knowing what they should and shouldn't be asking you for; you're responsible for knowing what things are dangerous to share, not just in general, but with this particular person or entity that you're interacting with in general, and by the way this is living on your device and if you lose your device this all goes away, so you need to know how to back this up and put it somewhere, and also be able to restore that later when things go; so we're asking for the, for holders in particular to have a huge amount of new cognitive load.

And there's the tension of if they don't have that load then they are able to do what a lot of us would like them to be able to do which is to be self sovereign in their actions.

And again this goes back to that storytelling thing of those of us that feel this is really important go yeah I'm willing to take on that additional cognitive load in order to do this thing that I think is important but it's a hurdle that we still need to get over and so hopefully this point I've talked long enough for Joyce to have her statement prepared, tell us how they're looking out for this with byways.

BC: Thank you so much Trev. With great power comes great responsibility. You're right.

JS: So I'm, I'm uniquely advantaged in this in that I am not a nerd. So I really come totally from the other side. Um, but I've been exposed to enough nerds, to understand a little bit about them.

And the story I always tell about this kind of thing this kind of question is early on in the 90s, I remember going to something that was, you know, a conference on the information superhighway; it was actually about like late night TV commercials, but they called that the information highway because in 1993 that's what you know what people thought the information highway was, but there were, like, 700 men in a ballroom at the Beverly Hilton, talking about you know basically late night TV commercials and one woman, besides me, and she got up and started talking about how cool it would be if there was something that could be for women that was on this thing called the information highway, because the only people that were on it were guys who were really into their whatever and she had a whole idea about what became wedding.com later right.

So, what, so I always tell that as sort of like the baseline story is that the main reason why Facebook actually happened in my opinion, is because women found it useful, because early on, there was nothing in the technology that interested women at all: Zero. What they need is help with, you know, connecting things in their lives, their, their friends and family to talk to, talk to the kids' schools, all of the things that facilitated women's communications in their lives.

And once they saw -- they didn't care what it was -- now we will put ourselves in this world, not because it's like a cool machine that does cool stuff. But because it helps me accomplish something that it was harder to do before. And so, I think if we get this through our, our technology brains that it's like just live where the

ladies live, or just live where the users live, to put it in nerd terms, cuz it, that's when you're solving problems that people want to be solved, then you get, then you get people to come around, it's, they're not into the just the coolness of the way the thing works, like, like many of us here at IIW are.

So back to the byway, that's what we're trying to do with the byways we're trying to solve a problem that communities have like right now there's a ton of communities out there and I don't care if they're like the collectors in the Midwest, who want to put, you know, dealers in antique plates from the 1930s or classic car parts; there are communities that exist out there doing all of this stuff, but they don't have a tool, they don't have the infrastructure, they don't have any of these great CRM systems or B2B systems or, or call centers or anything, they have nothing.

So the idea with the byway is to give infrastructure to naturally occurring communities of interest to be able to communicate with each other with an infrastructure that has as much -- what do you call it -- robustness to it as the big tech platform so I don't have to have it be the big tech platform. I can do it on my own.

A DYI kind of approach, but because we need the infrastructure, I want to share that infrastructure with other communities to get done what my community wants to get done.

That's, and it's working a bit; like right now, we're going to have a meeting at the Innovation Center in in Bloomington, Indiana, we're, you know, we went to try to do this, they invited us it's called the Mill it's their, it's their innovation center -- we're going to do an event called you know “beyond e-commerce” you know how to do it for your community. So, they're very excited about it.

So I think it's working and when you go where people live and what they care about.

BC: That's, that's super Joyce. Thank you very much. Then, in my mind, I'm summarizing what you said as begin with the end in mind, which to Marc's point doesn't come naturally to nerds who are more interested in the means. And, understand where the ladies are. I think those are two very important takeaways for me. I hope you don't mind me summarizing it so.

JS: No, I think it's great. I'm going to use that!

BC: Will, are you still with us? Your rectangle is. What thoughts do you have?

Will Abramson: You talking to me. Yes. I just been dipping in and out. So I can see can you repeat the question for me?

BC: I was just wondering what your thoughts were about what we've been saying but if what we've been saying is somewhat incoherent that's makes it a difficult question.

WA: And I think it's my fault. I've been not really engaged.

That's, that's that's quite all right i mean i think the question is like what can we do to move us to action, or like how can technology help us move to action.

And, you know, I think what you said at the start about the survey with only one person actually hosting their own stuff right like I mean I'm a techie and I don't do that either I mean I would like to do it more but I think it's, it's hard work, I think it's my perspective, it's hard work and it's like you gotta go learn and it

seems to change all the time with things that you need to know. And, yeah, so. Maybe on Joyce's thing I maybe it's like not how can I be moved to action maybe it's how can communities support that infrastructure or like that technology, you know, you know take on some of that burden because it is a burden to manage this stuff.

BC: Yeah, so thank you very much. Well you've added a third point for me to summarize Joyce's contribution, which is pay attention to communities. Thank you very much.

MD: There's another piece of gold in the story that you told, Bruce, that I think it's important to pull out. And when you talk to the farmers about databases and they perked up when you talked about fields; that in user interface design that's what's called a metaphor, and metaphors and UX designer are really key.

The reason we have a desktop on our computers is because it's, you know, borrowing from the previous desktop metaphor, and really good user interface design practice thinks not only about the communities, not only about the ends, not only about their motivations, but what are the *metaphors* that makes sense to the community you're trying to design for.

And of course one of the best ways to do that is what's called participatory design which is a whole process of bringing in the community and having them being involved in the design of the technology, but I think metaphors are really crucial.

And that's why your story is so great because, you know, your user community perked up on you. I mean it was a catachresis which is a mixed metaphor. You know that they misunderstood but in a weird way you could, like, imagine if you were taught database design by saying, we have fields and crops, right, what your fields and values, right, you know you could teach computer science in a farming metaphor.

You hit upon the metaphor by accident. So the word collision, because the semantic spaces overlap, but you could've taught the course by saying okay farmers, let me tell you about databases by talking about farming and crops and fields and plowing under things and letting things lay fallow and you know you could use the whole metaphor of farming to talk about databases.

And so I think that your story is great because it surfaces exactly this key point in the design of any technology is understanding the relevant metaphors that you want to use for the community you're trying to design for or with. [in chat: A hugely important and useful book: https://en.wikipedia.org/wiki/Metaphors_We_Live_By]

BC: Thank you, Marc. The wonder of hindsight. If I had thought of that at the time I might have had an anomalous small village community of farmers who are also database experts. That's a missed opportunity.

MD: How cool would that be.
Brian: I'm just gonna put out another blue sky thing, if we're really talking action and adoption.

To me, that also implies, how are you going to operationalize this? Joyce had a lot of great stuff to say about a community, but in communities you naturally build up leadership: experts that know a system and a technology or a method.

As this translates into something real: How do you operationalize it, especially in a decentralized system, who is a trusted authority?
Who does the user turn to when failures do occur? Do they turn to...

BC: Sorry. I would say likely, they turn to Brian and Jeff. Carry on. Sorry for the interruption.

Brian: Oh, no, it's a, it's a great interruption, because you have the means to do it, but then the intersection of the means and the people performing the action. And when they need help, that I think would be a very interesting place to push, because to go back to something like account recovery or a lost device, how do you manage that? And when we're talking about business adoption, that'll be one of their questions. In a very real sense, where do I route my customers, what do I do and who do I contact and who is culpable when these systems fail. So, I think it'd be wonderful to hear more on those subjects.

BC: In my experience, telling people about SSI, almost inevitably the person I'm talking to, If they listen to me long enough, will say, "What happens if I lose my phone?" So Brian, you're absolutely right, because they pick up on that immediately, even without being technical, they find the weak point in the story.

JO: Yeah, I've been playing with the idea of KY- PC, know your PC.

I think if you can encourage people to understand the relationship that they have and demystify what's going on they begin to move more closely into the space of functional understanding and functional relationship, so one of the analogies that I've been using for a fair number of years, and I always try and align things with nature and in particular our nature, if I may. So what I'll do to a person is I'll say you want to see your computers, you want to see its body.

Now I know what I'm talking about. So I do a Control Alt Delete and I pull up Task Manager Okay, I go over to the Performance tab and on the left column you see the CPU you see memory you see disk you see Wi Fi and you see maybe a GPU.

So I started the top and I say, a CPU is your brain is equivalent to your brain, we can see here how hard the computer is working, the RAM is its muscle we're seeing how hard it's having to work to hold up what it's thinking about; the discs are the busy hands and you see it's at 100% so right now going and clicking on things would be like tapping on somebody who you've asked to do work for you, like you and they're like, hold on a minute hold on and if you keep tapping ,you're queuing things up you drive him crazy, and the Wi Fi is a communications what we're hearing and talking about, and the graphics processing unit, if your computer has it, relieves the brain of being able to understand what it's seeing faster.

So when people get into a hung machine or they think their machine is hung up and they call me, they've learned to pop this and look at the brain; if I'm downloading from the internet I say if we do a download you're going to see that the hands are going to get busy after it listens from the web because it's hearing what it needs and it's putting it into the thing.

So the analogies can be really wonderful and very well-aligned with what people understand about themselves and I think they cherish direct line sensibility. It just demystified the whole damn machine. Suddenly it's like a dog.

And they understand why it's not responding or they can self diagnose it and it's low science in a way .

BC: That is great, Jeff, the people for whom you are the IT guy are blessed to have you in their lives. That's wonderful. Thank you. We're nearly out of time. Any closing comments from anyone?

MP: I think this is a great conversation and I think a lot of the comments hit home on my experience as a software developer and architect and I've worked with UX developers who don't care about UX and some who care very much.

And I've worked at companies that won the competitive battle like hearing about us, and you know yeah you can have a tool as 1000 times more powerful, but if I need a degree, to understand how to use the damn thing. I'm not going to use it. Whereas if I can give it to a kindergarten kid and he figures it out. Then, fantastic.

So I think we got to kind of go at it from that angle that we really are looking at people who they don't take the time to turn off your privacy settings on Facebook so you can see everything they post on Facebook. They don't care, but the other side of me comes back and says, Sure, but if I compare how many people do have privacy settings turned on now compared to 10 years ago. We've come a long way. so there is hope we can get there.

But we have to make sure we make a user experience where for probably three quarters the population, they can get the security they need, the privacy they need, the redundancy they need, without having to take on that cognitive load, and if we figure that out that's sort of the magic bullet and that is where we need to think about metaphors and think about how we make us look and realize that QR codes are actually scary to a large part of the population and not a convenience.

So, how do we get past that and how do we make that, so it's not a problem at all I really want to say to summarize my, what I'm taking away.

BC: Thank you so much. Bye, great summary. Thank you.

MD: So yet again for us your stories have pearls of wisdom and nuggets. So I just want to point out that your story about what you said when you talk to people about SSI or not technical and invariably they say what happens if I lose my phone.

And so there's tremendous information in that and I want to just point it out this way. What we haven't really done is not take our UX people here, it would have happened is a core usability analysis of SSI, in other words, what are the failure points

In other words, what are the failure points of failure? Where's their high cognitive load? Where's their high risk? You know we've been thinking because normally people here think of the systems as the machines, not the machines plus the people.

But if it's a socio-technical system which involves human beings and people working together, the analysis of where the points of failure, where the points of excessive load.

That's the kind of analysis that really has to be done in order for these systems to work, and I don't think that's happened. So I think your story is a great example where you need to do a socio-technical analysis of failure points, of excessive load, and the community hasn't really, as far as I know, done that yet. And so your story is a great indication of important work to be done.

BC: Thank you so much, Marc for that. Another funny thing about that "what happens if I lose my phone" story is that every time I escalate that question to someone in the SSI community, they direct me to Daniel

Hardman's paper about “what happens if I lose my phone.” But again, we're concentrating on the means there, and not the end.

JO: Yeah handling the emotional impact of that is a whole thing that I wonder if Daniel Hardman's thing touches on. Bruce, this is my last session -- I suppose all of us our last session this time -- and I hope I'm not out and you're sharing too far but you mentioned you're kind of kicking off your shoes and sitting on the deck a little more soon. I just want to express my appreciation for the companionship and the thought, just a thought. The bright beams of thinking that you shared with me up close and personal and with us at large, it's just been really great to hang with you and I sure hope that you're going to keep visiting us from the deck at least.

BC: Thank you. Thank you. Thank you so much, Jeff, I feel much the same way. And so, yes this is me practicing for retirement:

JS: Great. Practicing.

BC: Now I think I can handle this. And if I can't, as Vic mentioned, just a block away in the direction I'm looking, there is the public library that I can easily walk to, and sign into their business center.

I'll be okay and my wife and I are already talking about driving out to Mountain View in April, so hopefully we'll see you again.

JS: Cool. Thank you so much, Bruce, it was a good session.
TH: Thank you, Bruce.
MD: Thank you, Bruce, this is really great, really important and a great conversation. Excellent.

BC: Thank you everyone. I appreciate everything I've learned from you. And I'm looking forward to transcribing the recording, so that I can cement it in my mind, and it will ultimately be published on the web, for the world to see if they can find it.

MD: And make sure we get to it for the people on the call in the meeting that would be great.
BC: It will be in the conference proceedings.

Explainers Pt 2: After Brainstorm -> Planning/Outlining Explainers, Curriculum

Thursday 24N
Convener: Kaliya Young
Notes-taker(s):

Tags for the session - technology discussed/ideas considered:
Toward a Comms Community of Practice.

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

Kamal - proposal a wiki of SSI and how it might look - solutioning.

Way of looking - what problems we want to solve

What kind of content is a supply chain business trying to solve.
Certified Jem Stones industry - their industry bodies are yet to be convinced.

Business stakeholders and to understand the challenges
Systems integration
Changes in workflow.

Propose this lens.
Problems -

Audience - group of people
Industry -
Type of problems they have

Example:
Audience - Product manager
Industry - Supply chain
Problem - Consent privacy

Epistemology - management of knowledge

How industry is organized.
Many people are where many hats at different levels.

Too qualitative or too quantitative.
No one over-arching guide on how to create knowledge

Eg from parallel industry- been created in last 10 years?

- SMS automation
- FIDO

RFCs?
How Etherium has evolved - all different layers of Etherium managed differently
They really drive - Eth/Vitalik conscious effort to be community driven - documenting and sharing knowledge - community is strong - vs. technology being the best.

What role should DIF play - central body that can do these things.
Knowledge Management and popularizing.

There are at least 2 bodies who are funded to promote these technologies - DIF and ToIP

How did ETH foundation
Driven by incentives - bitcoin+smart contracts incentives.

Chris - Comms at DIF - slowly better about how we communicate about what is happening at DIF and talking about the technology.
Talk about a plurality of solutions - use a platform that is understandable and accessible in the community.

Work with Judith - work stay aligned - not duplicate work - leverage partnership and

Public Action Plan visible?
Milestones - putting
Weekly Community Comms call - strategize - collect feedback so far.
Link to weekly comms call at DIF
Link to DIF public calendar

Charles point - incentives.
Not problem - creating content - problem for SSI - come back that crypto community community is getting a lot of adoption but we are not getting it
Giving $ for articles that are written.
No incentive to issue and receive VCs.
We have seen crypto currencies building community.

Incentives are hard
What is the appropriate Tone to strike
Hardly disorganized and full of problems.

The foundation (DIF, ToIP) Comms people -
Why projects chose certain things.
Help them communicate about it well

Give them a chance to present.

Example: Sam Harris - invites people on to share their opinions.
- They edit things so they present things in the best light possible.

Giving the Leadership capacity to give their best story - why they did things the way they did.
Regardless of what we
Blogs websites / guides out there.

People not involved in the space are not going to come to the organization
They are going to read whatever is at the top of the search results
So SEO is the important.

Chris start a YouTube channel - solve 50% of the problem.
We need opinionated content - commission it.

Mediated Opinionated Content
Mike Jones - Daniel Hardman discussion about different choices.

Producing
Informational - Edutainment.

Learn to Earn - 3 platforms that do this
Polygon - has own course. You get paid - finish certification, complete it - issue a VC share on linked in.
Crypto Community is doing this.
https://www.coinbase.com/earn

https://phemex.com/learn-crypto/crypto-fiat

https://gitcoin.co/learn

We don't have enough talent or Talent Pipelines
Stickers - laptops

Collectable NFTs for Hackathon participation.

Went through below list of maybe topics

Judith - complete decentralized Universe vs. Decentralized way of VCs fith with Existing structures vs. Centralized phone home surveillance

We use words like "we" and "this community" has such disparate thoughts on what we should be doing.
Hard for a professional communications person.
Hard to take and package in any sort of message - message isn't clear.

DIF should communication - Decentralization looked at as a gradient. How DIF should represent. Here is the paradigm - then can talk about these things (particular protocols) - it fits into this paradigm
Can't talk about advantages and disadvantages. Its a spectrum.

Identity - then the other things these technologies can enable - not same conversation

Kamal - SSI is more then just SSI - more about trusted data.
Talk about your solution as a company - trusted data VCs
VCs relative to internet of things.

Hospitality and Travel Use-Cases posted to YouTube
- Walked through real world scenarios

Thoughts on what is needed:
I believe we have to meet the market where they are at and improve processes they have current strong emotional connection to.

Precedent:

- Verifiable Credential Flavors Explained
- Infographic for Verifiable Credential Flavors Explain
- Understanding the Global COVID Certificate Landscape

Interesting resource:
https://decentralized-id.com/

Explainers Comparing Key Things: ***That are simplified yet technically accurate***

Who are papers for?
Who is the audience - what is the purpose for the paper.
There might be more than one paper.

Business Leader
Technical CTO - influence

Who are decision makers that can say - YES
Who are the blockers that can say - NO
Different way to think about it.

Hope and promise - easy to merger and aquision
Massive Liability - can't audit data

What are the concerns of big organizations?

The range of philosophy / architecture:

- Decentralized Universe vs.
- Decentralized way of VCs fith with Existing structures vs.
- Centralized phone home surveillance

Include Use-Cases

Use-Cases would be good to develop - round out

- H&T SIG - using different perspectives

Cryptography Curves

- ED22519
- P256
- ____

Reason people pick different curves based on philosophy underpinnings.

Credential Exchange Explained

- OIDC-SIOP
- PE
- WACI-PEx
- CHAPI
- DIDCom

Danger of the QR Code Society and how to Prevent it:

Already Started - needs collaborators to complete

Identity in the Metaverse

(Johnannes is interested in this + unconf opportunity)

Comparing VCs to mDLs

- And the Hybrid - VCs do Gov I
- Where can VCs fit into mDL - Kantara wants to work on

Dark Actors in Today's Ecosystem and how SSI Addresses this problem

- ThreatMetrix and LexusNexus
- Trulioo

How SSI could reduce the dangers of Surveillance Capitalism

- + Its better then chinese system
- + Its better then Indian system

DIDComm vs OIDC models for Exchange
DID Methods & DID resolvers
Keri Explained

PKI - what it is and how it works in SSI

Potential metaphor to explain crypto: "mixing paint colors" — where a private key is a set of paint colors, and the public key is the resulting color from mixing that set. If you can produce the mixed paint color, you've proven you are the person who knows the set of paint colors that mix to produce that one color

SSI for Privacy Lawyers - why it is so much better

"The lawyers will save us" - The most effective "convincer" of why corp and gov IT needs to care about privacy - GDPR compliance and legislation on privacy.

Operational Arguments for SSI for Tech folks

- Privacy approach (they don't care about privacy)
- Operational Security - dont' have central service to run - operation easier - millions of people scalability -
- Scalability - Infinitely Scalable Low Cost Federation
- Openness to other - run digital infrastructure as a government - private sector can join.
- Open room for innovation - count more for governments
    - Give advantage for economy

Semantics

- None
- RDF
- JSON-LD

Making Facebook Obsolete - the path using SSI

- Might be a conference too

Deeper BackGrounders

Annotated Bibliography (maybe we do community annotation via Hypothes.is)

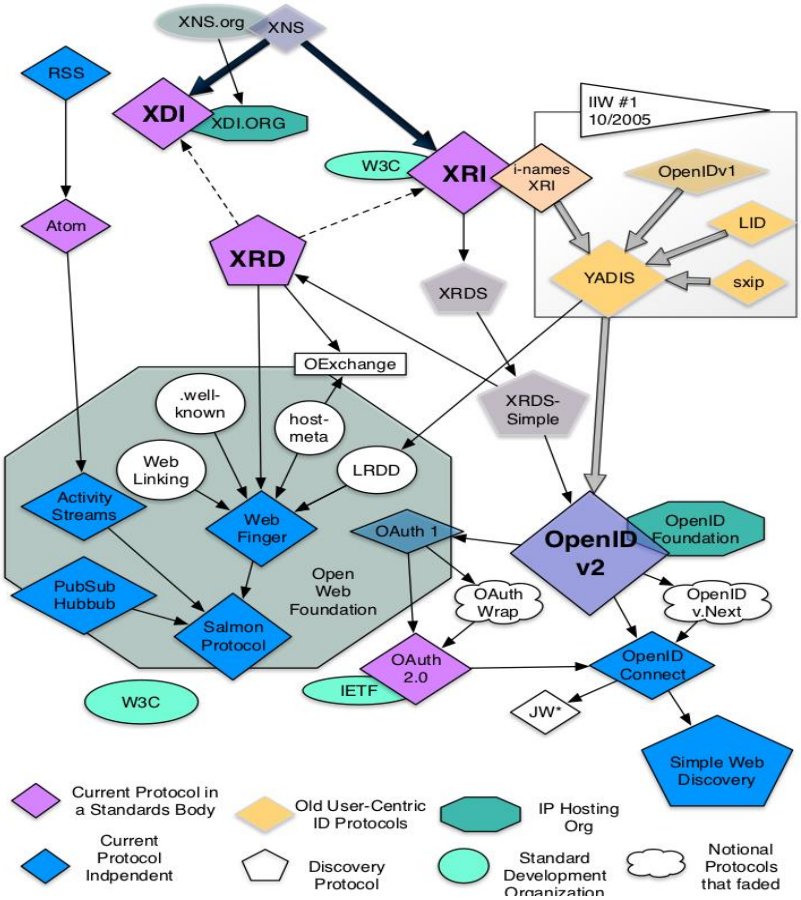
- Laws of Identity <- maybe write a new version with visuals?
- Relationship Layer of the Web - by Bob Blakley
- Becoming Artifacts by Mawaki Chango
- Protocol by Alexander Gallway
- Functional Identity

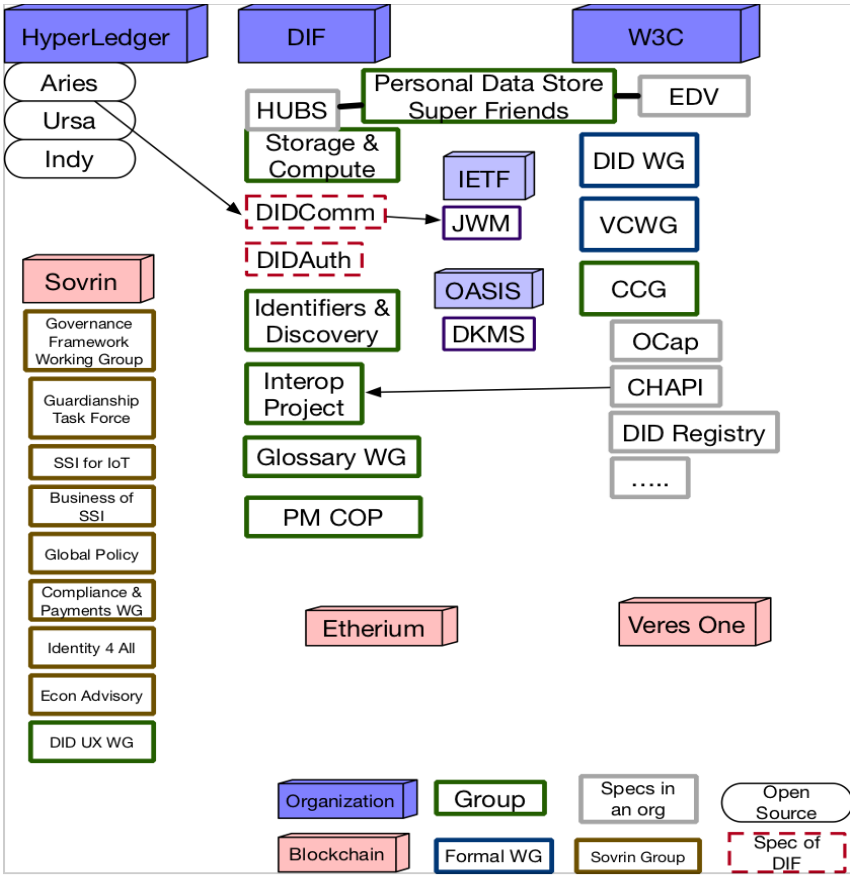
Core Identity Management Concepts

- Identifier
- Resolvable Identifier
- Authentication
- Authorization
- Identity Proofing
- Evidence of Identity

Identity Protocol Family Tree

Kaliya did some things sort of along these lines years ago:





Identity Protocol Families, a History - and the problems they solved

- SAML
- LDAP
- SCIM
- PIV
- MRTD (ICAO)
- DL standards -> mDL
- Information Cards
- OpenID v1
- OAuth
- OIDC
- Aadhaar
- DID
- VCs

Trade Associations of "other industries"

- Write with them on SSI for X
- Government Associations
    - AAMVA
    - NASCIO
    - Association of Counties
- HealthCare
- Education
- Travel

    - IATA
    - Hotelier
- Supply Chain
- Finance & Banking

Identity.orgs Industry Associations what they do, why they were founded, what they want done - how they relate

- OIDF
- Kantara (child of Liberty Alliance)
- OIX
- ToIP
- FIDO Alliance
- ICAO
- ITU-T
- IDPro
- NSTIC/IDESG
- DIF
- W3C-CCG
- ID2020
- Me2B Alliance
- IdentityCommons
- IIW
- EEA
- DIACC
- Sovrin
- Hyperledger
- Better Identity Coalition
- Secure Document Alliance
- Security Industry Alliance

Identity Events

- Connect:ID
- IdentityWeek
- IIW
- RSAC
- EIC

Standards Bodies & IPR umbrellas - the protocols they stewarded and how they work

- IETF
- W3C
- Kantara
- W3C Community Groups
- OASIS
- ISO
- ITU-T
- OIDF
- JDF (DIF & ToIP are under)
- IEEE-SA

Open Source Projects

- Hyperledger Aires, Indy, Ursa
- Cardea

Decentralized Web Actors/Projects

- Internet Archive - DWeb summits
- Matrix
- DIF

Scuttlebutt - The Gossiping Protocol

Thursday 23O
Convener: zelf (Zenna)
Notes-taker(s): Charles E. Lehner

Tags for the session - technology discussed/ideas considered:

Data Sovereignty, Distributed Systems, Community, Trust, Applications, Fun, Standards

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

Zelf (Zenna), Project manager for Scuttlebutt NGI - developing on the backend of Scuttlebutt

Scuttlebutt is a gossipping protocol, in both the technical and social sense. It is a protocol born of the IRC chat “mad scientists” that D. Tarr was part of. D. Tarr is a wild mad genius who lives in New Zealand on the boat. That is the origin of its creation - to be able to offline compatibly communicate with friends. It took off and grew rapidly into a larger social network. Now as far as we know about 25000(?) nodes/people…

[Presentation slides unable to be presented because of technical difficulties]

Offline-first social protocol based on social trust between people and nodes. Some of the reasons why the re-design of an internet architecture is needed is Data Sovereignty - people need to own their own data - and that goes for Communities as well. Maori communities using Scuttlebutt… culture…

Internet “centralized”... We don’t own our data but need a continuous upstream to access it. Cumbersome and unnecessary for access to our own data - and our friends’.

Scuttlebutt is as p2p as we can imagine without NAT punching(?). Development in the past year: “Rooms” (?).

Rise of cyber warfare… Google services down for one hour… November(?) 2020… People couldn’t even turn on lights in their own home because they relied on the connectivity.

Last week, Facebook and Whatsapp and Instagram were down for 6 hours, which is also due to a large extent to the Internet architecture design… continuous upstream, energy use…

Current Internet Infrastucture is quite exclusive, requires people to have high-tech devices to be able to access, they way we are used to in the Western World… 48% of the world does not have Internet access… easy to forget [when we have] open space technology online…

Climate crisis… 20 years collapse of society left?

Aaron: We’re good at patching things…

Z: We’re trying…

Our solution: open source trust-based(?) protocol…
Humans trusting humans with their communications… offline access to data (Data Sovereingy), open source (developed for and by the community)...
Illustrations....

Aaron: What’s your relationship to the project?

Z: Project manager for recent core development of the protocol. I’ve been doing that for the past year through NGI pointer. A team of 6-20 people working on it in various ways (core group of 6 people).

What is Scuttlebutt? How does it radically change the pattern of communication and Internet as we know it?
… It’s a combination of 3 different elements:
Version control (like GitHub)
Torrent-based sharing (kindof - sharing small packages of data)
Ledger-based storage.

These three, together with the format of how the data spreads - which starts with you, having a subjective perspective… We're each in our world… We have friends… You choose your friends, and they choose you… effectively establishing a data transfer agreement.
You store data on your computer… Each node acts as a server.
Your friends' friends - you also share their data and
Your friends' friends' friends' you see their data but do not store it.
Subjective view of the network: what you receive you have access to even offline - or over Mesh networks.

Aaron: Sounds like a lot of copies of any particular message…
Z: Yes…
A: Is the data explosion a problem?
Z: It could be if very large files are uploaded… That was a problem in the early versions of the protocol… Media files ("blobs") take up a lot of space. "Messages" (text-based) do not take up a lot of space. Another solution developed in past year ("partial replication")...

If someone out of your social proximity, you don't know they are on the network, and they don't know you are… no way to know unless there is some social path of trust…

Aaron: Is there a concept that smells like a retweet? Reshares… may be 5 steps away… deliberate action, chain…

Z: Could be. So far none of the applications have that functionality, but hypothetically it would be possible. You can also have separate network keys - that is completely private unless you have access to that key. Highly private if you want it to be.

That's the basic outline of how Scuttlebutt functions.. Above mentioned 3 points, and the pattern of social trust of spreading data

Radical new way of having a social network… Also meant that there are many "hacky", "messy" aspects - very different from usual user experience… no passwords, for example. There's a hack called "pubs" - an automated node/peer in the network to act as a constantly online peer… to enable spreading data… Rooms developed to address that in part… a relay server that does not share any data… just connects peers.

Aaron: Like a Torrent tracker?
Z: Yes

Also implemented "partial replication". Problem: have log you can't change or delete data, might continue together, people continue talking for 30 years… that's going to be a lot of data, even if it's text messages. So we implemented partial replication. That means you can have multiple logs of identity - and can choose which logs should be replicated… which kind of media it is you replicate… you can put a max cap on the data replication, can make ephemeral logs… that was a big redesign of Scuttlebutt from the protocol perspective. Also a new indexing format… 10x faster. If you tried joining Scuttlebutt you might have seen it took an hour to do the initial sync… Now we have it down to about 8 minutes.

Aaron: is there a process for discovery? How to find peers?
Z: Yes, that's what Rooms and Pubs are for.
Rooms are quite new, just finished last week(?)
Some rooms are running, but you may need an invite.

Aaron: like with Git… if I want to do a "shallow clone" I can limit by directories or by number of commits… is it all different channels and I pick some, or go back 100 MBs…?
Z: Everything possible, depends on UX perspective. From protocol perspective you can do both - but it depends on how it's implemented.

Aaron: what does the protocol look like? Do I have to follow messages back to the beginning of time?

Charles: traditional replication…

Synchronization

Sync from log id and byte...

Security audit of new protocol
15 people designing the protocol together, trying to see what would be possible to build within the time frame, and what is important to build right now.
Went for partial replication but also made "fusion identity" - still a bit out there but has something to do with "tangles"... to link two identities basically. The identities can then share a log. Design is finalized but not developed yet.
We're not an organization or company… just doing it as an interested [community], we're decentralized… next phase: "P2Panda"

Aaron: … Fusion identity…?
Z: A difficulty for Scuttlebutt because it's traditionaly based on [device keys].

Solved [many problems]. At this point pretty much starting to wrap up the package for our goals for offline-first trust-based communication protocol.

A: Ephemerality solved? Deleting data in distributed systems quite a thorny problem. If many nodes replicate, how do you know they deleted it?
Z: My understanding is that when you create a new branch you have to decide if it's ephemeral. If you decide that it has a timer on it…
C: Could be based on trust?
A: Could be… need to ask [...], doing security audit… quite critical. But yes, social trust is important.
A: Need to be careful who your peers are…
Z: Also it is now possible to be incognito on the network so that only some peers see you and replicate, to avoid unwanted interactions.

A: Solution for large blobs?
Z: Long-time conversation... one is to offline to another distributed protocol (such as hypercore) - another is to limit your local storage.

A: IPFS? Content centric.. Scuttlebutt message-centric…
Z: Scuttlebutt is more community-oriented. IPFS more similar to hypercore in my understanding… a very different way of distributing the data… Different individuals choose to distribute certain data. IPFS used more for business backend solutions. Different communities. Scuttlebutt doesn't do VC funding(?)

A: Thanks!

Brent: Thanks. Could you add slides to the notes when they become available?

Z: Yes.

A: Links to protocol specifications?
Z: Many links… trying to clean that up.

https://dev.scuttlebutt.nz/
A "treasure map"

Scuttlebutt developed in a distributed fashion, different values, different ways of working…

[Discussion about Twitter BlueSky]

Aaron: Value of network control
… Dimensionality of trust… e.g. speech mostly commercial - do you want to see it or not?
… Closed systems causing a lot of problems that opens sems can solved… could be the future of platforms. Hard to get things off the ground, could gain learnings…
… like Windows NT was an experimental kernel but now it's "the kernel" - but they also had a … drawbridge kernel… then they killed that project and moved the learnings into the main product.

Scuttlebutt compared to git?
Z: Subjective sharing of knowledge…
A: Necessary for distributed system. One global truth means need consensus algorithm, means need to connect to Internet…

Enddy: Can identity cease to exist? If people decide not to store it…
Z: No, it always exists at least for yourself.
… One person once failed to get online, started using it as just a diary… Then they connected with someone and their "diary" went public!
… If you have friends, it exists with them too.

Dmitri: Huge fan of Scuttlebutt… tried it last year… but lost key…
… Is there movement towards more like DIDs…?
Z: Yes…. good to write down in notebook… (I lost my first one too…)
A: Key generated randomly?
Z: Yes… can use [mnemonic] words
… Dark Crystal project, developed a beautiful way of sharing your key and getting back through social trust…. But unfortunately couldn't figure out to send it back without something like email…
… DID part: scoped out of current R&D in past year… now handing it over to the next team of developers ("P2Panda")... Scuttlebutt is as distributed in organizing as it is in protocol…

Domain name owners?
… Individuals, no foundation

Fusion identity? Can't say how specifically it's designed, but can say by linking identities together you can have the same messages go to different devices.

A: What do you use for NAT traversal? STUN and TURN servers?
Z: Not doing firewall bypass… we're doing services that don't store…
C: Room servers are like TURN servers…
End-to-end encryption

A: HTTPS?
Z: Need to send you the documentation.

A: Most projects using distributed hash tables…

Dmitri: do you have an ask for us? As developers or standards community?
Z: So many ways… but hard to say…
A: Standards people tend to be good at writing a spec.
Z: We've covered as much as we need at this point… Next would like to have mesh networks (not proprietarily). From a Scuttlebutt perspective, we are getting to a point where… documentation needs to be organized. Needs to be a larger security audit of the protocol…
Some parts have been audited - but not as a whole.
From a standards perspective - I'm new to that, would love guidance on that, personally.
Next steps: fusion identity - ready to go

[Dmitri, Aaron and Balazs talking about standards]

Aaron: … groups not having best practices on standards… how do you start?
Balazs: Hard… some standards written and not used… some broadly used but never received formal specification…
… "We made a new organization for this standard"
… Multiple approaches for standards… Every organization that works on them ends up having their own format, usually. Big boring background, political…

Audit Report: Secure Scuttlebutt Partial Replication and Fusion Identity
https://ssb-ngi-pointer.github.io/Audit%20Report_%20Secure%20Scuttlebutt%20Partial%20Replication%20and%20Fusion%20Identity.html
Fusion identity ^ (Not yet built) - Does not cover Rooms or the new indexing format.

Z: Standards…?
Dmitri: depends on how much time you have. Easiest way: join conferences like this. Then, join working groups or interest groups… like the DIF Interop WG (https://identity.foundation/interop/)… Many have bi-weekly calls. Getting in touch with community leaders [...] is good too..

Z: Great!

Balazs: https://identity.foundation/faq/ - educational page for going from new to decentralized identity to understanding why it gets complicated… with different layers and considerations, building up a stack, to be helpful for certain stages. From this you can get an understanding of the DID framework - without too specific/technical (hard to write…)

[Talking about Berlin]
[Talking about Boston]

E: Open Source?
Z: Yes.
A: Then you get bought by Oracle...
Z: But what is there to buy…?

Best way to engage with Scuttlebutt is to go on it.
People flow in and out depending on energy levels. It's a very fluid community.
Best way to engage is with your friends.
Because of the decentralization… one must feel their way around the parts and pieces to see what to engage with… One thing always desired is documentation. (D: That sounds familiar!) Specifically, organizing the docs… it's everywhere… including the repos themselves.

The primary thing is to fun.

One way to have fun: we recently built a demo app, where you can build whatever apps you want - and it runs over Scuttlebutt. A distributed application sharer.

E: I'd like to join...
Z: Just join and ask "stupid questions"...
A: I've got plenty of those…

Enddy: Big apps in production?
Z: Most maintained one currently is Manyverse - also building a desktop app. Patchwork has been "tombstoned" - not being continuously developed… beyond that there are many… Oasis (still maintained?), Patchfox, browser-based applications (popular when you can't download whole applications), patchbay still used but not maintained.

Notes in this book can also be found online at
https://iiw.idcommons.net/IIW_33_Session_Notes

Demo Hour / Day 1 & Day 2

Thanks to our Demo Hour Sponsors!

Stacks Foundation

DANUBE TECH GMBH

Demo Hour Day 1: Tuesday October 12, 2:30 - 3:30 (PDT)
Demo Hour Day 2: Wednesday October 13, 9:00 - 10:00 (PDT)

DEMO Table/SPACE #

1. **Tru Social Inc. beta App:** Jim Fournier
   URL: https://www.tru.net/how-it-works
   Tru provides verified social publishing built on JLINC. In beta, it connects networks of organizations and groups to people to help build effective movements.

2. **Spruce Systems - Walkthrough of the first Rebase Protocol:** Juan Caballero/Gregory Rocco
   URL: https://tzprofiles.com
   We will be doing a quick live demo of our first live implementation of our Rebase Protocol, the lightweight Tezos Profiles dApp, and answer technical, UX, and standards/adoption questions about the underlying open-source codebase and how it could be adopted to other contexts.

3. **Fyself:** Lianet Peña, Betty Franco
   URL: https://fyself.com/
   FySelf is the tool created to perform all kinds of online procedures from the digital identity. You can identify yourself, complete a form, take a survey or a smart contract, in which you can provide access to the part of your data that is necessary. It operates in the style of a social network, in which you achieve a digital reputation.

4. **HearRo Identity Based Communication (IDC):** Vic Cooper
   URL: https://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.

5. **godiddy.com - Universal DID Services:** Markus Sabadello - Danube Tech
   URLs: https://godiddy.com/
   godiddy.com is a hosted platform that makes it easy for SSI developers and solution providers to work with DIDs. It is based on open-source projects Universal Resolver and Universal Registrar.

6. **Aries Jupyter Playground:** Will Abramson
   URL: https://github.com/wip-abramson/aries-jupyter-playground
   An open-source Jupyter notebook based playground for education and experimentation with verifiable information exchange flows facilitated by ACA-Py.
   More Info:
   https://www.sciencedirect.com/science/article/pii/S2665963821000385

7. **TNO — "eassi" an SSI Gateway & Credential Catalog:** Peter Langenkamp
   Day 1: "eassi" an SSI Gateway
   URL: https://eassi.ssi-lab.nl/
   This service facilitates the adoption of SSI by providing an easy to use API, that allows credential issuing and/or verifying organization to integrate multiple SSI wallets—that may be based on different underlying technologies—with a single interface, taking inspiration from the payment service provider model for online payments.

   Day 2: Credential Catalog
   A catalog of offered SSI credentials types, helping verifiers find what accredited data exists so they can use it in their business processes. This encompasses not only technical information on attributes and protocols, but importantly also business-level information for decision makers, like assurances.

8. **SecureKey Technologies - TrustBloc Overview:** Rolson Quadras, Mike Varley, Troy Ronda
   URL: https://securekey.com/services/trustbloc/; https://github.com/trustbloc
   Open Source platform to build Digital Identity solutions Build and manage verifiable credential solutions, from identity wallets to trusted ecosystems with the TrustBloc technology platform. Based on W3C standards and interoperable with other existing W3C compliant verifiable credential networks.

9. **Evernym's Verity Flow as used in IATA Travel Pass / Lab Pass:** Richard Esplin, Director of Product, Evernym
   URL: https://www.evernym.com/labs/
   Digital COVID-19 test results are vital for safe global air travel. Evernym partnered with the International Air Transport Association and labs around the globe to make issuing these records not only easy but also secure, privacy-preserving, and immediately verifiable.

10. **Ping Identity - Ping Identity and Personal Identity:** David Waite
    URL: https://www.pingidentity.com/en/solutions/personal-identity.html
    Learn more about the vision for where Personal Identity fits into a more traditional IAM product line, and the standards focus for collaboration into the broader decentralized identity ecosystem.

11. **Trinsic - Trust Registries (Completing the Trust Triangle):** Tomislav Markovski
    URL: https://trinsic.id/
    Trinsic allows verifiers to trust not just the verifiable credential, but the issuer. In a permissionless blockchain environment where anyone can issue anything, trust ecosystem providers can close the trust gap through trust registries, domain proofs, and governance-as-code.

12. **NEON - NEON ID:** Gillian Delaunay (Founder and CEO of NEON)
    URL: https://www.neonid.com/; https://www.youtube.com/watch?v=PcxjnoGuXB8
    NEON is a new Internet experience built intentionally for the Identity Ownership Economy. Your NEON ID is home for your online identity where you customize an avatar with your own personality, regain your Internet privacy, and profit directly from advertisers trying to reach you.

13. **Dock.io - Anonymous credentials library:** Lovesh Harchandani
    URL: https://github.com/docknetwork/crypto
    Demonstration of DID operations such as resolving, creating, updating, deactivating, and more, in a DID-method independent way. The library is written in Rust and we show its usage in JS through WASM bindings. We will show its usage with bilinear map accumulator and composite proofs.

14. **VC Schema Generator & Manager:** Kamal Laungani
    URL: https://ui.schema.affinidi.com.
    Creating new VC schemas are hard, usually take a long time, and non-technical people can't do it. Affinidi's Schema Manager gives you the ability to create, host, and manage new VC schemaswithin 2 mins, they're ready to use in your applications right away.

Closing Circle - Zoom Chat Comments

16:05:45 From Mike Ebert to Everyone:
+1 to the Revolution session, it was good
16:07:40 From Mike Ebert to Everyone:
He's probably a distant cousin
16:08:15 From Aaron Goldman to Everyone:
Herd of them
16:08:31 From Andy Morales to Everyone:
“Good luck, and don’t f it up” as RuPaul would say
16:09:36 From Brent Zundel to Everyone:
curves also have different security considerations
16:09:40 From Aaron Goldman to Everyone:
Just use the cure the NSA gave you 😳
16:11:33 From Paul Trevithick1 to Everyone:
who was the presenter about human colossus?
16:11:49 From Bruce Conrad to Everyone:
Robert
16:12:01 From Andrew Hughes1 to Everyone:
Robert Mitwiki
16:12:05 From Paul Trevithick1 to Everyone:
thx
16:14:50 From Andrew Hughes1 to Everyone:
A purpose of identification is to control access.
16:15:07 From Aaron Goldman to Everyone:
ZKP
16:15:07 From Laura Jaurequi to Everyone:
It was amazing!
16:15:12 From Mike Ebert to Everyone:
I will have to read those notes
16:15:15 From Drummond Reed to Everyone:
Link?
16:15:57 From John Wunderlich @PrivacyCDN to Everyone:
https://dwhuseby.medium.com/zero-architecture-is-the-way-forward-5a0080925c76
16:17:24 From David Huseby1 to Everyone:
https://dwhuseby.medium.com/zero-architecture-is-the-way-forward-5a0080925c76?source=friends_link&sk=c6c64d124bbc1361a0bbc24ffa283951
16:17:34 From David Huseby1 to Everyone:
Private friend link for everybody who wants to read it ^^^
16:17:41 From Kent Bull to Everyone:
thanks
16:18:16 From David Huseby1 to Everyone:
Is Bruce calling in a drone strike on my GPS location?
16:18:26 From David Huseby1 to Everyone:
If so, I love you guys. :)
16:18:37 From Mike Ebert to Everyone:
XD
16:18:38 From Andrew Hughes1 to Everyone:
Yes - on the bat phone
16:18:51 From Bruce Conrad to Everyone:
Sorry to disappoint. My ears got tired of the headphones is all

16:19:38 From Nader Helmy to Everyone:
I dropped my summary notes in for that session Doc
16:19:44 From Nader Helmy to Everyone:
Short but sweet
16:19:55 From Marc Davis to Everyone:
Was Doc's session recorded?
16:20:16 From Dounia (Facilitation Team) to Everyone:
Yes!
16:20:22 From Marc Davis to Everyone:
Yay!
16:20:55 From Dounia (Facilitation Team) to Everyone:
Both of Doc's sessions were recorded and are now on the agenda wall to the right of the session notes column
16:22:09 From David Huseby1 to Everyone:
Email @John?
16:22:26 From John Wunderlich @PrivacyCDN to Everyone:
John@wunderlich.ca
16:24:10 From John Court to Everyone:
One paragraph in that Zero Architecture starts to sound like the Infinite Improbability Drive creation chapter from Hitch Hikers :-)
16:27:18 From David Huseby1 to Everyone:
Except it doesn't provide decentralized solutions to 4 of the 9 fundamental problems of decentralization
16:27:29 From David Huseby1 to Everyone:
You have to subscribe to a "super node" to be able to find your friends
16:27:33 From David Huseby1 to Everyone:
Discovery is centralized
16:27:43 From David Huseby1 to Everyone:
scuttlehub.com is a billion dollar opportunity
16:27:53 From David Huseby1 to Everyone:
And you can capture the entire scuttlebutt user base
16:27:55 From Aaron Goldman to Everyone:
Link for 9 fundamental problems of decentralization?
16:27:55 From Charles E. Lehner to Everyone:
David, check the notes for the updates regarding that
16:28:05 From Mike Ebert to Everyone:
I really liked being co-presenter on the DID Login session, so much fun
16:28:31 From David Huseby1 to Everyone: https://medium.com/swlh/a-unified-theory-of-decentralization-151d6f39e38?source=friends_link&sk=b2a71917dcb5ce948196887c7ff48fde
16:28:38 From David Huseby1 to Everyone:
A unified theory of decentralization ^^^
16:29:06 From David Huseby1 to Everyone:
That's about the 9 fundamental problems of decentralization
16:29:06 From Drummond Reed to Everyone:
That's nice!!
16:29:23 From windley to Everyone:
I feel like I've been dropped into an episode of Ants with that background
16:29:35 From Mike Ebert to Everyone:
Yep
16:31:07 From Andrew Hughes1 to Everyone:
@trevethick- that is Robert M
16:32:10 From David Huseby1 to Everyone:

+❤️ Brent Zundell
16:32:16 From Judith Fleenor to Everyone:
Brent I love that background…
16:32:17 From David Huseby1 to Everyone:
I love the Brady Bunch background
16:32:30 From Andrew Hughes1 to Everyone:
Arghhhh another ear worm!
16:32:38 From Drummond Reed to Everyone:
OMG, I've never seen that!!!
16:32:48 From TelegramSam to Everyone:
That's amazing.
16:32:50 From Marc Davis to Everyone:
So Brent is Alice?
16:32:56 From Drummond Reed to Everyone:
Yes!!!
16:32:56 From David Huseby1 to Everyone:
yes
16:32:57 From Andrew Hughes1 to Everyone:
lol
16:33:11 From Drummond Reed to Everyone:
You've all heard of Alice and Bob, right? ;-)
16:33:19 From David Huseby1 to Everyone:
There might not be THE KERI network but there has to be A KERI network
16:33:19 From Mike Ebert to Everyone:
That's the best
16:33:23 From David Huseby1 to Everyone:
That isn't decentralization
16:33:26 From Marc Davis to Everyone:
Ha! Drummond.
16:33:34 From Rouven Heck1 to Everyone:
Oh no - and I missed the first 45min in the call …
16:33:44 From Rouven Heck1 to Everyone:
🙂
16:34:03 From Rouven Heck1 to Everyone:
Maybe that was the missing part to convince me that blockchains don't make sense ;)
16:34:25 From Kaliya Identity Woman to Everyone:
https://docs.google.com/document/d/1xrBPmK3Oc98t8FzJCBMRE57Yl2JygJZds1pmydoHfCk/edit
16:34:43 From Timothy Ruff to Everyone:
@Rouven - Yeah, that's it! Actually blockchains make sense... for cryptocurrency and NFTs. :)
16:35:31 From Mike Ebert to Everyone:
I think there are some other kinds of VC _data_ that makes sense on the blockchain, even if we decide that's not where identity goes.
16:35:37 From David Huseby1 to Everyone:
You don't need blockchains for NFTs
16:35:44 From TelegramSam to Everyone:
Bruce is just phoning it in again.
16:35:46 From David Huseby1 to Everyone:
Just an agreed upon trust anchor and time source
16:35:55 From Drummond Reed to Everyone:
What a phone!!!

16:36:08 From Brent Zundel to Everyone:
love the phone
16:36:17 From Mike Ebert to Everyone:
Again, I have to read your stuff @David Huseby
16:36:21 From Aaron Goldman to Everyone:
David Huseby1 do we need time or just causality
16:36:57 From TelegramSam to Everyone:
Bokeh Kings.
16:37:51 From David Huseby1 to Everyone:
The agreed upon time source has some requirements that aren't obvious (e.g. can't forge future timestamps)
16:38:11 From Eric Weber to Everyone:
Will the next IIW be hybrid?
16:38:13 From David Huseby1 to Everyone:
But the external time frame of reference is needed for total global ordering for the system that uses the time source
16:38:27 From Charles E. Lehner to Everyone:
https://www.w3.org/mid/14e6b577-4991-022e-4bf4-149ffc502b12@digitalbazaar.com
16:38:39 From Kaliya Identity Woman to Everyone:
maybe Phil can touch on what we heard from the community
16:38:58 From Aaron Goldman to Everyone:
David Huseby1 in that case I would use causality and hashes to make the time stamps
16:39:00 From David Huseby1 to Everyone:
I want to see the DID spec die in a fire. Just my opinion obviously
16:39:03 From Drummond Reed to Everyone:
https://www.evernym.com/blog/w3c-vision-of-decentralization/
16:39:14 From Aaron Goldman to Everyone:
E.g hash of latest block
16:39:14 From Drummond Reed to Everyone:
Sorry, Dave
16:39:20 From David Huseby1 to Everyone:
:)
16:39:33 From Brent Zundel to Everyone:
Feedback we got during the DID FO session yesterday has helped tremendously. Thanks all.
16:40:33 From David Huseby1 to Everyone:
We're raising the bar on the amount of knowledge you need to keep up
16:40:52 From David Huseby1 to Everyone:
Especially with the cryptographic techniques
16:41:14 From Brent Zundel to Everyone:
I can't do the multiple sessions thing. It breaks my brain.
16:41:18 From evanwolf to Everyone:
This nearly the definition of the singularity, when the velocity of change exceeds your ability to keep up.
16:41:23 From TelegramSam to Everyone:
Us mere mortals struggle with 2
16:41:28 From Simon Nazarenko to Everyone:
same
16:41:49 From Brent Zundel to Everyone:
heck, I struggle with 1 most of the time
16:41:50 From Andrew Hughes1 to Everyone:
I struggle with sequential sessions 🙂

16:41:58 From Charles E. Lehner to Everyone:
Going to physical will probably winnow it down
16:42:02 From David Huseby1 to Everyone:
I want the DID spec to die as a form of personal absolution. I feel guilty for all of the incorrect contributions I made to that spec. Specifically the idea of selective disclosure.
16:42:13 From David Huseby1 to Everyone:
That doesn't preserve privacy under any circumstances
16:42:40 From Judith Fleenor to Everyone:
There needs to be a nap room for the hybrid IIW 😀
16:42:55 From evanwolf to Everyone:
@Charles, same-place kills some of the diversity.
16:42:57 From Ariel Gentile to Everyone:
+1 John
16:43:21 From Drummond Reed to Everyone:
+1 to the nap room. I did take one of them during one of the "hour breaks". It was perfect!
16:43:40 From Simon Nazarenko to Everyone:
I am from outside and it is hard to follow through
16:43:43 From TelegramSam to Everyone:
Drummond took two naps at the same time.
16:43:50 From Drummond Reed to Everyone:
LOL!!!
16:43:52 From Mike Ebert to Everyone:
Yeah, it's quite the learning curve.
16:43:59 From John Wunderlich @PrivacyCDN to Everyone:
One of the advantages of in-person is exactly that it takes me away from 'the office' so I can focus on IIW and leave the other stuff behind.
16:44:07 From Judith Fleenor to Everyone:
@sam LOL!
16:44:16 From Brent Zundel to Everyone:
+1 John
16:44:19 From James Ebert to Everyone:
+1 to John ^^^
16:44:20 From TelegramSam to Everyone:
Just tell people you are traveling to it, then don't.
16:44:27 From Mike Ebert to Everyone:
LOL @Sam
16:44:31 From evanwolf to Everyone:
just Newbie Tracks in your first IIW. Walk the Decentralized Body of Knowledge.
16:44:39 From Drummond Reed to Everyone:
So I'm going to take ask the question: is the next IIW going to be in person?
16:44:42 From John Court to Everyone:
No-one bothers me from 12am-6am so its fine
16:44:57 From TelegramSam to Everyone:
Drummond want's prophesy.
16:45:09 From Drummond Reed to Everyone:
Yes, prophesy!!
16:45:22 From John Phillips - Sezoo to Everyone:
+1 John C
16:46:16 From Alan Karp to Everyone:
I thought that Zoom would never work.
16:46:19 From Rouven Heck1 to Everyone:

Instead of hybrid - maybe iterating onside vs. remote?
16:46:39 From Mike Ebert to Everyone:
Online in the winter and in person in the summer?
16:46:52 From Drummond Reed to Everyone:
Yes, I'm leaning towards that
16:47:03 From John Phillips - Sezoo to Everyone:
Think Global Mike - not everyone's summer is everyone's summer...
16:47:07 From Vic Cooper to Everyone:
+1 split virtual and in person
16:47:07 From Brent Zundel to Everyone:
two words: telepresence robots
16:47:09 From dsearls to Everyone:
Phil's lava lamp looks lame. Maybe a brighter bulb?
16:47:21 From Mike Ebert to Everyone:
But if it's in person, as long as the conference location has summer, it's good, right?
16:47:24 From Bruce Conrad to Everyone:
Phil was heard saying "I wish people would stop using the word 'identity'". So are we now in I⃠W? Or, I took it out of context…
16:47:25 From Enddy Dumbrique to Everyone:
Yes diversity is key.
16:47:33 From evanwolf to Everyone:
+1 Marc.
16:47:47 From John Wunderlich @PrivacyCDN to Everyone:
+1 Marc Alternating In-Person and Virtual
16:47:58 From Kent Bull to Everyone:
Maybe remote format for short events, in person for longer events.
16:48:04 From camparra to Everyone:
Please do in person… some of these sessions turn to lectures and don't carry the spirit of IIW of collaboration.
16:48:27 From TelegramSam to Everyone:
I wonder if we can adapt the conference in virtual form to make the days easier.
16:48:40 From Timothy Ruff to Everyone:
Maybe alternate spring and fall, in person, remote
16:48:50 From Ariel Gentile to Everyone:
+1 Tim
16:48:56 From TelegramSam to Everyone:
Another vote for alternating.
16:49:01 From Marc Davis to Everyone:
+1 TimothyRuff
16:49:05 From Vic Cooper to Everyone:
I'm picking up my grandkids so I'm not able to fully participate in the closing. But I am listening as much as possible. Thanks everyone for a great IIW!
16:49:22 From Drummond Reed to Everyone:
Thanks Vic!!
16:49:24 From camparra to Everyone:
Maybe but in person IIW was so much more easier to discuss things
16:49:42 From Mike Ebert to Everyone:
Cute Vic!
16:49:43 From Drummond Reed to Everyone:
I agree with Heidi. And with Marc. I'd go for alternating in-person and virtual.
16:49:45 From TelegramSam to Everyone:
Both forms have huge merits.

16:50:07 From Judith Fleenor to Everyone:
+1 Heidi I agree regarding openspace not suited for hybrid well.
16:50:17 From windley to Everyone:
How does Vic have grandkids? I thought he was 35. Maybe it's just the camera
16:50:42 From Marc Davis to Everyone:
Agree with Heidi: Hybrid does not (currently) work. Strongly advocate that if you want in person, alternate fully in person and and fully remote IIWs.
16:50:43 From Laura Jaurequi to Everyone:
Agreed!
16:50:45 From Brent Zundel to Everyone:
+1000
16:50:47 From Brian Richter to Everyone:
+1
16:50:53 From Drummond Reed to Everyone:
+1
16:51:57 From Brent Zundel to Everyone:
thanks Drummond
16:51:59 From Andrew Hughes1 to Everyone:
All Seasons!
16:52:06 From Brian Richter to Everyone:
I'm not American but I'd still vote for Brent!
16:52:20 From Charles E. Lehner to Everyone:
+1
16:52:34 From Heidi (facilitation team) to Everyone:
Hi Gus!
16:53:10 From Dounia (Facilitation Team) to Everyone:
Hi Gus!! 🐕
16:53:20 From Drummond Reed to Everyone:
Sam's the man!!
16:53:31 From SamSmith to Everyone:
Thankyou Adrian+
16:54:53 From Marc Davis to Everyone:
Yay Sam!
16:55:16 From Drummond Reed to Everyone:
Brent for President!!
16:55:20 From Brent Zundel to Everyone:
you guys are making may day, thank you!
16:55:32 From dsearls to Everyone:
Mark is in Canada now. Just saying.
16:55:56 From dsearls to Everyone:
I bow to our Canadian overlords.
16:56:03 From Marc Davis to Everyone:
Lol!
16:56:06 From evanwolf to Everyone:
🍁
16:56:28 From John Phillips - Sezoo to Everyone:
I wouldn't have thanked him if I'd known he was Canadian! (kidding)
16:58:27 From Trent Larson to Everyone:
Plus, Phil is a beautiful shade of orange today.
16:58:43 From Kent Bull to Everyone:
XD

16:58:45 From Timothy Ruff to Everyone:

16:59:08 From Kyle Den Hartog to Everyone:

16:59:13 From Mike Ebert to Everyone:

17:00:01 From windley to Everyone:
Better Trent?
17:00:04 From Mike Ebert to Everyone:
Thanks Bruce!
17:00:14 From Mike Ebert to Everyone:
Means a lot!
17:00:58 From Stephen Curran to Everyone:
+1 Drummond — great work Phil and Kevin!
17:00:59 From Trent Larson to Everyone:
Ha! Actually, yes, Phil… you look more healthy now.
17:01:08 From Philip Feairheller2 to Everyone:
Thank you very much Drummond!!
17:01:30 From windley to Everyone:
The default auto white balance on this camera is not great.
17:01:45 From Drummond Reed to Everyone:
Phil and Kevin: richly deserved
17:02:15 From Adrian Gropper to Everyone:
Next IIW dates
17:02:19 From Adrian Gropper to Everyone:
?
17:02:23 From Charles Lanahan to Everyone:
thanks everyone
17:02:24 From Paul Trevithick1 to Everyone:
And thank you Kaliya!
17:02:26 From Judith Fleenor to Everyone:
Go Giants!
17:02:28 From Brian Richter to Everyone:
Thanks all, see ya next time!
17:02:28 From Timothy Ruff to Everyone:
Great job everyone!
17:02:35 From Adrian Gropper to Everyone:
April 26-28
17:02:40 From dsearls to Everyone:
I like how Lisa's dog goes in and out of focus.
17:02:47 From Stephen Curran to Everyone:
Awesome job — thanks all — great stuff!
17:03:18 From Neil Bourgeois to Everyone:
Thank you - everyone! This was amazing.
17:03:20 From dsearls to Everyone:
Great job, team.
17:03:22 From Robert to Everyone:
Thanks a lot everyone was great time!
17:03:23 From Judith Fleenor to Everyone:
Lisa is the a Dog on the internet?
17:03:27 From Mike Ebert to Everyone:

So good!
17:03:28 From Marc Davis to Everyone:
Thank you Kaliya, Phil, Doc, Heidi, Lisa, and Dounia for an amazing IIW!
17:03:58 From Mike Ebert to Everyone:
+1000
17:04:07 From evanwolf to Everyone:
Perhaps Miro next time. Post-its!
17:04:12 From Gillian Delaunay to Everyone:
This was AWESOME. THANK YOU!!!!
17:04:21 From Charles E. Lehner to Everyone:
Cheers!
17:04:25 From Dan Yamamoto to Everyone:
Thank you everyone, this is really special opportunity
17:04:28 From Joyce Searls to Everyone:
Thanks, everyone. It keeps getting better.
17:04:29 From Trev Harmon to Everyone:
Thanks everyone
17:04:29 From John Phillips - Sezoo to Everyone:
Thanks all - till next time.
17:04:36 From Kent Bull to Everyone:
This was a wonderful first IIW. Thanks to all the presenters!
17:04:36 From Peter Langenkamp to Everyone:
Thanks everyone, bye!
17:04:38 From Brent Zundel to Everyone:
I'm gonna take my kids (and myself) out for pizza. You are all fantastic.
17:04:41 From Drummond Reed to Everyone:
Thanks all!!!!!!!!
17:05:03 From Wip to Everyone:
Thanks everyone! I would love to make it to an in person if I can
17:05:07 From Marc Davis to Everyone:
I personally hope the next IIW is remote too :-). Thank you all!

Stay Connected with the Community Over Time - Blog Posts from Community Members

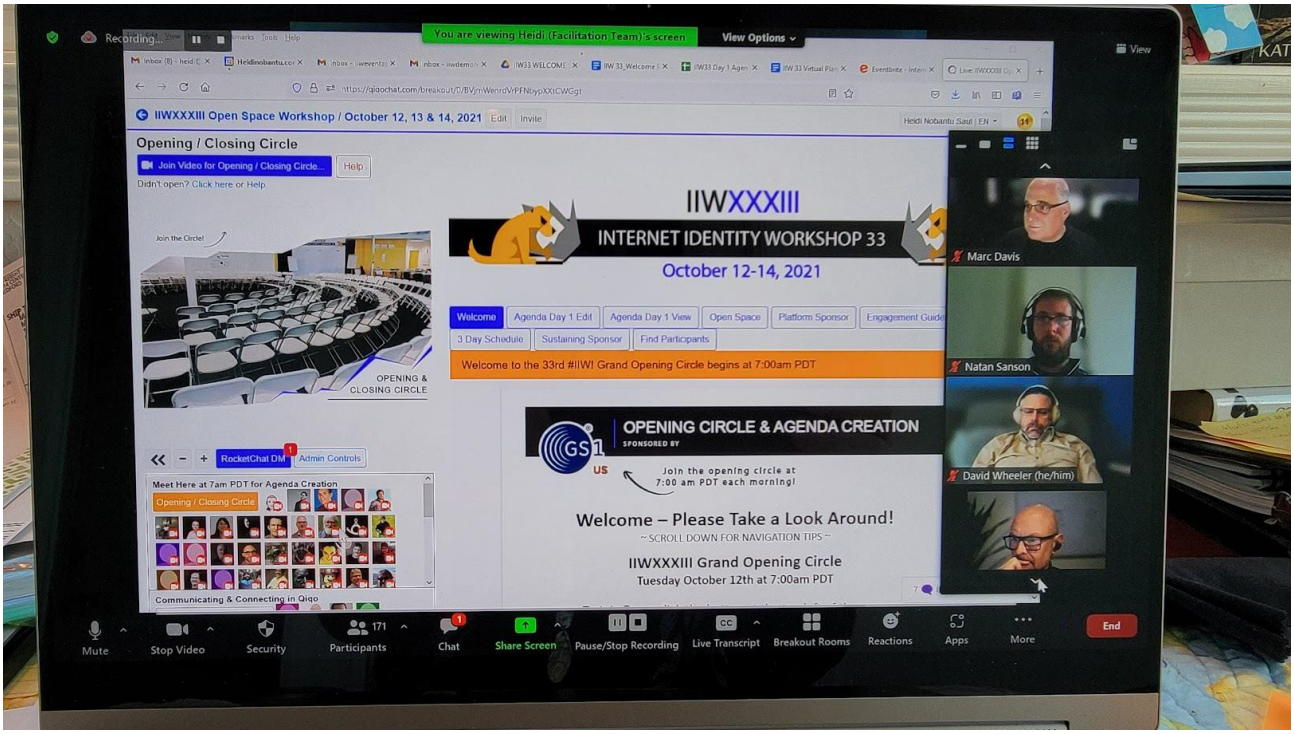
New Community Resource
Each week Kaliya, Identity Woman and Informiner publish a round of the week's news from the industry. It is called **Identosphere - Sovereign Identity Updates (weekly newsletter)**
You can find it here: https://newsletter.identosphere.net/

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/



Hope to See you April 26, 27 and 28, 2022

for

IIWXXXIV

The 34th Internet Identity Workshop
We'll be In Person at the Computer History Museum

REGISTER HERE

www.InternetIdentityWorkshop.com