IIWXXXVIII

INTERNET IDENTITY WORKSHOP 38

April 16-18, 2024

Book of Proceedings

www.internetidentityworkshop.com

Computer History Museum / Mountain View CA

Bjorn @blhjelm · Apr 16

It's baaaaaack! @idworkshop is now live.

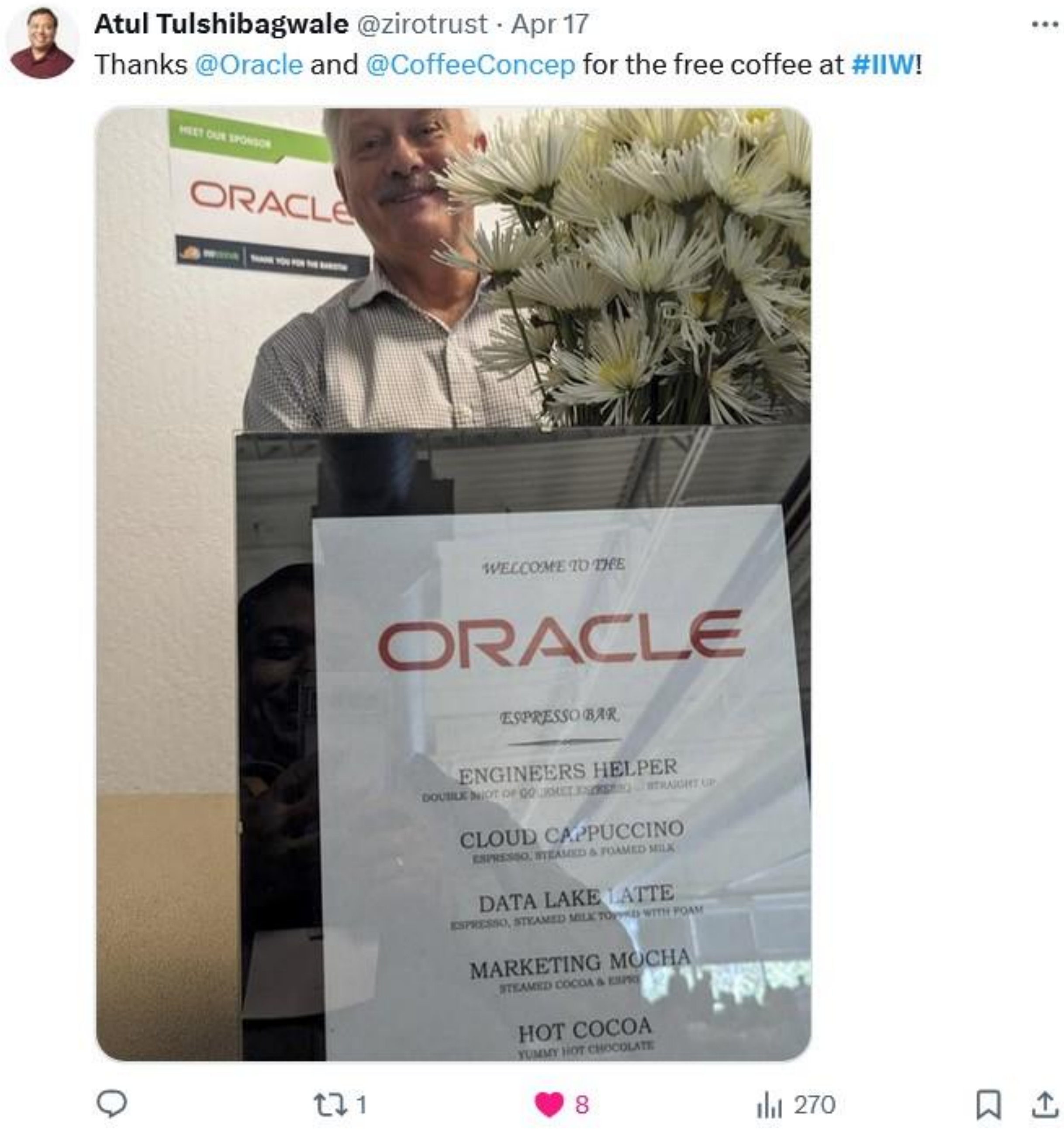
Notes Wrangled, Collected & Compiled by
HEIDI N. SAUL & EMMA WINDLEY

IIW founded by Kaliya Young, Phil Windley and Doc Searls
Co-produced by Heidi Nobantu Saul, Phil Windley and Kimberly Culclager-Wheat
Facilitated by Heidi Nobantu Saul & Kaliya Young

IIWXXXIX In Person in Mountain View, CA
October 29 - 31, 2024

Thank You! Documentation Center & Book of Proceedings Sponsors: Curity * polygonID and an Anonymous Sponsor

Contents



Atul Tulshibagwale @zirotrust · Apr 17

Thanks @Oracle and @CoffeeConcep for the free coffee at #IIW!

About IIW

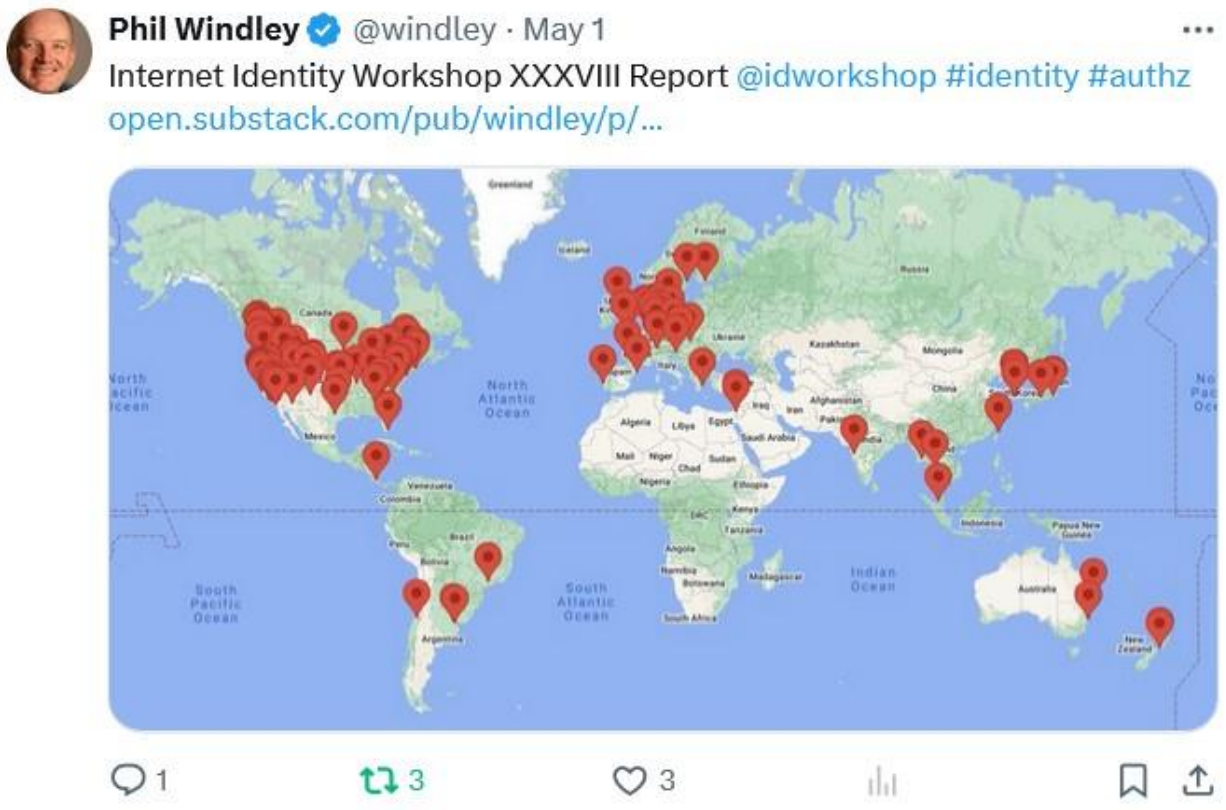
The Internet Identity Workshop (IIW) was founded in the fall of 2005 by Phil Windley, Doc Searls and Kaliya Young. It has been a leading space of innovation and collaboration amongst the diverse community working on user-centric identity.

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 19th year and is Co-produced by Phil Windley, Heidi Nobantu Saul and Kaliya Young. IIWXXXIx (#39) will be October 29 - 31, 2024.



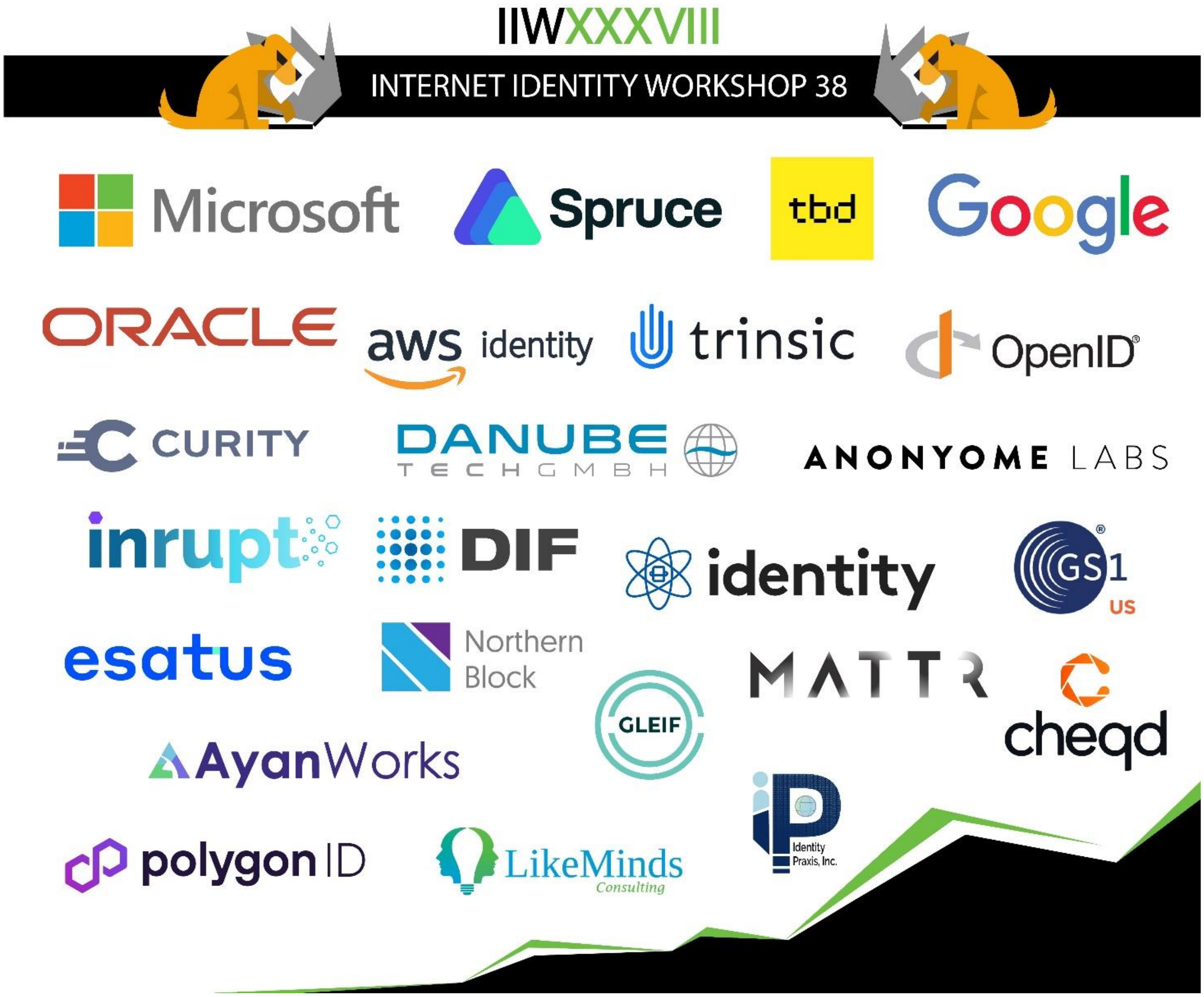
Phil Windley @windley · May 1

Internet Identity Workshop XXXVIII Report @idworkshop #identity #authz open.substack.com/pub/windley/p/...

https://www.windley.com/archives/2024/04/internet_identity_workshop_xxxviii_report.shtml

#IIW is powered by #openspacetech and the magic #selforganizing and has been since 2007!

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 #39
October 29 - 31, 2024
In Person in Mountainview, CA
https://internetidentityworkshop.com/

IIWXXXVIII 3 Day Schedule

TUESDAY, April 16 / Doors Open at 8:00

Doors Open at 8:00 AM for Registration

Barista! - Bagels (PB&J, Cream Cheese) - Yogurt - Krispy Kreme Donuts - Fruit - String Cheese etc.

Barista! And Continental Breakfast	8:00 - 9:00	Lunch	1:00 - 2:00
Welcome Introduction	9:00 -10:00	Session 3	2:00 - 3:00
Opening Circle / Agenda Creation	10:00 - 11:00	Session 4	3:00 - 4:00
Session 1	11:00 - 12:00	Session 5	4:00 - 5:00
Session 2	12:00 - 1:00	Closing Circle	5:00 - 5:45

Welcome Reception & Dinner 6:00

Off the Rails Brewery 111 S Murphy Avenue Sunnyvale, CA 94086 (408) 773-9500

WEDNESDAY, April 17 / Doors Open at 8:00

Barista! - Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme Donuts - Fruit - String Cheese etc.

IIW Women's Breakfast Roundtable's	**7:45 - 9:00**	Lunch	12:30 - 1:30
Opening Circle / Agenda Creation (SHARP)	8:45 - 9:30	Speed Demo Hour	1:30 - 2:30
Session 1	9:30 - 10:30	Session 4	2:30 - 3:30
Session 2	10:30 - 11:30	Session 5	3:30 - 4:30
Session 3	11:30 - 12:30	Closing Circle	4:30 - 5:30

Conference Reception & Dinner

Cuban Kitchen (w/plenty of V&V options) - Here at CHM!

<table>
<tr><td colspan="4"><b>THURSDAY, April 18 / Doors Open at 8:00</b>
Barista! - Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme Donuts - Fruit - String Cheese etc.</td></tr>
<tr><td>Opening Circle / Agenda Creation (SHARP)</td><td>8:45 - 9:30</td><td>Session 4/Working Lunch</td><td>12:30 - 2:00</td></tr>
<tr><td>Session 1</td><td>9:30 -10:30</td><td>Session 5</td><td>2:00 - 3:00</td></tr>
<tr><td>Session 2</td><td>10:30 - 11:30</td><td>Closing Circle</td><td>3:00 - 4:00</td></tr>
<tr><td>Session 3</td><td>11:30 - 12:30</td><td colspan="2"><b>IIWXXXIX October 29 - 31, 2024</b></td></tr>
<tr><td colspan="4"><b>Drinks/Dinner 5’ish No Host @ Das Bierhauz 135 Castro Mountain View</b>
https://dasbierhauz.com/</td></tr>
</table>

IIW38 Agenda Creation = Schedule & Workshop Sessions

Phil Komarny @PhilKomarny · Apr 18

What does the day 3 agenda of #IIW 38 hold?

The community decides

Circle time!!

168 distinct sessions were called and held over 3 Days.

We received notes, slide decks, links to presentations and photos of whiteboard work for 144 of these sessions.

Tuesday April 18, 2023 ~ Day 1

Session 1

1A/Open ID4VC - 101 / Joseph Heenan & Kristina
1B/ NO SESSION
1C/ Content Authenticity 101 / Eric Scouten
1D/ VOCABULARY - What does all of this mean? / Michael K.
1E/ AI Authorization on Human's Behalf / Colby Anderson
1F/ Personal AI / Reza Rassool
1G/ The Hitchhiker's Guide To KERI / Nuttawut Kongsuwan
1H/ NO SESSION
1I/ Digital Credentials Consortium Updates / Dmitri Zagidulin
1J/ NO SESSION
1K/ NO SESSION
1L/ NO SESSION
1M/ DIDComm 101 Introduction to DIDComm & secure bi-directional communications / Colton / Wolkins
1N/ NO SESSION

Session 2

2A/ Identity and The Open Social WEB in 2024 - Best Practices Today / Johannes Ernst
2B/ Intro to OpenID Connect - an IIW 101 Session / Mike Jones

2C/ Landing the Commons / Day Waterbury and Friends
2D/ NO SESSION
2E/ SSI for Democracy / Pam Dingle, Britt Blazer, Britt made up space Z -
2F/ Should Proof of Humanity Apply to My Personal AI? / Adrian Gropper
2G/ ISO MDOC 101 (AMA = ask me anything) - Oliver Terbu
2H/ Trust OveIP (ToIP) Foundation / Judith Fleenor
2I/ DIF for DEVS - Labs Working Group Coming!! / Andre & Kim
2J/ Agentic Collective Identity / Travis Well
2K/ NO SESSION
2L/ NEW!! The Last DID Method = Trust DID Web DID: TDW / Stephen Curran
2M/ Organizational Identity & Verifiable Authority / Timothy Ruff
2N/ NO SESSION

Session 3
3A/ EBA Pilot Using the vLEI / Karla McKenna & Lance Byrd
3B/ Authorization 101 - Intro to authorization concepts - An IIW 101 Session / Steve Venema
3C/ PDF - What to do about them? / no name
3D/ NO SESSION
3E/ Syper Persuasive Bots (NOT) Without using pseudonymity / no name
3F/ SD - JWT (SD-JWTVC & SD-JWT VCDM) / Kristina Yasuda & Oliver
3G/ *POKE HOLES * In out knowledge based authentication method. / Matthew Vogel
3H/ Where Am I? How did I get here? - Human OS / Jeff Orgle
3I/ Local First / SSI Fediverse UpDates Notes from the Field / Dmitri Zagidulin
3J/ NO SESSION
3K/ NO SESSION
3L/ Simple SSI - How to make the SSI Codebase attractive for devs to use? / Juna Than Rayback
3M/ Authenticity in a ML World / Matt Miller
3N/ The DEI Backlash & the Identity Profession / Heather Flanagan

Session 4
4A/ WIGG Digital Credentials API / Lee Campbell, Sam Curren & Tim
4B/ FIDO 101 and Passkeys - an IIW 101 Session / John Bradley
4C/ OpenID AuthZEN: (zero) to interop in 6 Months! / Omri Gazitt
4D/ Latest Research in Metastable Networks - How did we get the web but NOT the web of trust? / Dave Huseby
4E/ Privacy Enhancing Mobile Credentials- an update / John @privacyCPN
4F/ NO SESSION
4G/ OpenIDID Comm - Using them both Spec + Demo by ID Union / Sam Curren
4H/ An Intro To …. Self-Sovereign Identity (SSI) An IIW 101 Session / Limari Navarette & Steve McCowen
4I/ Decentralized Storage & Bring Your Own Identity / Aaron Coburn
4J/ Empowerment Tech - the good, bad, ugly / James Monaghan
4K/ Public Verifiable Data for Websites, People, and organizations DIF LInked-up / JC and Brian
4L/ The Business of SSI & Authentic Data / Timothy Ruff

4M/ I'll be presenting a governance model that combines life cycle perspective and ToIP stack model / Ismael Avila
4N/ Unique Media ID to Fight Disinformation / Todd Carpenter

Session 5
5A/ SSI didn't work, we are Pivoting! Ask me anything / Riley Hughes
5B/ Zero Trust with Zero Data (Verifiable Credentials) / Phil Windley
5C/ Open Wallet Foundation Overview / Sean Bohan
5D/ What is required to trust A.I. with your Personal ID? Marc Aurele Besner
5E/ Functional Privacy / Joe Andrieu
5F/ Status/Revocation Mechanisms Comparison / Paul Bastian & Mollik (?)
5G/ NO SESSION
5H/ Verifiable Presentation as a Signature / Dan Yamamoto
5I/ NO SESSION
5J/ Protocols for a Return to Animist WorldView and Reindigination / Day Waterbury and Friends
5K/ State of Adoption - bring a real-world use case / James Monaghan
5L/ OID4VCI Event Signaling / Oliver Terbu
5M/ TSP draft Pat I / Wenjing Chu
5N/ W3C Federated Identity WG +Digital Credentials / Heather Flanagan

Wednesday April 19, 2023 ~ Day 2

Session 6
6A/ Cross Platform Demo of Digital Credential API / Eric M, Helen, Andreas, Lee
6B/ KERI for Dummies / Timothe Ruff. Phil Fearheller
6C Content Authenticity 201: Identity Assertion Technical Working Group / Eric Scouten
6D/ Open Source HERESY Functional Source LIcense and Other Approaches to Designing for Sustainability
6E/ Defend Against ENSHITTIFIACATION - Brainstorm: How can we build safeguards (governance) against the hostile spiral of anti-individual extraction?
6F/ NO SESSION
6G/ Identity Dynamics 0 to 1 - Born w/out to Born w/in Human OS/ Jeff O
6H/ Digital Identity Landscape (World Bank) / Christian Gray
6I/ NOSTR / Max
6J/ The State/Role of Academic Research in Identity - open discussion / Evan
6K/ NO SESSION
6L/Healthcare - Data, SSI, ID, Etc.. / Leah Houston HPEC
6M/ DDID ecosystem development - Two Years of Lessons Learned / Ismael Avila
6N/ NO SESSION

Session 7
7A/ Open ID 4 VP + OpenID4VP over Browser API / Joseph, Kristina Y, Torsten L
7B/ Characteristics of a healthy identity ecosystem? / Justin & John
7C/ Report Our + Winners Demo = DIF Hackathons / Limari @DIF, Ken Watanabe from WasedaU
7D/ How Might we… Normalizing Wallet Interactions - Open Discussion / Matt Miller
7E/ Autonomous Identity - Digital Identity for Humans AND AI / Jeremy Frank
7F/ The "LAWS" of Externalized Authorization / Omri Gazitt
7G/ DID:DHT 6mo later - Decentralized without a Blockchain / Gabe
7H/ Identity of Media - Channels & Brands +PART II+ Olaf & Todd

7I/ Trust Registry FACE OFF!! / Andor K, Mathieu Glaude, Sam Curren
7J/ NO SESSION
7K/ NO SESSION
7L/ MOSIP - Modular Open Source Platform - An Exploration & Report from Their Connect Conference / Kaliya Young
7M/ The 5 Rights of Secure Health Data = a Proof of Concept - KERI-ACDC/ Jared J and Phil F
7N/ NO SESSION

Session 8
8A/ Discussion on USER/HOLDER BINDING Mechanisms & Proposal for CLAIM BASED BINDING / Paul Bastian
8B/ GNAP with a focus on Personal AI and Large Language Models / Justin Ritcher & Adrian Gropper
8C/ SSI?VCs Not Dead (yet) : Hot takes and lessons learned from assi/VCs Consulting / Lucy Yang & Kaliya Young
8D/ Improving Service Discovery over DID Documents with Service Profiles / Andor Kesselman
8E/ NO SESSION
8F/ OIDC vs VC Delivering OIDC use cases with VC's? / Gina Biernacki & Dirk Belfanz
8G/ ABAC vs ReBAC Smack-down! / Omri Gazitt
8H/ Identity of Media Channels & Brands Part III / Olaf Steenfadt & Todd Carpenter
8I/ Decentralized Web Nodes (DWN) / Daniel Buchner & Liran Cohen
8J/ STORY and Decentralized Identity / Erica Connell
8K/ Building the Regen CoLab Stack / Day Waterbury and Friends
8L/ Did:tdw DID Resolution: open questions and remaining work / Andrew Whitehead, Stephen Curran
8M/ TSP Part II / Wenjing Chu
8N/ Split Key ECDSA and A??G for Wallet Proof of Possession / Holder Binding / John Bradley

Session 9
9A/ Privacy With Accountability: Towards an abstraction enabling mixing and matching VC formats and zero knowledge proof libraries / Mark Moir
9B/ Global Interoperability of Digital Identity Infrastructure with OECD, WorldBank, UN, 22+ Countries + 25 standards bodies + non-profits. Learn & Help! / Elizabeth Garber, Gail Hodges, Kim Duffy, Judith Fleenor
9C/ DID Linked Resources - Solving hard real world problems… / Tasos D & Alex Tweedale
9D/ AOE Verification (everything) / Iain Corby
9E/ Decentralized AI Ecosystem - What does it look like? How to make $$'s / Cam Geer
9F/ Governance of Digital Trust Ecosystems / Scott Perry
9G/ What is BBSignature? 101 NO Math / Kazue Sako
9H/ Roast my revocation approach! / Mirko Mollik
9I/ EMBODIMENT and our identity - What would digital embodiment look like? / Bruce Conrad
9J/ NO SESSION
9K/ I Built a Crypto / Blockchain from Scratch That's Listed on Coin Market CAP. AMA Session/ Matt Vogel
9L/ ACR - AMR IYKYK / Pam Dingle & Dale Olds
9M/ HI-Assurance DID:WEB Using DNS / Marrieu Glaude
9N/ 2024 Election - How to best use identity tools to help overlooked communities share underrepresented lived experiences before the Presidential Election. / Blake Stoner

Session 10

10A/ Self-Sovereign Personal AI / Doc Searls
10B/ CESR 2.0 Performance features - Deep dive annotation - Comparison to JSON CBOR and more / Sam Smith
10C/ Navigating the Credential MAZE with DIF! / Kim Duffy & Otto Mora
10D/ FedCM for beginners / Aaron Coburn
10E/ Identity Delegation - A Useful Pattern / Kai Peacock
10F/ DID-Powered Trust Chains for EIDAS2.0 / Alex Tweedale
lG/ Lock-In Lock-Out What grinds your gears? Workshop to gather concerns / Robert Lopes
10H/ Open Wallet Foundation Credential Profile Comparison + Wallet and Agent Overview / Mirko Mollick & Samuel
10I/ DHS-OBIM Bringing it all together ; People, Tech, Policy, Gov't + Business / Troy ?
10J/ Credence ID - Comprehensive digital ID Verification Solution / Navya Kumar & Yash Shah
10K/ NO SESSION
10L/ Venture Capital - I'm a VC investor - Why am I here? - How do Investors think about this? What do VS's do / Mark McGo
10M /Test - Suite Testing Implementation across frameworks / Patrick St-Louis
10N/ Credentialsfor Human + Non-Human Use Cases = Possible? (IETF SPICE) / Heather Flanagan

Thursday April 20, 2023 - Day 3

Session 11
11A/ OID4VP - Suggestions for query syntax (P.E.) Simplification / Tobias L + Kristina Yasuda, Oliver Terbu
11B/ Content Authenticity Identity User Experience / Eric Scouten & Pia Blumenthal
11C/ Deploying Multi Tenant Secure Witnesses for KERI / Phil Feairheller
11D/ NO SESSION
11E/ Proof of Personhood - UX Dichotomy + Continuous Control (brainstorm) / Colby Anderson
11F/ PASSKEYS A.M.A. / Matt Miller & Tim Capelli
11G/ Survey of Cloud, On-prem, Hybrid, etc. BRAINSTORMING / Jonathan Rayback & James Monaghan
11H/ Let's Destroy the World!!! A hostile thought experiment / Kai Peacock
11I/ Talk Workshopping = How good should Institutional Memory be? Reframing (Digital) Identity Systems as Institutional Memory / Kaliya Young
11J/ NO SESSION
11K/ NO SESSION
11L/ AnonCreds in W3C VCDM Format / Stephen Curran wBC Gov
11M/ What's Wrong with My Wallet?? A consumer's point of view / Susan Stroud
11N/ The MIssing Link…. "Humans" In the Quest of Identity! Why are we doing an of this, for who? / Ken Gantt
Session 12
12A/ A Bridge to the Future: Connecting XSo9 and DIDs/VIDs / Eric , Drummond Reed, Wenjing Chu , Scott Perry , Steven Chen
12B/ Verifiable Ownership of Permissioned Data / Nara Lau and Troy
12C/ TSP Draft Part III Implementation / Wenjing Chu
12D/ NET WORK cooperative - self-owning + governing social graph / Brad DeGraf
12E/ NO SESSION
12F/ Identity - Related Fraud / Fincen / Cam Geer
12G/ The Coming Wave of Perfectly Personalized Pricing!!! How lack of privacy means you will never get another DEAL! BrainStorm / Joyce Searls
12H/ Dazzle Office Hours: FediTest: testing distributed, heterogeneous systems w/complex protocols (Fediverse) / Johannes Ernst

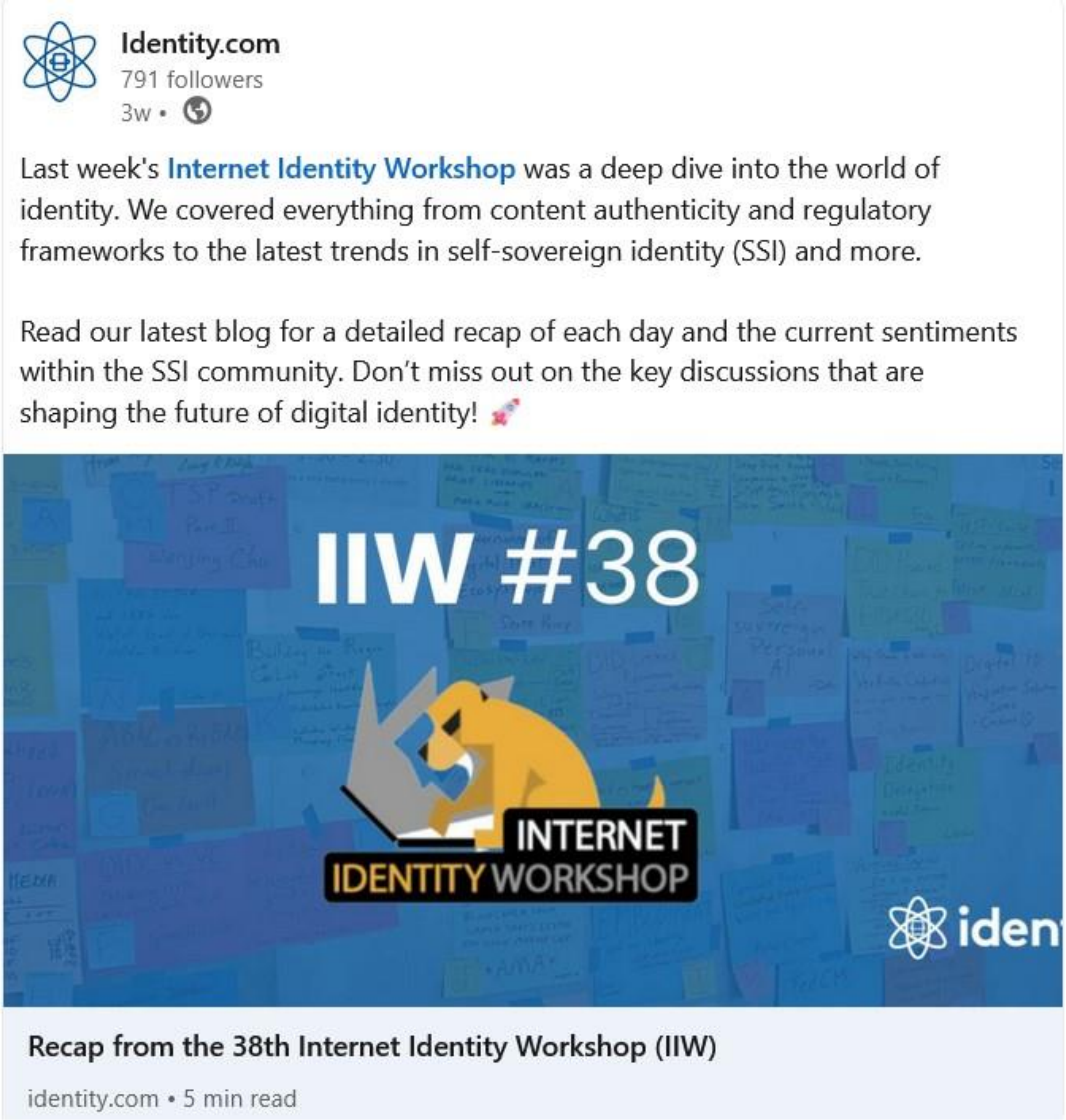
12I/ How to design/implement OpenID4VC Profiles / Kristina Yasuda, Joseph, Sten
12J/ NO SESSION
12K/ NO SESSION
12L/ Running Lean w/SSI The business model to go from Idea to Company / Jared J & Timothy Ruff
12M/ Identity v. Anonymity: How to best interconnect both to expand discussion on issues across countries? America's November Election / Blake Stoner
12N/ AuthZ Conf. Planning Call - Who & How to Convene a comm? / Rohit Khare

Session 13
13A/ Advanced Topics for OpenID4VCI / Paul , Kristina Yasuda
13B/ Trust Establishment with OpenID Federation / Mike Jones, John Bradley
13C/ DID or not? The Value of an Identifier Metasystem is EIDAS wrong? / Sam Curren
13D/ Provenance from First Principles Part 1 / Dave Grantham
13E/ NO SESSION
13F/ Identity Dynamic Modalities 0 to 1 / Jeff Orgle
13G/ Access / Auth 2 Assurance NIST 800-63D? / Robert Lapes
13H/ Accountable Wallets / A wallet can prove a wallet's legitimacy using VC and ZKP / Masato Yamanaka
13I/ Personal Datastore Face OFF!!! / Andor Kesselman, Aaron Coburn
13J/ NO SESSION
13K/ Five Failed Blockchains - Why Trade Needs Protocols, Not Platforms / Timothy Ruff
13L/ Multifactor Fusion in a VC / Francisco Corella
13M/ Tokens, Tokens Everywhere / George Fletcher
13N/ Authentic AI ToIP Aim Task Force / Wenjing Chu

Session 14
14A/ DBSC API Cookie Theft / Sam Goto & Anmom Bingislom
14B/ Cardano Transactions and Keri / Can a cardano Tx be affected based on AID's current keys? / Ed Eykholt
14C/ NO SESSION
14D/ Provenance From First Principles Part 2 / Dave Grantham
14E/ NO SESSION
14F/ Design the Patient Journey / Adrian Gropper
14G/ VC with BBS+ and 2K-SNARK for predicate proofs / Dan Yamaoto
14H/ Talk Workshopping - Biometrics & Communication: Identity Implications / Kaliya Young
14I/ WIDER WELCOME to the World Wise Web / Dan Waterbury and friends
14J/ NO SESSION
14K/ NO SESSION
14L/ State of eIDAS + German eIDAS Wallet Consultation Project + Wallet Challenge / Paul , Torsten Lodderstedt, Kristina Yasuda
14M/ vLEI (verified Legal Entity Identifier) Demystified / Nuttawut Kongsuwan
14N/ NO SESSION

Session 15
15A/ Wallet Attestation + OAuthZ Attestation-based Client Authentication. IETF Draft / Paul E & Tobias L
15B/ I don't sign my credentials and neither should you! Why unbound signatures (tokens) are insecure and how to use KERI instead. KERI for Enterprise / Sam Smith
15C/ No more plaque buildup! Learning & Employment Records (LEAR's) Governance & User Adoption / Mahesh Balan

15D/ The “Official” Riley Session = What hasn’t worked? / Dave Grantham
15E/ NO SESSION
15F/ Favorite & Hated Standardization Process Myths & Legends / Tim & Heather Flanagan
15G/ Bitstring for Privacy: Randomization Why and How / Kevin Dean
15H/ NO SESSION
15I/ NO SESSION
15J/ NO SESSION
15K/ NO SESSION
15L/ Decentralized Apps 1/Solid & PICOS / Phil Windley & Bruce Conrad
15M/ Digital Identity - What, Who, How, and When does this come together for people, customers, humans? I want to hear from you! Ken the ID Guy
15N/ The 4 Parts of Access Control: Where and When / Alan Karp



Identity.com
791 followers
3w •

Last week's Internet Identity Workshop was a deep dive into the world of identity. We covered everything from content authenticity and regulatory frameworks to the latest trends in self-sovereign identity (SSI) and more.

Read our latest blog for a detailed recap of each day and the current sentiments within the SSI community. Don’t miss out on the key discussions that are shaping the future of digital identity! 🚀

Recap from the 38th Internet Identity Workshop (IIW)

identity.com • 5 min read

Notes Day 1 / Tuesday April 16 / Sessions 1 - 5

SESSION #1

OpenID4VC 101

Session Convener: Joseph / Kristina
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

OpenID for Verifiable Credentials, OpenID4VCI

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

Slides used are here:
https://drive.google.com/file/d/1k3HHoBm0MJfRtHJHF4XwlRhvwU9YzVkQ/view?usp=sharing

Content Authenticity 101

Session Convener: Eric Scouten, Adobe
Session Notes Taker(s): Jin Wen

Tags / links to resources / technology discussed, related to this session:
https://ericscouten.dev/2024/content-authenticity-101/

Content Authenticity Initiative, Coalition for Content Provenance and Authenticity (C2PA)
CAI, C2PA

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

======= START HUMAN ON-SITE NOTE TAKING =====================================
Motivational example: the famous fake photo of the pope in the white puffer coat.

Content Authenticity non-goals

- fact-checking
- fake image detection
- politically opinionated

Major participants of CAI:

- BBC, Reuter
- Adobe, Microsoft, Google
- Nikon, Leica, Sony
- ARM, Qualcomm

Demo: How it works in Photoshop
Showing a modified photo of a pyramid in Egypt using a snow filter.

Who's who

Content Authenticity Initiative (CAI):
Outreach, Advocacy, Open Source
Coalition for Content Provenance and Authenticity (C2PA):
Technical Standards: What/How
Creator Assertions Working Group**: CAWG**

C2PA data model:

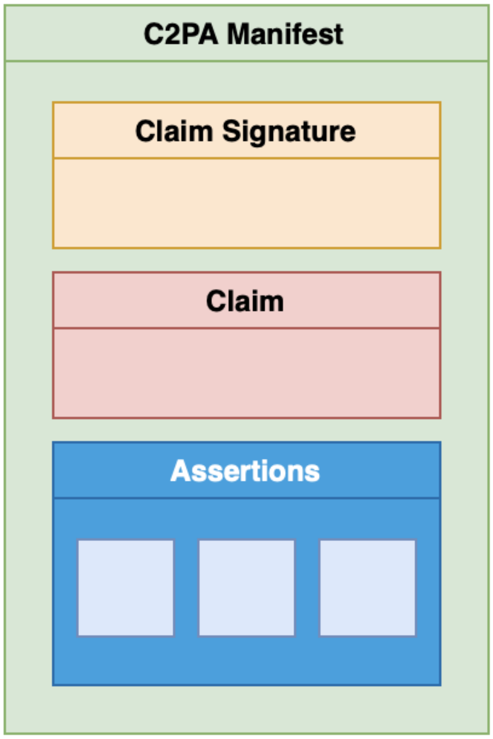


Figure 1. A C2PA Manifest and its constituent parts

source: https://c2pa.org/specifications/specifications/2.0/specs/C2PA_Specification.html

asset: any piece of digital media that we wish to describe
C2PA Manifest: Each asset in C2PA has an active manifest which describes the current asset
Assertions: are opt-in statements that cover areas such as:
note: Assertions can be redacted (overwritten by zeros) by future manifest producers.

an example:

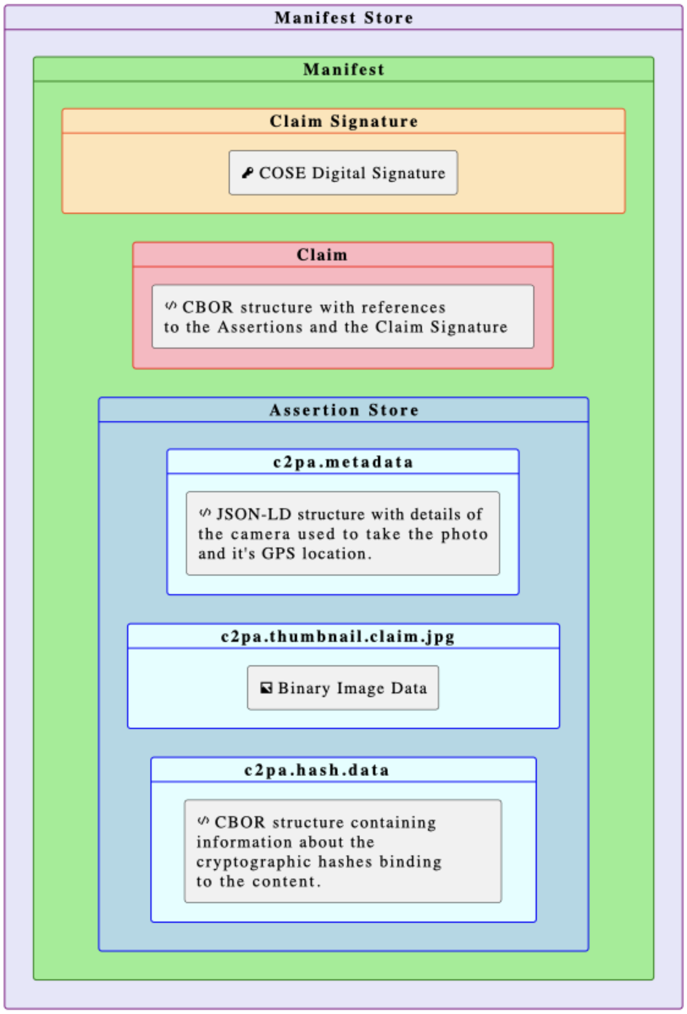

Manifest Store
Manifest
Claim Signature
COSE Digital Signature
Claim
CBOR structure with references to the Assertions and the Claim Signature
Assertion Store
c2pa.metadata
JSON-LD structure with details of the camera used to take the photo and it's GPS location.
c2pa.thumbnail.claim.jpg
Binary Image Data
c2pa.hash.data
CBOR structure containing information about the cryptographic hashes binding to the content.

Figure 2. Example C2PA Manifest of a Photograph

some examples of non-C2PA assertions:

- identity of the content creators
-

Current focus on data types: still images, videos, sounds, fonts
Text content is a bit trickier: e.g. text on the web can have different tags later if you change your CMS

C2PA Design Goals
source:
https://c2pa.org/specifications/specifications/2.0/specs/C2PA_Specification.html#_design_goals

Goal	Description
Privacy	Enable users to control the privacy of their information, including consumption data and information recorded in provenance
Responsibility	Ensure consumers can determine the provenance of an asset
Scalability	Enable creation/consumption/validation of media provenance at the same scale as media creation/consumption on the web
Extensibility	Ensure future metadata and credential providers are able to add their information without requiring input or approval from the C2PA
Interoperability	Ensure that differing implementations are able to operate with each other without ambiguity
Whole Workflow Applicability	Maintain the provenance of the asset across multiple tools, from creation through all subsequent modification and publication/distribution
Technology Minimalism	Create only the minimum required novel technology in the specification by relying on prior, well-established techniques
Security	Design to ensure that consumers can trust the integrity and source of provenance, and ensure the design is reviewed by experts
Content Ubiquity	Enable the inclusion of provenance for all common media types, including documents
Flexible Locality	Enable both online and offline (asset-only) storage and consumption/validation of provenance

Global Universality	Design for the needs of interested users throughout the world
Accessibility	Ensure that the technology can be used in a way that conform to recognized accessibility standards, such as WCAG
Harms and Misuse	Design to avert and mitigate potential harms, including threats to human rights and disproportionate risks to vulnerable groups
Evolving	Continuous review of the specification against these goals to ensure that they remain our priority

Identity assertion: Why?
Overview: allows a credential holder to sign a data structure we call signer_payload, which contains

- Tamper-evident references
- Role of credential subject with regard to the content

Identity assertion is **optional**
identity assertion may be repeated any numbers of times
identity assertions can be redacted if needed for privacy/safety reasons

Creators are invited to participate in weekly meetings.
URL: ??

======= END HUMAN ON-SITE NOTE TAKING ====================================
== START PERPLEXITY.AI SUMMARIZATION BASED ON AUDIO TRANSCRIPT USING OPENAI WHISPER==

The provided transcript and sources delve into the intricacies of the Content Authenticity Initiative (CAI) and the Coalition for Content Provenance and Authenticity (C2PA), highlighting their efforts to combat misinformation and ensure the authenticity of digital content. Here are the discussion notes, key understandings, outstanding questions, observations, and action items derived from the information:

Discussion Notes and Key Understandings

- **Initiatives' Goals**: Both CAI and C2PA aim to address the growing concern of digital misinformation by developing standards and technologies for certifying the authenticity and provenance of digital media (images, videos, documents, etc.). This includes the creation, editing, and sharing phases of digital content[1][2][3][4][6][7][8][11][12][16].

- **Technical Approaches**: The initiatives employ cryptographic asset hashing, tamper-evident seals, and possibly blockchain technology to secure metadata and ensure that any alterations to digital content are detectable[4][14][16]. This approach does not aim to judge the truthfulness of the content itself but to provide transparent information about its origin and alterations[20].
- **Industry Collaboration**: A wide range of industry players, including Adobe, Microsoft, Intel, BBC, and various camera manufacturers like Leica, Nikon, and Sony, are involved in these initiatives. This collaboration underscores the cross-industry effort to establish a global standard for content authenticity[2][3][6][7][11][12][14][16].
- **Consumer Education and Empowerment**: A significant focus is placed on educating consumers about digital content authenticity and providing them with tools to verify the integrity of the content they encounter online. This is crucial for rebuilding trust in digital media[2][4][8][20].
- **Open Standards and Interoperability**: The initiatives emphasize the importance of open standards and interoperability among different tools and platforms to ensure that authenticity mechanisms can be widely adopted and are tool-agnostic[2][3][4][6][11].

Outstanding Questions

- **Handling of AI-Generated Content**: How will the initiatives address the challenges posed by AI-generated content, especially as AI becomes more sophisticated in creating realistic media?[20]
- **Global Adoption and Regulation**: What steps are being taken to ensure global adoption of these standards, and how will regulatory bodies across different countries be involved?[2][20]
- **Impact on Creative Processes**: How will these standards affect the creative processes of artists and content creators who rely on digital alterations as part of their art?[20]

Observations

- Shift Towards Transparency: There is a clear shift towards transparency in digital content creation and sharing, with a focus on empowering consumers to make informed decisions about the content they trust[2][4][8][20].
- Technological Innovation: The initiatives are at the forefront of technological innovation, leveraging advanced cryptographic techniques and potentially blockchain technology to secure digital content authenticity[4][14][16].

Action Items and Next Steps

- **Further Development of Standards**: Continue the development and refinement of technical standards for content provenance and authenticity, ensuring they are adaptable to future technological advancements[3][11][19].
- **Expansion of Industry Collaboration**: Engage more industry players, including social media platforms, news organizations, and content creators, to join the initiatives and contribute to the development of standards[6][7][11][12].
- **Consumer Education Campaigns**: Launch comprehensive education campaigns to raise awareness among consumers about content authenticity and how to verify it[2][8][20].

- **Pilot Implementations**: Conduct pilot implementations of the standards in real-world scenarios, gathering feedback from creators, publishers, and consumers to refine the approaches[4][14].
- **Regulatory Engagement**: Engage with regulatory bodies and governments to explore how these standards can be supported or mandated to combat misinformation effectively[2][20].

These action items and next steps are crucial for advancing the goals of the CAI and C2PA, ensuring the integrity of digital content, and rebuilding trust in the digital media landscape.

Citations: [1] https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/1617151/d1974169-4f02-421b-9bb3-eb873c7e7434/paste.txt [2] https://www.scoredetect.com/blog/posts/content-authenticity-verification-tools [3] https://c2pa.org/faq/ [4] https://contentauthenticity.org/how-it-works [5] https://smartframe.io/blog/content-authenticity-initiative-what-you-need-to-know/ [6] https://blog.adobe.com/en/publish/2021/02/22/adobe-continues-content-authenticity-commitment-founder-c2pa-standards-org [7] https://blog.adobe.com/en/publish/2019/11/04/content-authenticity-initiative [8] https://contentauthenticity.org/blog/test [9] https://blog.adobe.com/en/topics/content-authenticity [10] https://blog.witness.org/2020/08/adobe-content-authenticity-initiative-approach-authenticity-infrastructure-media-manipulation/ [11] https://c2pa.org [12] https://truepic.com/glossary-the-abcs-of-content-authenticity/ [13] https://contentauthenticity.org/blog/the-content-authenticity-initiative-summit-collaborating-to-drive-trust-and-transparency-online-7249m [14] https://cmavideo.co.uk/what-is-the-content-authenticity-initiative/ [15] https://smartframe.io/blog/c2pa-everything-you-need-to-know-about-the-c2pa-project/ [16] https://en.wikipedia.org/wiki/Content_Authenticity_Initiative [17] https://originality.ai/blog/verify-writings-originality [18] https://blog.spruceid.com/content-authenticity-in-the-age-of-ai/ [19] https://c2pa.org/specifications/specifications/1.3/index.html [20] https://contentauthenticity.org/faq

==

Audio transcript Summary

The transcript primarily discusses the Content Authenticity Initiative (CAI) and the Coalition for Content Provenance and Authenticity (C2PA), focusing on their efforts to combat misinformation and ensure the authenticity of digital content. Here are the key points highlighted in the transcript:

1. Introduction and Purpose: The speaker, Eric Skelton from Adobe, introduces the Content Authenticity Initiative (CAI) and its connection to the broader goals of content authenticity and combating misinformation. The initiative aims to provide mechanisms for well-intentioned content creators to distinguish themselves from those spreading misinformation by making tamper-evident statements about their content[1].

2. Content Authenticity Initiative (CAI) and C2PA: The CAI and C2PA are efforts led by Adobe and other industry partners to address digital misinformation through the development of standards for content provenance and authenticity. The CAI focuses on promoting and providing an open, cross-industry approach to media transparency, while the C2PA develops technical standards for certifying the source and history of media content[2][3][5].

3. Technical Aspects and Implementation: The transcript delves into the technical aspects of implementing content authenticity, including the use of data models, assertions, and manifest stores. It discusses how digital content can be authenticated from creation to editing and sharing, ensuring that any alterations are transparent and verifiable[1].
4. Privacy and User Control: Privacy concerns and user control over data are emphasized, with mechanisms in place to ensure that content creators can choose what information to attach to their content and have control over whether provenance data is included[8].
5. Global Adoption and Open Standards: The initiatives aim for global adoption of digital provenance techniques through the creation of a rich ecosystem of digital provenance-enabled applications. This includes open-source development and cross-industry collaboration to ensure interoperability of tools and standards[6].
6. Impact on Professional Creators and Consumers: The standards and technologies developed by CAI and C2PA are critically important for professional creators, ensuring attribution and transparency in their digital work. For consumers, these standards help in understanding more about the content they consume, fostering trust in digital media[11].
7. Future Directions and Challenges: The transcript touches on future directions, including addressing the challenges of implementing these standards across different types of digital content and platforms. It also mentions the potential for regulatory bodies and governmental agencies to utilize these standards to establish norms for digital provenance[9][10].

In summary, the transcript outlines the efforts of the Content Authenticity Initiative and the Coalition for Content Provenance and Authenticity to combat misinformation and ensure the authenticity of digital content through the development of open standards, technical specifications, and global collaboration among industry partners.
Citations:

[1] https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/1617151/d1974169-4f02-421b-9bb3-eb873c7e7434/paste.txt
[2] https://contentauthenticity.org/faq
[3] https://c2pa.org
[4] https://truepic.com/glossary-the-abcs-of-content-authenticity/
[5] https://en.wikipedia.org/wiki/Content_Authenticity_Initiative
[6] https://opensource.contentauthenticity.org/docs/introduction/
[7] https://www.thesslstore.com/blog/real-photo-vs-ai-generated-art-a-new-standard-c2pa-uses-pki-to-show-an-images-history/
[8] https://contentauthenticity.org/how-it-works
[9] https://c2pa.org/specifications/specifications/1.3/specs/_attachments/C2PA_Specification.pdf
[10]
https://c2pa.org/specifications/specifications/1.0/specs/_attachments/C2PA_Specification.pdf
[11] https://www.imaging-resource.com/news/2022/10/21/adobes-content-authenticity-initiative-partners-with-leica-and-nikon-to-pro
[12] https://www.youtube.com/watch?v=nQNTMicYu6E

== END PERPLEXITY.AI SUMMARIZATION BASED ON AUDIO TRANSCRIPT USING OPENAI WHISPER==

Vocabulary - What does all of this mean?

Session Convener: Michael K.
Session Notes Taker(s): Michael K.

Tags / links to resources / technology discussed, related to this session:

- Sovrin Glossary
- Edelman Trust Barometer

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

Following content formatted in Markdown (My bad, sorry!)

- **IEEE** Institute of Electrical and Electronics Engineers - A professonal body that encourages standardization.
- **IETF** Internet Engineering Task Force - Output is RFC's, BCP's, etc.
- **RFC** Request for Comments - It an internet standards document.
- **Authentication** Who are you.
  - Similar to "Authentic" i.e. allowing verification whether something is Authentic.
- **Authorization** What are you allowed to do.
- **Foundational ID** An identification, usually issued by a government that identifies who you are. This varies by country - some countries may use a Birth Certificate, others may use a passport or a personal ID. Be culturally conscious when using this term.
- **Functional ID** An Identifier that provides a benefit. e.g. a Passport provides the benefit of cross-border travel. A Driver's license provides the benefit of driving.
- **Foundational Record**
- **Levels of Assurance**
- **CRVS** Civil Registration of Vital Statistics
- **Credential**
  - A digital assertion containing claims about itself or another entity.
- **Claims**
  - An assertion about an Attribute of a Subject
- **Records**
- **Verification**
- **Identification**
- **OAuth2**
  - Client Credentials Flow
  - Authorization Code Flow
- **OIDC**
  -
- **Token**
- **Access Token**
- **Identity Token**

- **SAML** Security Assertion Markup Language
- **Subjects**
- **Holder**
- **SPIFFE**
- **Issuer**
- **Certificate**
- **x509**
- **PKI** Private Key Infrastructure
- **Selective Disclosure**
  - The ability to only offer access to the claims relevant to a particular authorization.
- **Signature**
- **Governance and Trust Framework**
- **Identity Binding**
- **Relying Party**
- **Digital Public Infrastructure**
- **MDL**
- **PGP**

Statements made of note:

- We here at IIW get into a lot of nitty gritty details about these topics and words, but the complexity and ambiguity of the language we use, comes off as a lack of clarity to outside observers. To be taken seriously, a much more simplified vocabulary is needed.
  - I.e. We're nerds, but we need to learn how to present to non-nerds.

Cultural nuances are critical. what might be a valid credential in one culture may not be in another. One culture may trust their government and their issued statements, another does not. Even words may have very different meanings based on the cultural and linguistic background of the speaker (An american english speaker will assume a different definition than a norwegian-native english speaker, as they carry preconceptions from their language-of-origin)

AI Authorization on Human's Behalf

Session Convener: Colby Anderson
Session Notes Taker(s): Jeremy Frank

Tags / links to resources / technology discussed, related to this session:

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

The discussion centered around how AI agents can be authorized to perform actions on behalf of humans. Several ideas were discussed:

1. Focus on the principle of least privilege and use a proxy/middleware that will manage authorization that is given to the AI, especially if server side changes can't be made to adapt to handle AI interactions.
    a. A new proxy would have to be built for each service to be interacted with which would impede the usefulness
    b. AI assistant -> proxy w/ token -> service
    c. Potentially the proxy could prompt the user (human controller of AI) with 2FA
2. Token-based approach: human controller delimits permissions, give token to AI assistant, AI assistant then goes to service with token
3. Service accounts for AI
    a. Not sufficient for autonomous entities that may make mistakes or act maliciously
4. Rabbit approach -> give credentials to AI?
5. Federated training -> arriving at a consensus on policy for personal AI?

Personal AI

Session Convener: Reza Rassool
Session Notes Taker(s): Doc Searls

Tags / links to resources / technology discussed, related to this session:

- https://kwaai.ai
- https://en.wikipedia.org/wiki/Physics-informed_neural_networks
- https://doc.searls.com/2022/10/11/p7012/
- https://duckduckgo.com/?q=rag+retrieval+augmented+generation&ia=web

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

Reza explained what Kwaai is and does. https://kwaai.ai

It's an org and a movement.

80% personal AI dev
10% research
10% policy

Working with Inrupt and Solid, which will work in the solutions stack.

Question about business models and getting free from giants.

Kwaai wants the simplest possible implementations. Easy install.

PINNS Physics-Informed Neural Networks mentioned https://en.wikipedia.org/wiki/Physics-informed_neural_networks

IEEE P7012 mentioned. Doc Searls wrote about it here: https://doc.searls.com/2022/10/11/p7012/

Day Waterbury: We should look for using some of the surplus compute in the world. Also, education: memetic battle over what it means is going on. The bigs want us to think that if we tune a model around what they have and do, and putting our Personal AI inside of that. And that's a bad thing. So the question is, is education a part of this?

Erica Connell: What are the options in the meantime, while Kwaai is out there? (Aside: https://www.getgather.com/about is moving in that direction.)

RAG is relevant: https://duckduckgo.com/?q=rag+retrieval+augmented+generation&ia=web

Ruth Rassool told the story of her experience around AI as an English teacher, using "Penny" the AI. This is a local AI.

Wearables were discussed. A framework that runs on a hybrid computing platform.

Question from Phil Kamarny about where personal AI is stored. Extant data outside, e.g. gmail data? Answer: Outside data stays there, but the main thing is to have and control your own data.

Question from Day Waterbury's son about the monopolies out there? Answer: Nvidia, Microsoft, Google, Meta. That's game over for the economy.

Hitchhiker's Guide to KERI

Session Convener: Nuttawut Kongsuwan
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

Link to Slides: http://bit.ly/keri-iiw38

Link to Blog Posts
https://medium.com/finema/the-hitchhikers-guide-to-keri-part-1-51371f655bba
https://medium.com/finema/the-hitchhikers-guide-to-keri-part-2-what-exactly-is-keri-e46a649ac54c
https://medium.com/finema/the-hitchhikers-guide-to-keri-part-3-how-do-you-use-keri-2d1724afa432

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

Type You Notes Here

Digital Credentials Consortium Updates

Session Convener: Dmitri Zagidulin
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

DIDComm 101

Session Convener: Colton Wolkins
Session Notes Taker(s): Sam Curren, Martina Kolpondinos

Tags / links to resources / technology discussed, related to this session:
https://didcomm.org/

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

Slides: Copy of DIDComm v2 101

Documentation (Under Development) http://book.didcomm.org

Browser Based Demo http://demo.didcomm.org
Note the 'Help' link in the top right, which contains explanations on how to use it.

Summary from the Session

Intro

Handle writing for DIDCom is not different from http (better patterns now). However, it is a protocol that is designed for a wide variety of use cases. Hence, it's important to highlight the common path through (easy flow), don't try to solve all of the things!

Characteristics of DIDComm

- secure
- private
- extensible
- message oriented (not streaming a ton of data → yet, does not prohibit to send large files but it's often not adviced to do so as the receiver might reject them)
- asynchronous
- routable
- transport-agnostic (e.g., https, http, web sockets, ..)
- interoperable (DIDComm within CHAPI is possible, yet, not very common)

Default behavior

- One sender and one recipient with a secure connection in between
- DID → resolver → DIDDoc → service end-point
    - whether done on a high-end server or on a mobile device, the architecture protocol is always the same
- DID is anchor for DIDCom

- Service end-points are only needed if it is unknown who the recipient is
    - With DID Methods that do not support service end-points it has to always be clear who the recipient is
- The sender defines in the DIDDoc how a message is being routed and which encryption algorithm has to be used
    - the message is encrypted to the recipient
        - only the intended final recipient (e.g., Bob) is able to decrypt the message
    - Mediators (hops) can be used
        - internal and external mediators exist

SESSION #2

Digital Identity and the Open Social Web in 2024

Session Convener: Johannes Ernst
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

https://fedidevs.org – hang out with other Fediverse and related developers
https://fediforum.org – unconference for the Fediverse run by Johannes and Kaliya

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

This session had been intended to talk about specific identity-related use cases that the fediverse does not solve very well today.

However, many people in the room were looking for more basic information about what the fediverse is, how it works, what protocols are involved, who is working on it and where etc.

Some ideas on how to "upgrade" the use of public keys in the fediverse today (focused mostly on just signing HTTP requests) to something that can be used for content signing, prove identity across multiple servers etc.

Introduction to OpenID Connect

Session Convener: Mike Jones
Session Notes Taker(s): Mike Jones

Tags/links to resources / technology discussed, related to this session:

The presentation is posted at https://self-issued.info/?p=2518.

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

The session was well attended. There were good discussions on how OpenID Connect relates to other initiatives in the OpenID Foundation and other identity standards efforts.

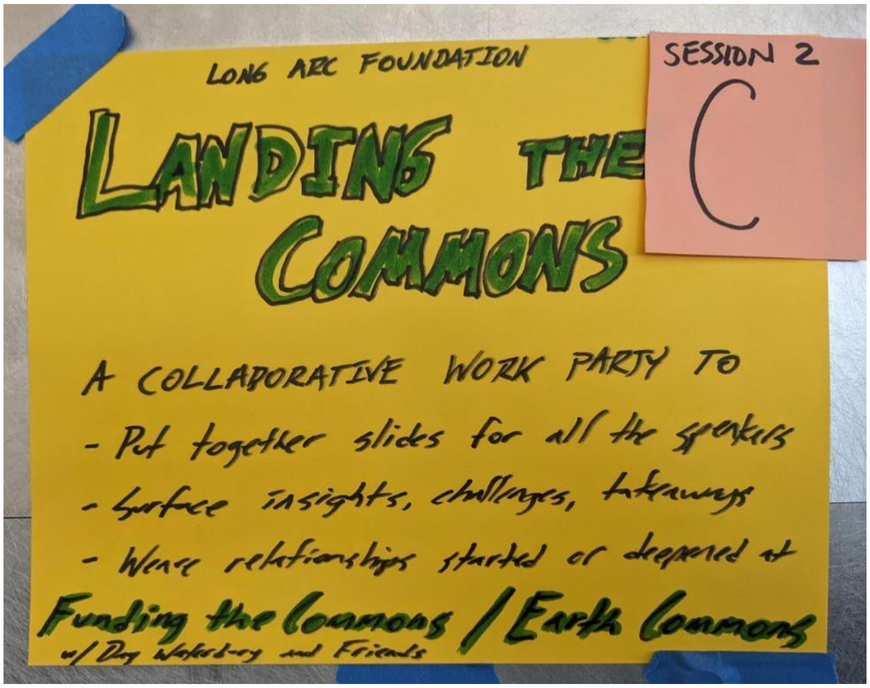
Landing the Commons

Session Convener: Day Waterbury
Session Notes Taker(s): Day Waterbury

Tags / links to resources / technology discussed, related to this session:

https://fundingthecommons.io
https://fundingthecommons.io/earth-commons-san-francisco-bay-area-2024

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



LONG ARC FOUNDATION

SESSION 2

C

LANDING THE COMMONS

A COLLABORATIVE WORK PARTY TO

- Put together slides for all the speakers
- Surface insights, challenges, takeaways
- Weave relationships started or deepened at

Funding the Commons / Earth Commons

w/ Day Waterbury and Friends

I have compiled some of these decks and connections, which were indeed epic. I don't have time to upload them all here at this time. Please be in touch with me via Signal @deiim.69 if you're interested.

- Here's a Proton Drive folder I'll put stuff in over time (PW: FtC+ECB24->IIW38)
  - There's strong alignment with Benjamin Life at Open Civics: OpenCivics.co
  - And with Samantha Power of Finance for Gaia: https://FinanceForGaia.com
- From Daniel Friedman of Active Inference Institue:
  - Active Inference Institute - main site
  - Activities · AII Onboarding - participatory activities
  - daniel@activeinference.institute for email
- Jessy Kate, of course! Lawyering for the Planet
- And Brett Levin: https://drive.google.com/file/d/1gdt-61bHOouGxIfxO4nsjMSqAoxAE8Qh/view?usp=drive_web
- Matthew Monahan: Earth Commons / Ma Earth - April 14 2024

SSI for Democracy

Session Convener: Britt Blazer
Session Notes Taker(s): Doc Searls

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

18 people in attendance, more in the zoom waiting room

Decisions in elections are based on decisions made in the 19th century

Democracy 3.0 is baked on a concept that 1.0 was propertied white guys, and 2.0 was wealthy white guys deciding things. 3.0 is building it ourselves.

Crowdsource policy making. Voting doesn't matter.

The one SS thing in our lives is deciding how we live.

Explained the League of Technical voters, constituent verification and proclamation, committee-picker robot (congress.gov) and committee rep picker.

Britt will send Doc the .pdf being showed on screen.

It's about making lobbying available to everyone, and a new hack for activists.

What can verified constituents say to move the needle?
Detail on specific questions and exhibits a verified constituent might present

Democracy 3.0 | Civilization software
Lots of data pulled from Congress.gov

21st Century voters

Want people to understand that being a self-sovereign citizen means you can be an effective lobbyist.

It's how you can have direct effects. How you can be far more than a voter.

It's how you can be a real influencer.

Wendy Seltzer: what happens when this becomes a big success, what prevents corruption?

Something gets sent to the address, is cross-referenced to the voter roll, and that makes you obligated to support the policy sentiment of the majority of voters. Verified citizen. (Britt needs to correct this.)

Ethan Vanklozen, former lobbyist and campaign guy, pushed back. Loves the concept. Would use the tools, but not in the game right now.

Several questions about situations where the majority opinion is at odds with the user of the tool(s).

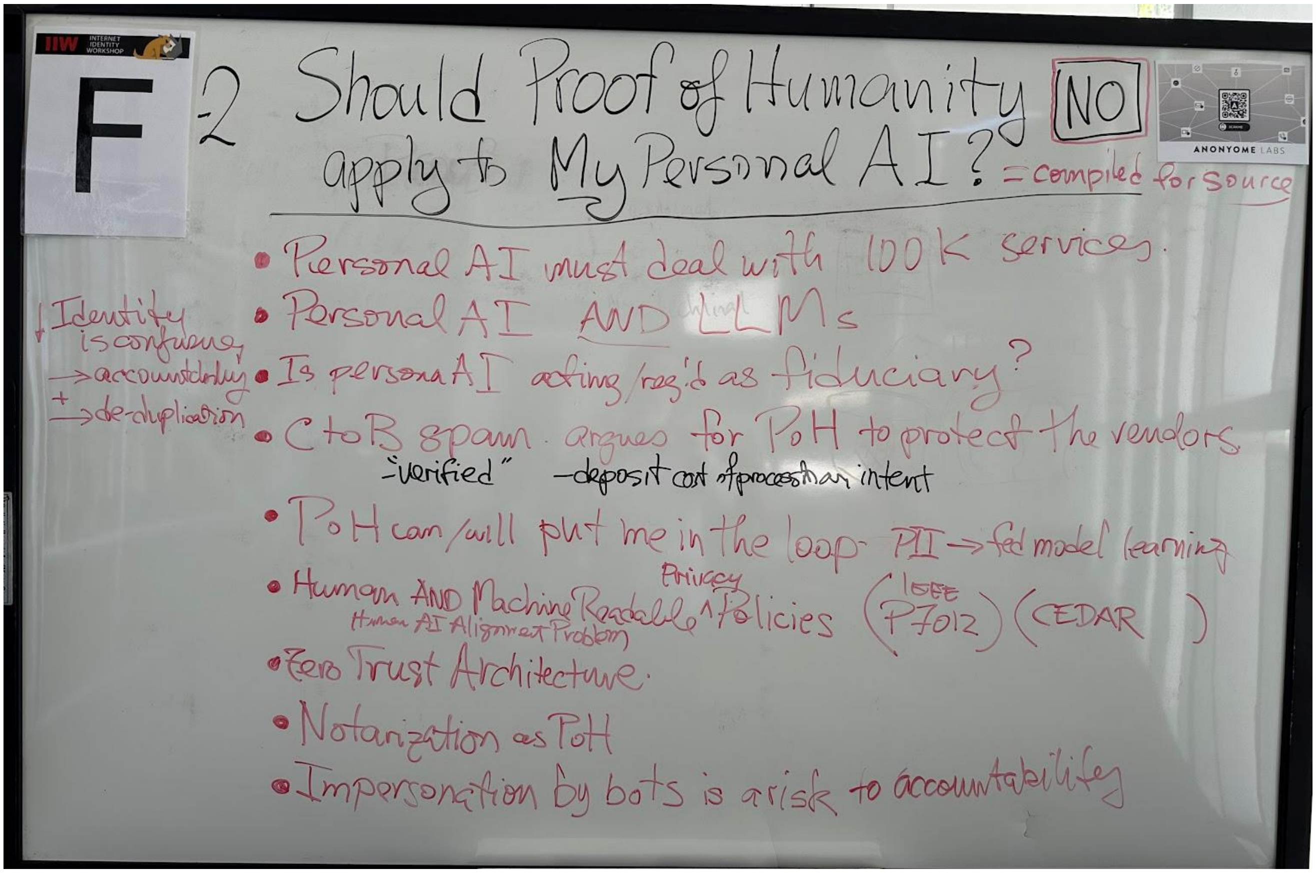
Ethan: this amplifies what the polls say.

The model in Phil Windley's head is a model where the most influential citizen get a responsibility to carry water for the group wanting to lobby through them.

Should Proof of Humanity Apply to My Personal AI?

Session Convener: Adrian Gropper
Session Notes Taker(s): Adrian Gropper

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



F-2 Should Proof of Humanity apply to My Personal AI? NO =compiled for source

- Personal AI must deal with 100K services.
- Personal AI AND LLMs
- Is persona AI acting/reg'd as fiduciary?
- C to B spam argues for PoH to protect the vendors
  "verified" —deposit cost of processing an intent
- PoH can/will put me in the loop PII → fed model learning
- Human AND Machine Readable Privacy Policies (IEEE P7012) (CEDAR)
  Human AI Alignment Problem
- Zero Trust Architecture.
- Notarization as PoH
- Impersonation by bots is a risk to accountability

↓ Identity is confusing
→ accountability
+ → de-duplication

ISO mdoc 101

Session Convener: Oliver Terbu
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

materials used are here:
https://docs.google.com/presentation/d/164EGm7NJiMeDGEdIPtIdayft3rL-7-sotSVDD4rIdto

Trust Over IP (ToIP) Fondation

1. **Learn about a Digital Trust Ecosystem**
2. **Learn about the Current and Future Work of ToIP**
3. **Learn about how to engage at ToIP**

Session Convener: Judith Fleenor, Executive Director, ToIP
Session Notes Taker(s): Judith Fleenor

Tags / links to resources / technology discussed, related to this session:

ToIP Introduction Deck:

- Highlighting the ToIP Dual Stack, how the Technology Stack and Grovenance Stack work together to allow Ecosystems to select their required elements.
- Highlighting the key work products being developed at ToIP Currently
- And, about membership and contribution options.

ToIP's current work and who do I talk to?
A list of our current work products with QR Codes for more information and who to contact for further discussion.

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

ToIP's Mission: To simplify and standardise how trust is established over a digital network or using digital tools.

We focus on both:

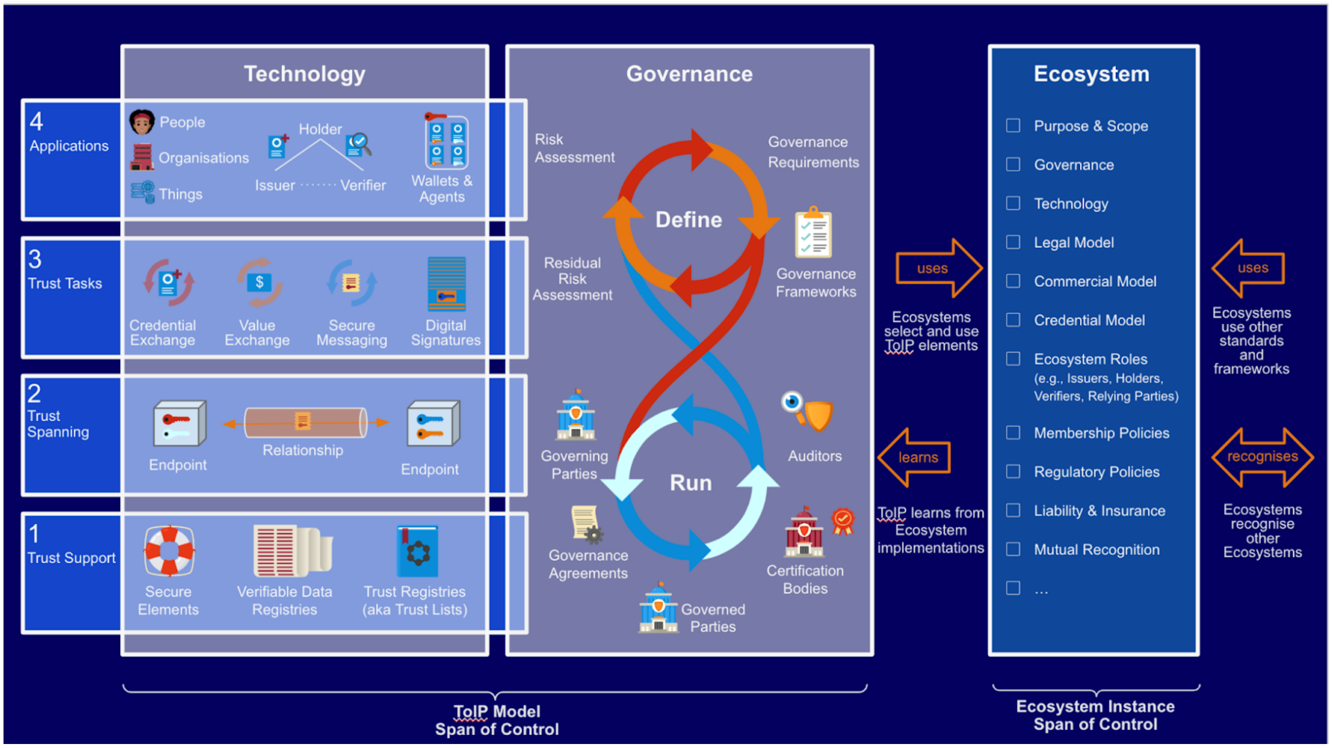
- Interoperability and cryptographic verifiability at the machine layers
- Human accountability at the legal, business, and social layers

ToIP creates:

1. Specifications – that can be in code
2. Templates – that can be instantiated as documents
3. Definitions – that can be can be incorporated by different organizations
4. Recommendations –that can be that can be followed
5. Implementation plans - that can be executed
6. White Papers – that can be understood to clarify complex issues
   in the Self Sovereign Identity and Verifiable Credentials space, and the entire digital trust landscape.

Here is a list of ToIP's most current work.

This is an image for the ToIP dual stack and how ecosystems interact with it:



View the IIW #38 ToIP Intro deck to see how each of the work products fit into the ToIP Stack.

ToIP is Joint Development Foundation (JDF) project within the
Linux Foundation (LF)

- The JDF is the standards development organisation within the Linux Foundation open source community with connections to ISO and other standards bodies.
- Linux Foundation and the JDF is our fiduciary to manage the ToIP funds and provide the legal structure for the foundation.
- Linux Foundation provides the infrastructure for our work and is known for collaborative processes.

ToIP is:

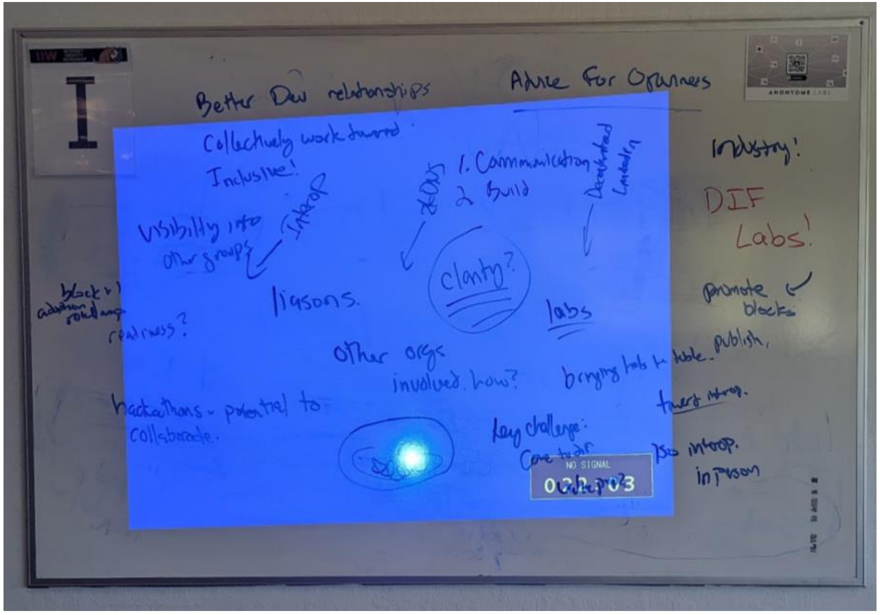
- Collaborative Community
- International Community meetings happen in various time zones via Zoom.
- Asynchronous collaboration via Google Docs and GitHub and the ToIP Slack Workspace.
- Industry experts and people new to decentralised identity.
- The Trust Over IP (ToIP) Foundation was launched in May 2020 with 27 original founding member organisations.
  ToIP now (*Spring 2024*) has **over 500** member organisations and individuals.
- We are financially supported by our membership.
- The work gets done by contributors like you!

DIF for DEVS - Labs Working Group Coming!!

Session Convener: Andre & Kim
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

Labs Working Group - IIW Spring 2024



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

- Make it easier for developers to build things
- Added missing part of lifecycle: using applications

- Looking for feedback for
- More ongoing focus on interoperability
- Name: labs feels more open than clinics
- Encourage experimentation
- Advice for openness
    - who shows up: harder for smaller companies to show up to these weekly meetings
    - make it easier to easier to publish something (blogs)
- reviewed lifecycle
- oidf: interop events and hackathons
- how to reach
- science fair
    - in-person element
- how to incorporate feedback
- Next steps
    - Clarify that any decentralized identity tech is welcome
    - inclusivity matters
    - improve dev relationships
    - give visibility into other groups
    - hackathons, potential to collaborate
    - communicate and build

Agentic Collective Identity

Session Convener: Travis Well
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

NEW!! The Last DID Method = Trust DID Web `did:tdw`

Session Convener: Stephen Curran
Session Notes Taker(s): Jin Wen

Tags / links to resources / technology discussed, related to this session:

Latest Draft:

Summary: A new DID Method that builds on did:web that adds access to a verifiable history of the DID as the DIDDoc evolves, authorised keys for updating a DID, and the DID includes a self-certifying identifier (SCID) that enables movement of the DID to other DID locations when required or desired. The DID Method has relatively low complexity dependencies — nothing fancy!! Further, since HTTPS URLs are so easy to use, the DID Method makes it easy to translate DID URLs into HTTPS URLs for retrieving DID-related files. Special callout to <did>/whois, which is a DID Method URL that resolves to a Verifiable Presentation where the DID is the `credentialSubject` in the VCs in the Verifiable Presentation.

We also covered advanced features, such as publishing a parallel did:web DID, key pre-rotation support, what keys are "authorised" per the DID-Core specification, multi-signature authorization handling, the two implementations and more.

Session Presentation: Trust DID Web - A New Web-Based DID Method
Specification: https://bcgov.github.io/trustdidweb
Typescript Implementation: **https://github.com/bcgov/trustdidweb-ts/**
Python Implementation: https://github.com/bcgov/trustdidweb-py

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

outstanding questions: Mike mentioned that similar issue happen to SAML could happen here because

What is did:tdw

- similar to did:web, but with ledgerless, verifiable, authorized history
- instead of/beside did:web's did.json file, there is a did.jsonl file
  - JSON Lines (jsonl) – lines of JSON - jsonlines.org
- Could publish both `did:tdw` and `did:web` DIDs - although using the `did:web` DID reduces the security model.

Who fund this: BC Gov

- Started with well-defined (but not obviously implemented) requirements
- Result - clear, simple and complete specification and 2 implementations.
- Builds on many years of listening to the challenges.

Mechanics

Each entry is a JSON array of 6 elements:
[entryHash, versionID, versionTime, parameters, DIDDoc, dataIntegrityProof]

parameters - configurations for entry processing

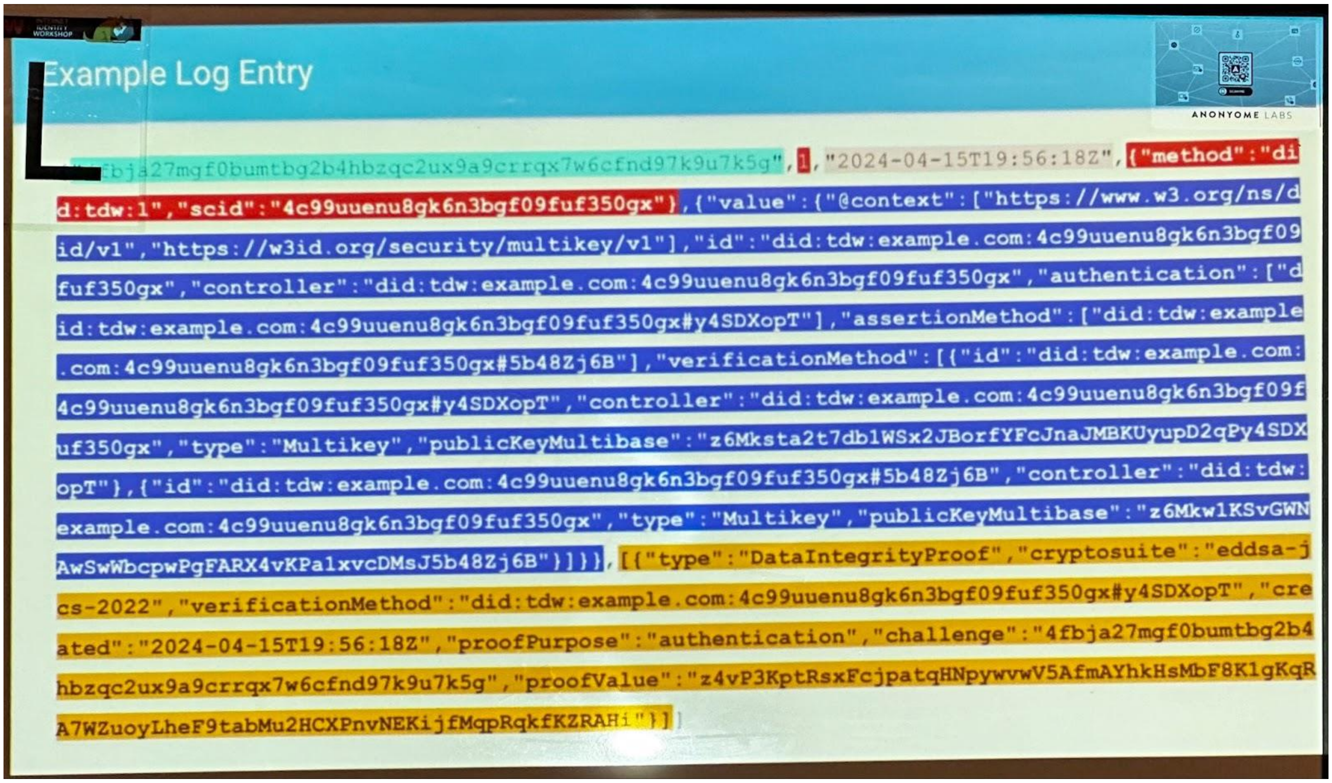
- examples - algorithms in use: did:tdw spec, hash, cryptosuite

Dependencies

- Hash — default to sha256 but specification can add more schemes
- Base32 Encoding
- JSON Canonicalization Scheme
- JSON-Patch (used to define the transition from one DIDDoc to the next)
- W3C Data Integrity

Creation, Verification Process

how SCID is generated: from initial DIDDoc – placeholders in place of SCID {SCID}
a did:tdb log is shown here



Example Log Entry

```
"fbja27mgf0bumtbg2b4hbzqc2ux9a9crrqx7w6cfnd97k9u7k5g",1,"2024-04-15T19:56:18Z",{"method":"di
d:tdw:1","scid":"4c99uuenu8gk6n3bgf09fuf350gx"},{"value":{"@context":["https://www.w3.org/ns/d
id/v1","https://w3id.org/security/multikey/v1"],"id":"did:tdw:example.com:4c99uuenu8gk6n3bgf09
fuf350gx","controller":"did:tdw:example.com:4c99uuenu8gk6n3bgf09fuf350gx","authentication":["d
id:tdw:example.com:4c99uuenu8gk6n3bgf09fuf350gx#y4SDXopT"],"assertionMethod":["did:tdw:example
.com:4c99uuenu8gk6n3bgf09fuf350gx#5b48Zj6B"],"verificationMethod":[{"id":"did:tdw:example.com:
4c99uuenu8gk6n3bgf09fuf350gx#y4SDXopT","controller":"did:tdw:example.com:4c99uuenu8gk6n3bgf09f
uf350gx","type":"Multikey","publicKeyMultibase":"z6Mksta2t7db1WSx2JBorfYFcJnaJMBKUyupD2qPy4SDX
opT"},{"id":"did:tdw:example.com:4c99uuenu8gk6n3bgf09fuf350gx#5b48Zj6B","controller":"did:tdw:
example.com:4c99uuenu8gk6n3bgf09fuf350gx","type":"Multikey","publicKeyMultibase":"z6Mkw1KSvGWN
AwSwWbcpwPgFARX4vKPa1xvcDMsJ5b48Zj6B"}]}},[{"type":"DataIntegrityProof","cryptosuite":"eddsa-j
cs-2022","verificationMethod":"did:tdw:example.com:4c99uuenu8gk6n3bgf09fuf350gx#y4SDXopT","cre
ated":"2024-04-15T19:56:18Z","proofPurpose":"authentication","challenge":"4fbja27mgf0bumtbg2b4
hbzqc2ux9a9crrqx7w6cfnd97k9u7k5g","proofValue":"z4vP3KptRsxFcjpatqHNpywvwV5AfmAYhkHsMbF8K1gKqR
A7WZuoyLheF9tabMu2HCXPnvNEKijfMqpRqkfKZRAHi"}]]
```

Interesting Topics

- parallel publishing with did:web
- DID URL Handling: Paths

Use cases

/whois

Traversing the Web of Trust from 2018 paper
Link to implicit service definition

Transcript summary for the basic content portion:
Key points in the transcript:

1. The goal is for a DID to provide a verifiable presentation linked to the DID subject and signed by the DID itself, accessible via a /whois click.

2. The simplicity of transforming a DID to an HTTP URL is emphasized, as it simplifies usage and is compatible with any DID method.

3. The project is funded by BCGov and achieved significant progress in about a month and a half, including two implementations and a full specification ready for feedback.

4. The implementation is concise, with less than 1500 lines of Python code, and the mechanics involve a DID to HTTP transformation similar to DID web but with an added 'L'.

5. The system uses a JSON array with six elements for each entry, which includes a version ID, version time, parameters item, and a data container group signed by an authorised user.

6. The parameters allow for the configuration of entry processing, including hash algorithms, crypto suites, and DID spec versions, allowing for evolution and advanced features like DID migration.

7. Dependencies for the system are minimal, including SHA-256, Base32 encoding, a JSON canonicalization scheme, JSON patch, and data integrity proofs.

8. The creation of data process involves inputs like the DID document and preset parameters, with requirements for an ID and an authentication key within the DID document.

9. The system uses a method called "scid" that replaces placeholders in the DID document and ensures data integrity through a chaining mechanism. Note: It does not use KERI directly due to dependency considerations, but it is inspired by KERI

10. The entry structure in the file is an array with a consistent format, and the system allows for changes in parameters to be made mid-stream.

11. There is some discussion about the choice of data structures and the proof mechanism, with a focus on simplicity and minimal dependencies.

12. The possibility of parallel publishing using DID:WEB is discussed, with considerations for verifiability and adoption.

13. The system defines two services, cache files??, and cache news??, which are included in the spec and can be used implicitly or explicitly added to the DID doc.

14. The system does not change how a key within the DID doc is referenced; it uses the same method as the DID core specification.

Additional discussions:

Flexible format of SCID: scid is part of the URL?

Moving DID's Web Location

- **social network porting from A to B**
- **Bluesky related use case — it hosts DIDs. Wouldn't it be nice if you could decide to move your Bluesky-based DID to another platform, while retaining the entire DIDDoc history.**

Next Steps:

- Move to standard bodies: ToIP, W3C, DIF? Suggestions on which one.
- More implementations beyond Typescript and Python.
- Adding to Aries Cloud Agent Python, including for use in rooting AnonCreds VCs.

Organizational Identity & Verifiable Authority

Session Convener: Timothy Ruff
Session Notes Taker(s): Kalyan Kulkarni

Tags / links to resources / technology discussed, related to this session:

Digital Identity Requirements

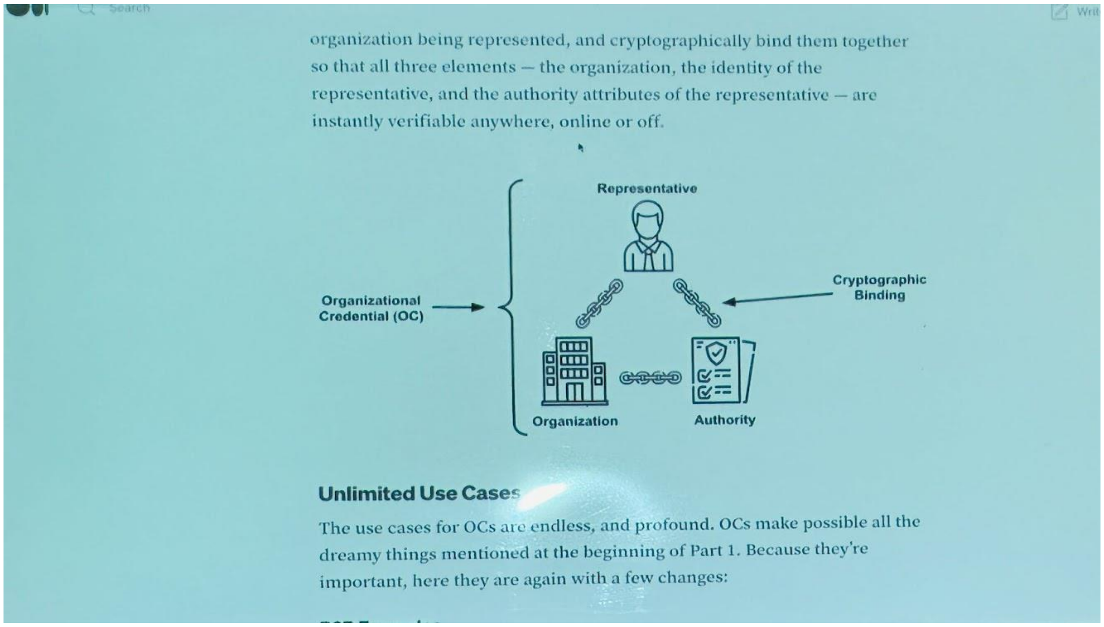
eIDAS: https://digital-strategy.ec.europa.eu/en/policies/discover-eidas

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

Organisational Identity is not about the Organization, it is about the authorities that represent the organisation.

So organisational Identity is authority on a representative

Entity + Representatives + Authority = Bind together the identity



organization being represented, and cryptographically bind them together so that all three elements — the organization, the identity of the representative, and the authority attributes of the representative — are instantly verifiable anywhere, online or off.

Unlimited Use Cases

The use cases for OCs are endless, and profound. OCs make possible all the dreamy things mentioned at the beginning of Part 1. Because they're important, here they are again with a few changes:

on a driving licence there are several bindings - name, photo, issuance by govt authority
Representative can be anything, authority is a role to do certain things

In organisational context, privacy mostly is zero

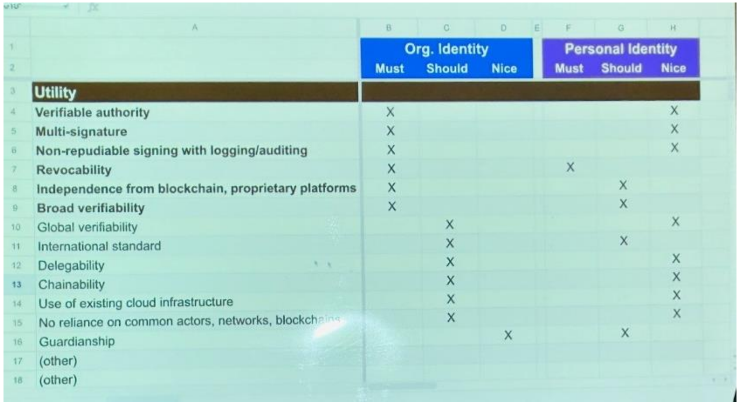
What kind of self-sovereignty one has when representing an entity
Autonomy

Utah has most of the organisations that have 'At will' employment.

Organisations have ability to put credentials in individual's wallet that are expected at or at no will of the individual

Privacy and Self-sovereignty are not the same when it comes to organisations
<u>A comparison between organisational identity v/s personal identity:</u>
Link to Timothy's spreadsheet: **[Digital Identity Requirements]**

Utility perspective:



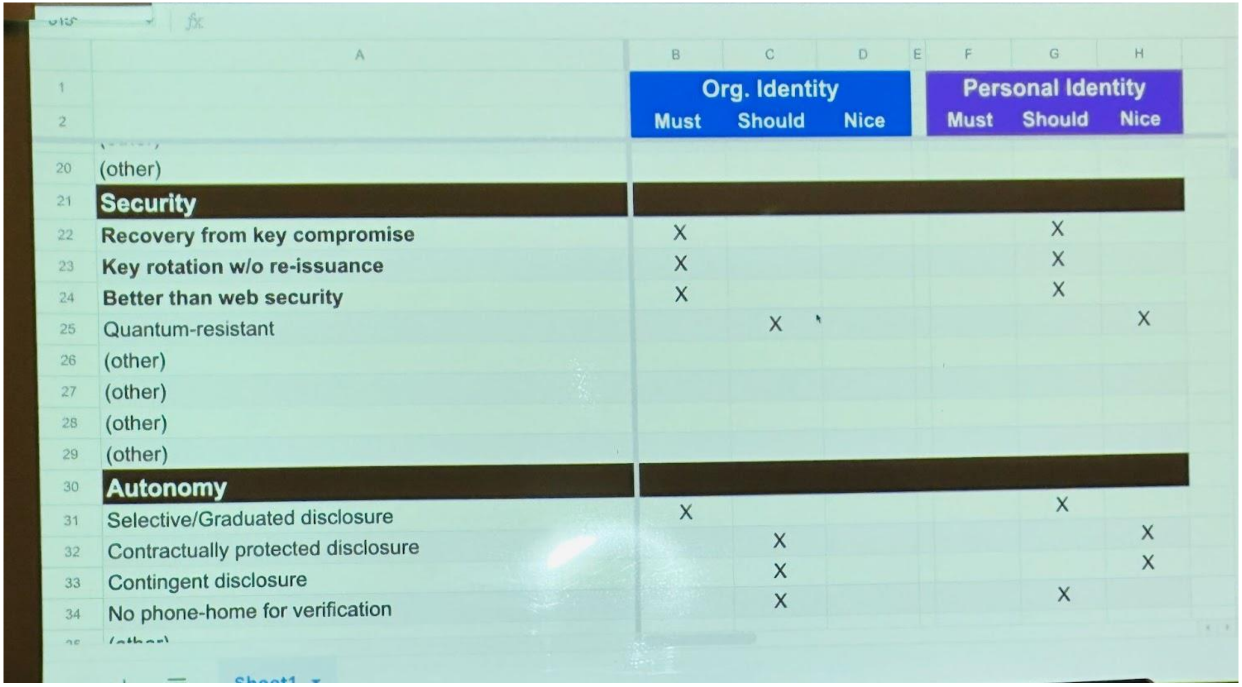
	Org. Identity			Personal Identity		
	Must	Should	Nice	Must	Should	Nice
Utility						
Verifiable authority	X					X
Multi-signature	X					X
Non-repudiable signing with logging/auditing	X					X
Revocability	X			X		
Independence from blockchain, proprietary platforms	X				X	
Broad verifiability	X				X	
Global verifiability		X				X
International standard		X			X	
Delegability		X				X
Chainability		X				X
Use of existing cloud infrastructure		X				X
No reliance on common actors, networks, blockchains		X				X
Guardianship			X		X	
(other)						
(other)						

Verifiable Authority for example - a police officer needs to prove he's so to a common man

Independence from Blockchain - independence from platforms but can use any protocol

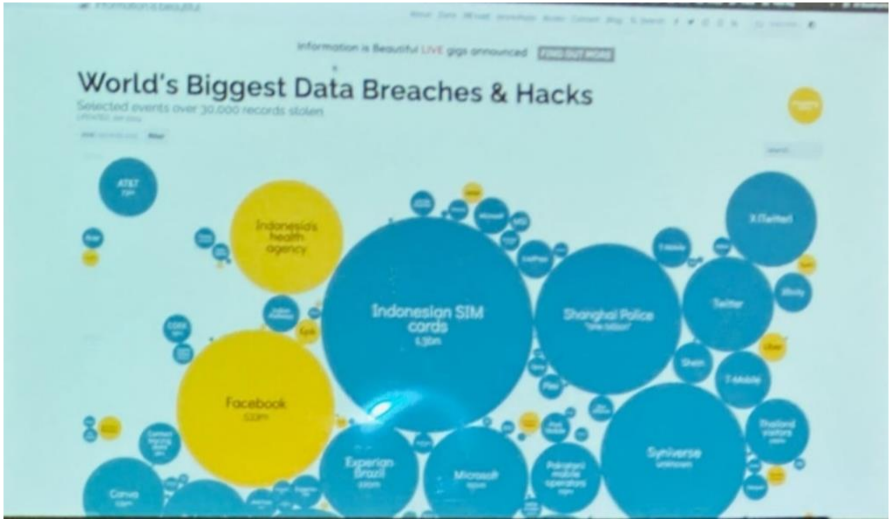
Broad verifiability - verifiability of your authority outside your organisation.
Global Verifiability - not every organisation needs to verify itself globally
It was discussed that cloud infrastructure can be optional and does not need to be in 'should' or 'nice'

Security perspective:



	A	B	C	D	E	F	G	H
1		Org. Identity				Personal Identity		
2		Must	Should	Nice		Must	Should	Nice
20	(other)							
21	**Security**							
22	**Recovery from key compromise**	X					X	
23	**Key rotation w/o re-issuance**	X					X	
24	**Better than web security**	X					X	
25	Quantum-resistant		X					X
26	(other)							
27	(other)							
28	(other)							
29	(other)							
30	**Autonomy**							
31	Selective/Graduated disclosure	X					X	
32	Contractually protected disclosure		X					X
33	Contingent disclosure		X					X
34	No phone-home for verification		X				X	

The web is broken -
an example of the same -



Which is why "better than web security" (like KERI) is needed.

SESSION #3

EBA Pilot Using the vLEI

Session Convener: Karla McKenna & Lance Byrd
Session Notes Taker(s): Karla McKenna .

Tags / links to resources / technology discussed, related to this session:

Participants attending the session were interested in both the operational processes and technical developments needed to execute the pilot, as well as the motivations of the various stakeholders, particularly the EBA and the banks in wanting to leverage the vLEI. There also was recognition that this approach could have more widespread applicability if adopted across a wider set of use cases

Rather than a link to the Slides as requested Slides in jpeg format were inserted ;)

Enabling global identity
Protecting digital trust

vLEI Pilot with European Banking Authority

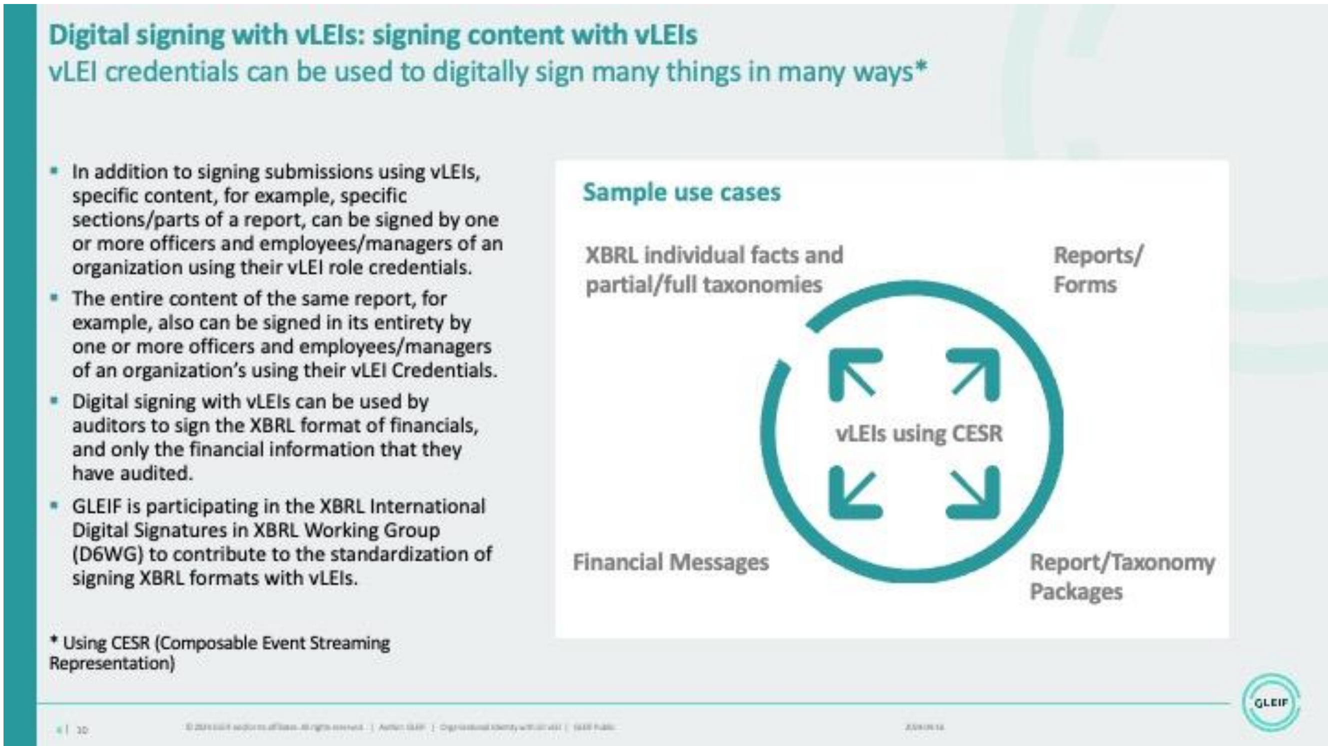
Pillar 3 Report Pilot
Internet Identity Workshop 38
April 16, 2024

Agenda

1. Digital signing using vLEIs
2. Technical View: Pillar 3 EBA Pilot

Enabling global identity
Protecting digital trust

Digital signing with vLEIs



Digital signing with vLEIs: signing content with vLEIs

vLEI credentials can be used to digitally sign many things in many ways*

- In addition to signing submissions using vLEIs, specific content, for example, specific sections/parts of a report, can be signed by one or more officers and employees/managers of an organization using their vLEI role credentials.
- The entire content of the same report, for example, also can be signed in its entirety by one or more officers and employees/managers of an organization's using their vLEI Credentials.
- Digital signing with vLEIs can be used by auditors to sign the XBRL format of financials, and only the financial information that they have audited.
- GLEIF is participating in the XBRL International Digital Signatures in XBRL Working Group (D6WG) to contribute to the standardization of signing XBRL formats with vLEIs.

Sample use cases

XBRL individual facts and partial/full taxonomies

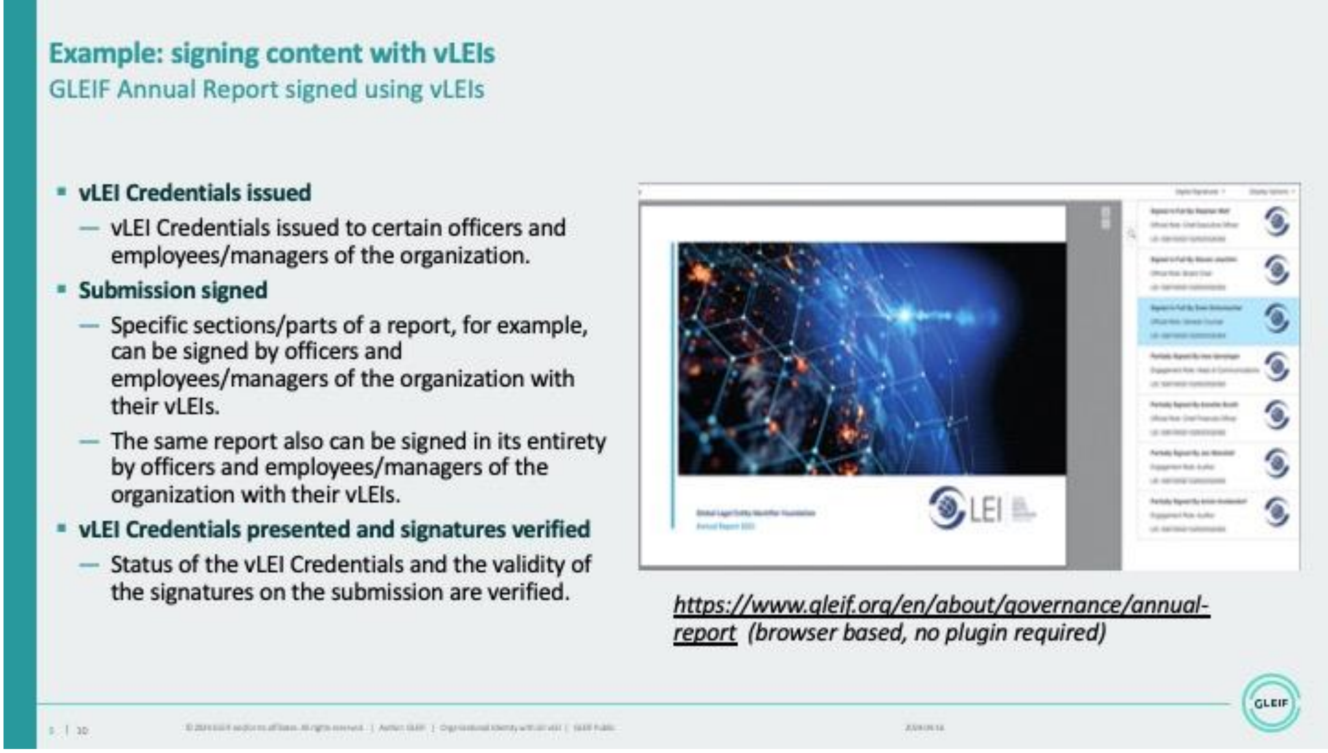
Reports/ Forms

vLEIs using CESR

Financial Messages

Report/Taxonomy Packages

* Using CESR (Composable Event Streaming Representation)

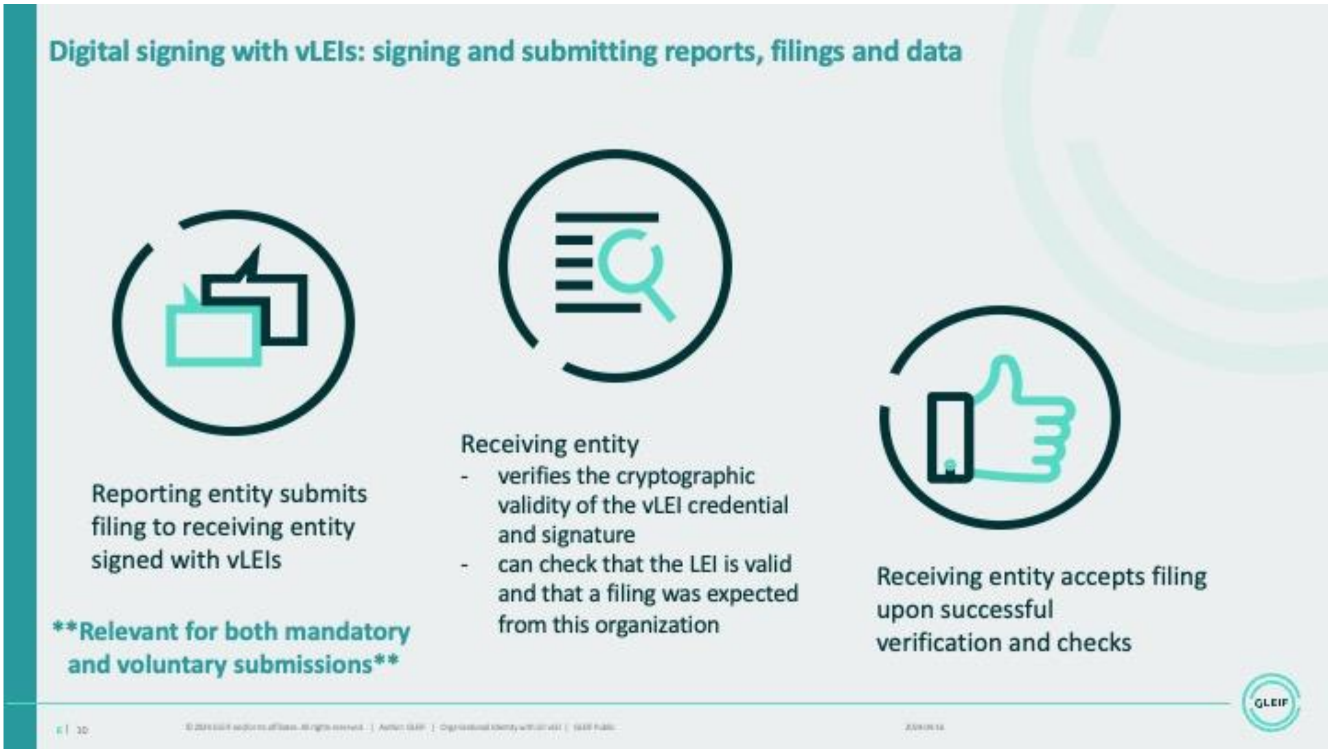


Example: signing content with vLEIs

GLEIF Annual Report signed using vLEIs

- **vLEI Credentials issued**
  - vLEI Credentials issued to certain officers and employees/managers of the organization.
- **Submission signed**
  - Specific sections/parts of a report, for example, can be signed by officers and employees/managers of the organization with their vLEIs.
  - The same report also can be signed in its entirety by officers and employees/managers of the organization with their vLEIs.
- **vLEI Credentials presented and signatures verified**
  - Status of the vLEI Credentials and the validity of the signatures on the submission are verified.

https://www.gleif.org/en/about/governance/annual-report (browser based, no plugin required)



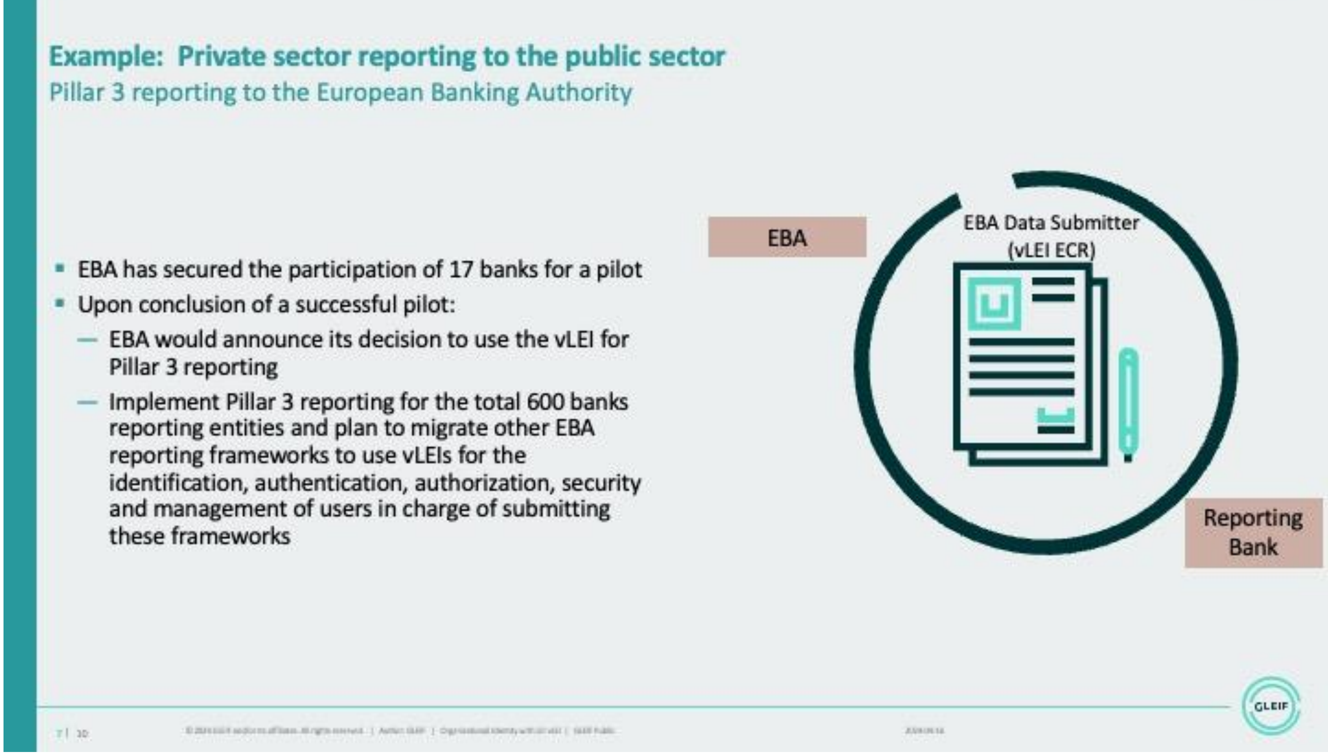
Digital signing with vLEIs: signing and submitting reports, filings and data

Reporting entity submits filing to receiving entity signed with vLEIs

****Relevant for both mandatory and voluntary submissions****

Receiving entity
- verifies the cryptographic validity of the vLEI credential and signature
- can check that the LEI is valid and that a filing was expected from this organization

Receiving entity accepts filing upon successful verification and checks



Example: Private sector reporting to the public sector

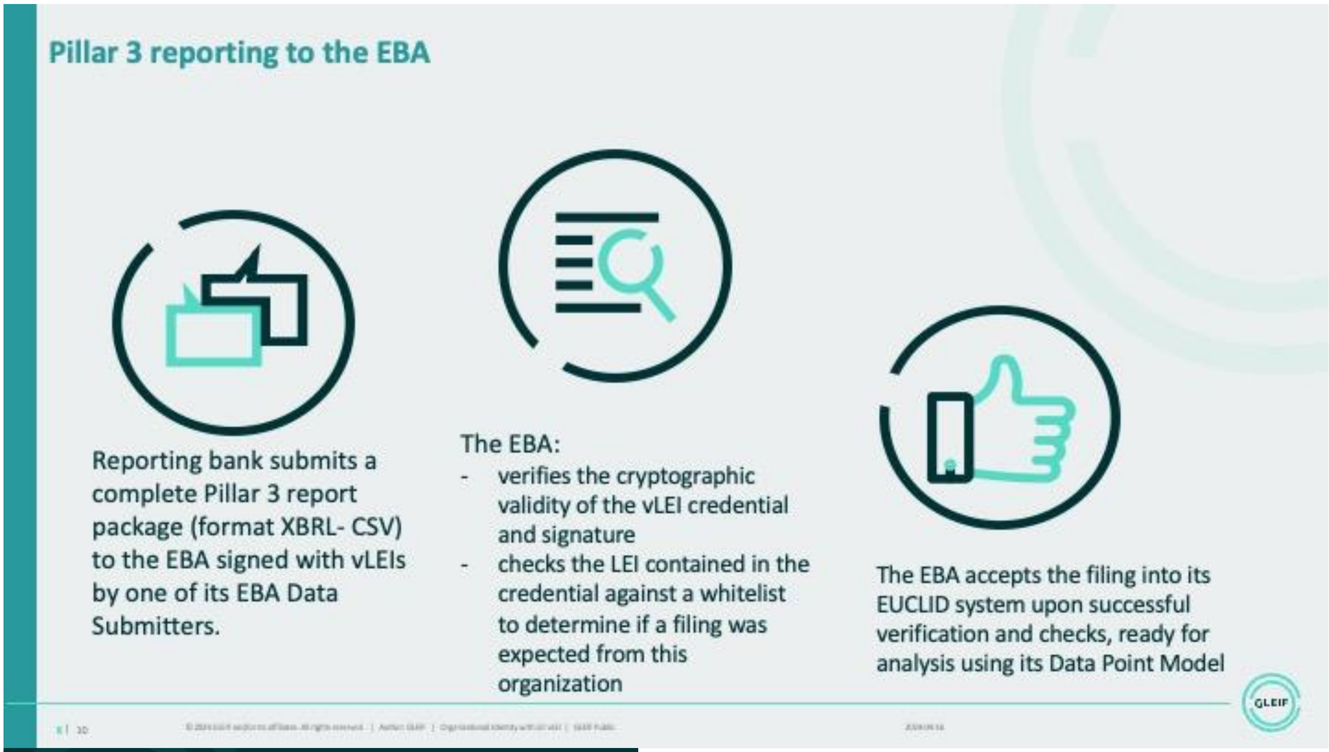
Pillar 3 reporting to the European Banking Authority

- EBA has secured the participation of 17 banks for a pilot
- Upon conclusion of a successful pilot:
  - EBA would announce its decision to use the vLEI for Pillar 3 reporting
  - Implement Pillar 3 reporting for the total 600 banks reporting entities and plan to migrate other EBA reporting frameworks to use vLEIs for the identification, authentication, authorization, security and management of users in charge of submitting these frameworks

EBA

EBA Data Submitter (vLEI ECR)

Reporting Bank



Pillar 3 reporting to the EBA

Reporting bank submits a complete Pillar 3 report package (format XBRL- CSV) to the EBA signed with vLEIs by one of its EBA Data Submitters.

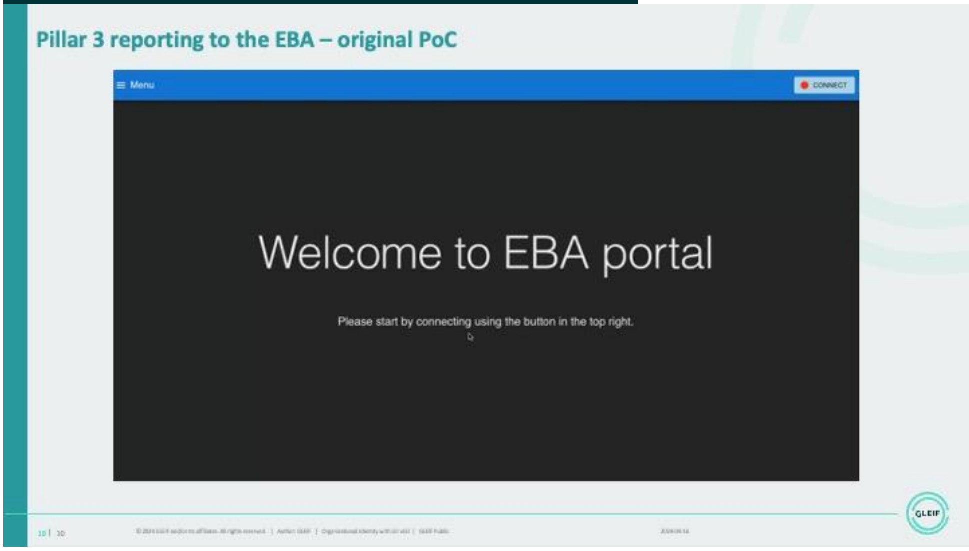
The EBA:

- verifies the cryptographic validity of the vLEI credential and signature
- checks the LEI contained in the credential against a whitelist to determine if a filing was expected from this organization

The EBA accepts the filing into its EUCLID system upon successful verification and checks, ready for analysis using its Data Point Model

GLEIF
Enabling global identity
Protecting digital trust

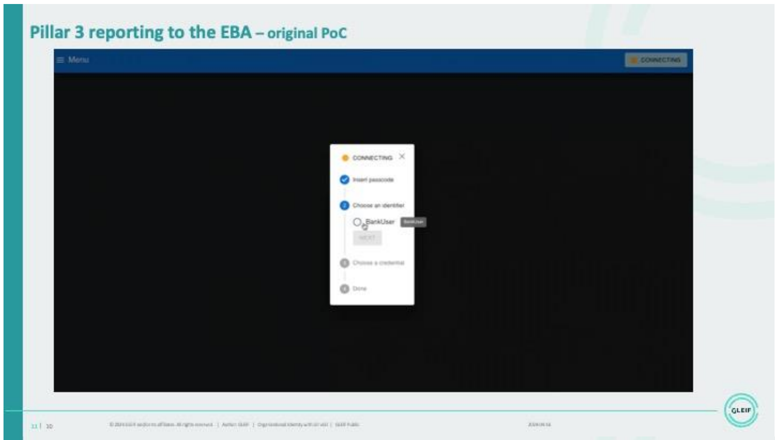
Technical View: Pillar 3 EBA Pilot



Pillar 3 reporting to the EBA – original PoC

Welcome to EBA portal

Please start by connecting using the button in the top right.

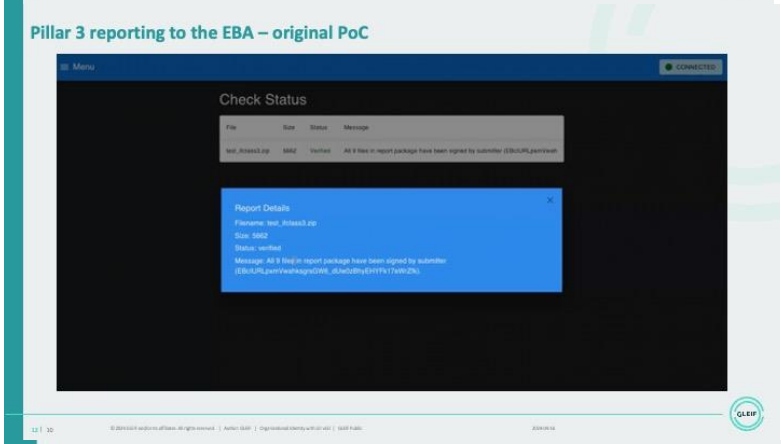


Pillar 3 reporting to the EBA – original PoC

11 | 30

© 2024 GLEIF and/or its affiliates. All rights reserved. | Author: GLEIF | Organizational identity with vLEI | GLEIF Public

2024-04-16



Pillar 3 reporting to the EBA – original PoC

Check Status

File	Size	Status	Message
test_ifclass3.zip	5662	Verified	All 9 files in report package have been signed by submitter (EBcIURLpxmVwah

Report Details

Filename: test_ifclass3.zip

Size: 5662

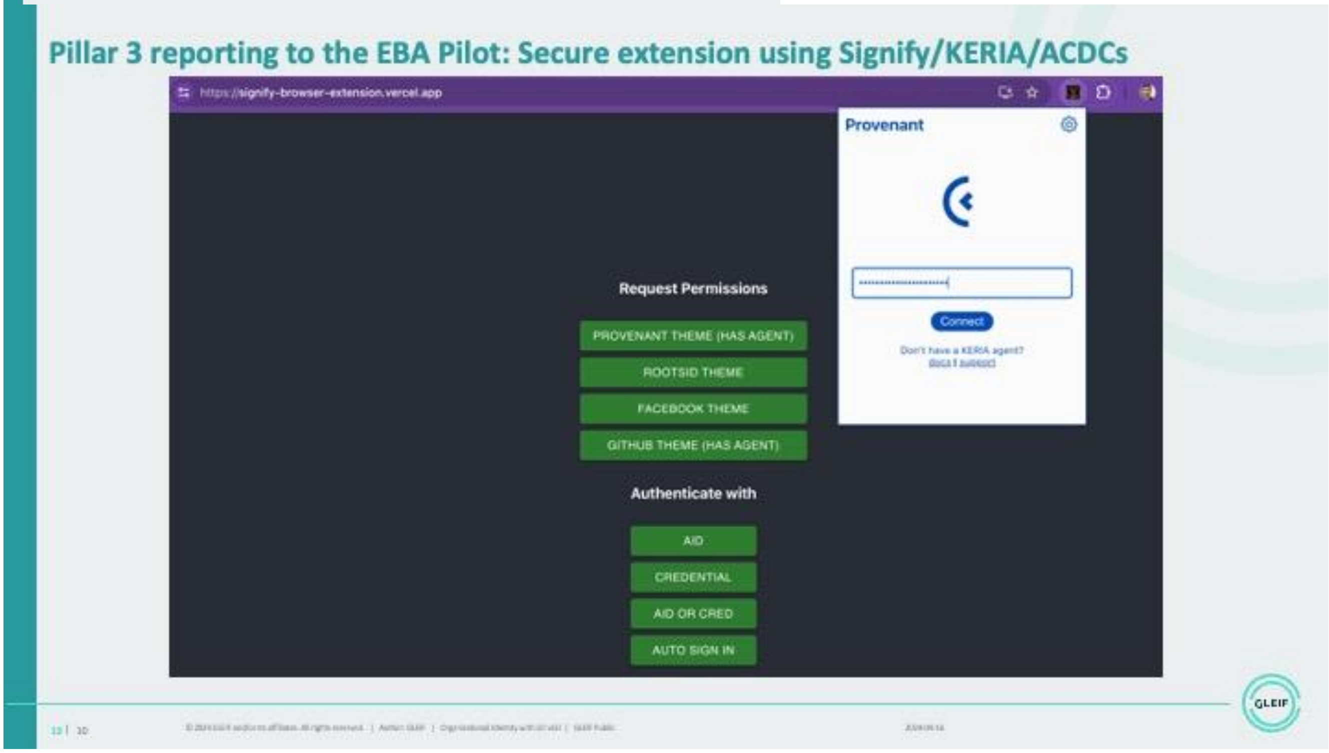
Status: verified

Message: All 9 file(s) in report package have been signed by submitter (EBcIURLpxmVwahksgnsGW6_dUw0zBhyEHYFk17eWrZlk)

12 | 30

© 2024 GLEIF and/or its affiliates. All rights reserved. | Author: GLEIF | Organizational identity with vLEI | GLEIF Public

2024-04-16

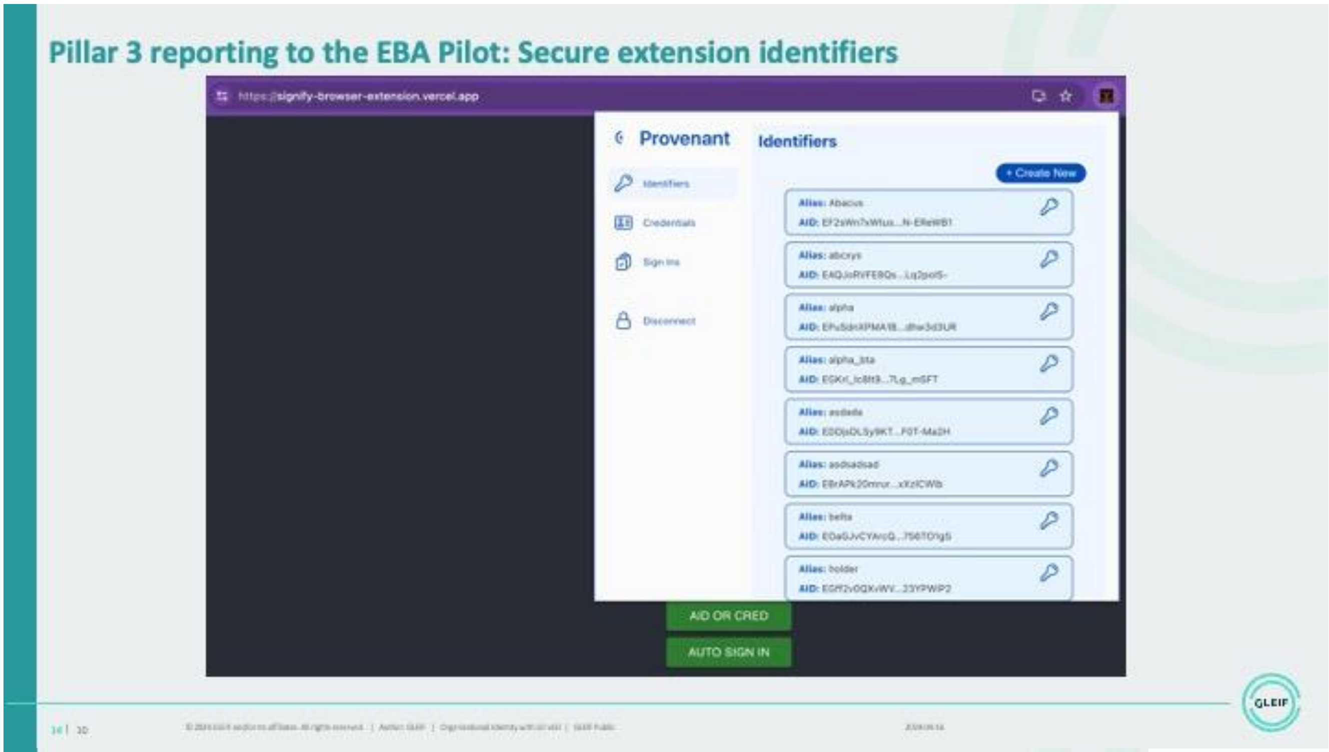


Pillar 3 reporting to the EBA Pilot: Secure extension using Signify/KERIA/ACDCs

13 | 30

© 2024 GLEIF and/or its affiliates. All rights reserved. | Author: GLEIF | Organizational identity with vLEI | GLEIF Public

2024-04-16



Pillar 3 reporting to the EBA Pilot: Secure extension identifiers

Identifiers

Alias: Abacus
AID: EF2sWn7xWtus...N-EReWB1

Alias: abcxys
AID: EAQJoRVFE8Qs...Lq2poI5-

Alias: alpha
AID: EPuSdnXPMA18...dhe3d3UR

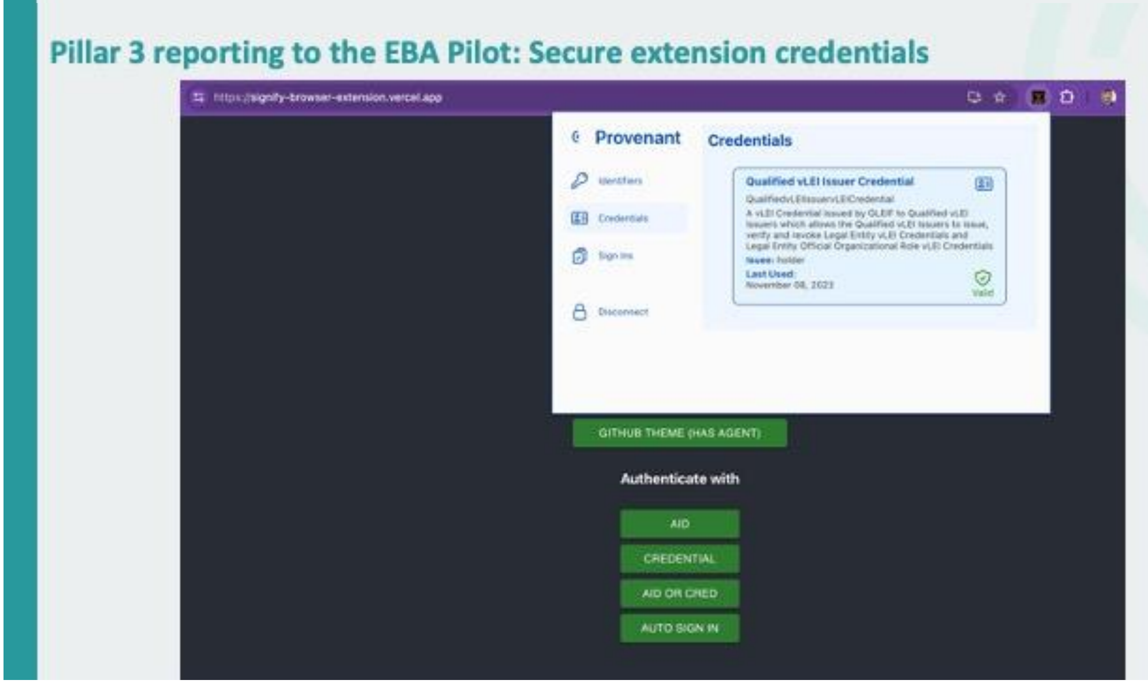
Alias: alpha_bta
AID: EGKrl_lc8lt9...7Lg_mSFT

Alias: asdada
AID: EDDjsDLSy9KT...F0T-Ma2H

Alias: asdsadsad
AID: EBrAPk20mrur...xXzlCWb

Alias: belta
AID: EOaGJvCYArcQ...756TO1g5

Alias: holder
AID: EGff2v0QKvWV...23YPWP2

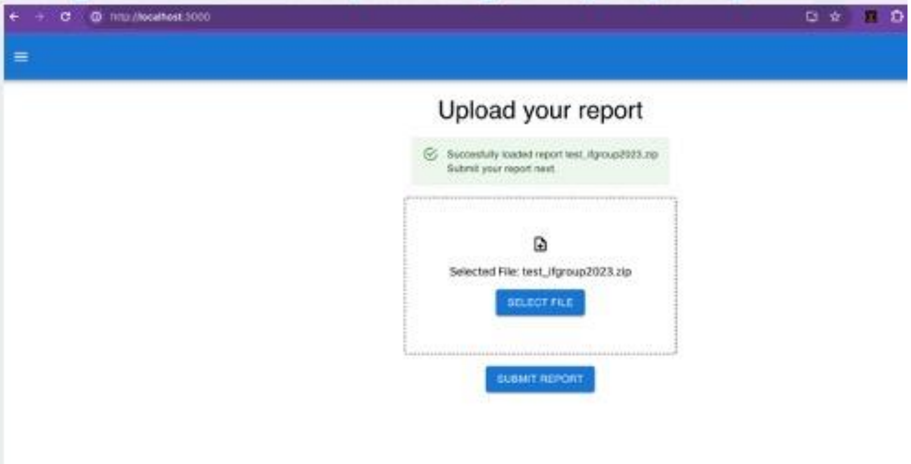


Pillar 3 reporting to the EBA Pilot: Secure extension credentials

Credentials

Qualified vLEI Issuer Credential
QualifiedvLEIIssuervLEICredential
A vLEI Credential issued by GLEIF to Qualified vLEI Issuers which allows the Qualified vLEI Issuers to issue, verify and revoke Legal Entity vLEI Credentials and Legal Entity Official Organizational Role vLEI Credentials
Issuee: holder
Last Used:
November 08, 2023
Valid

Pillar 3 reporting to the EBA Pilot: Upload a signed report package

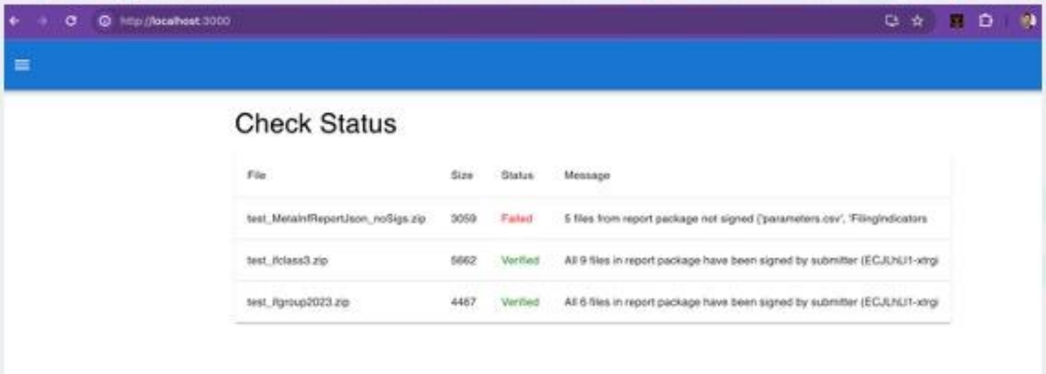


Upload your report

Successfully loaded report test_ifgroup2023.zip
Submit your report next

Selected File: test_ifgroup2023.zip

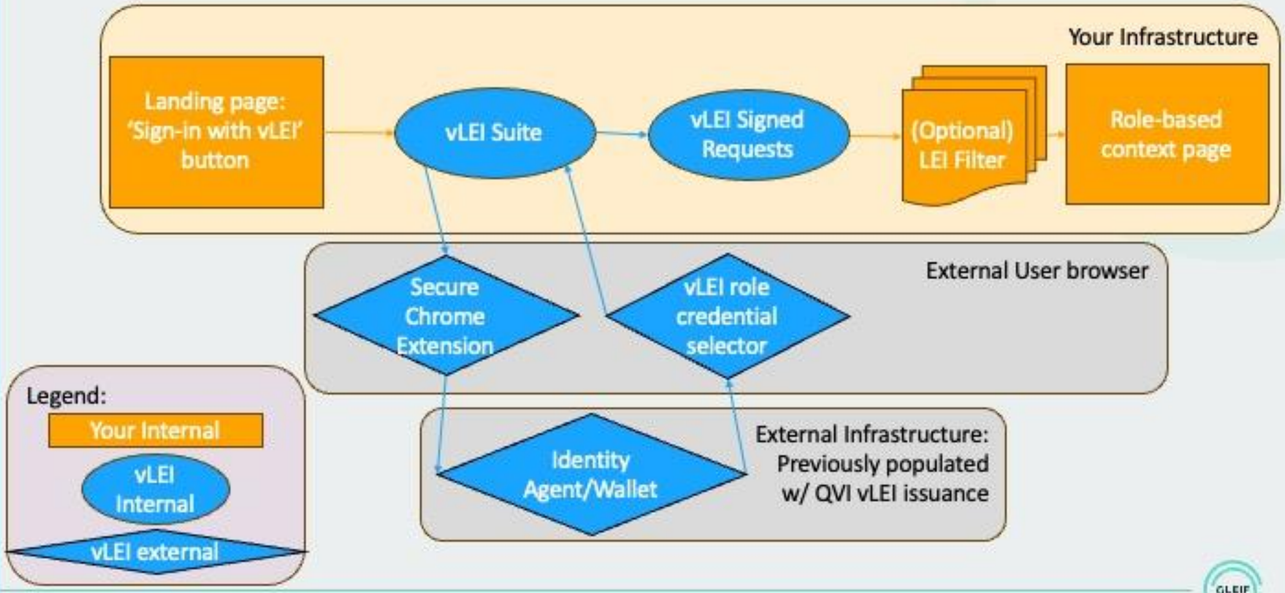
Pillar 3 reporting to the EBA Pilot: Check the status of your submitted report packages

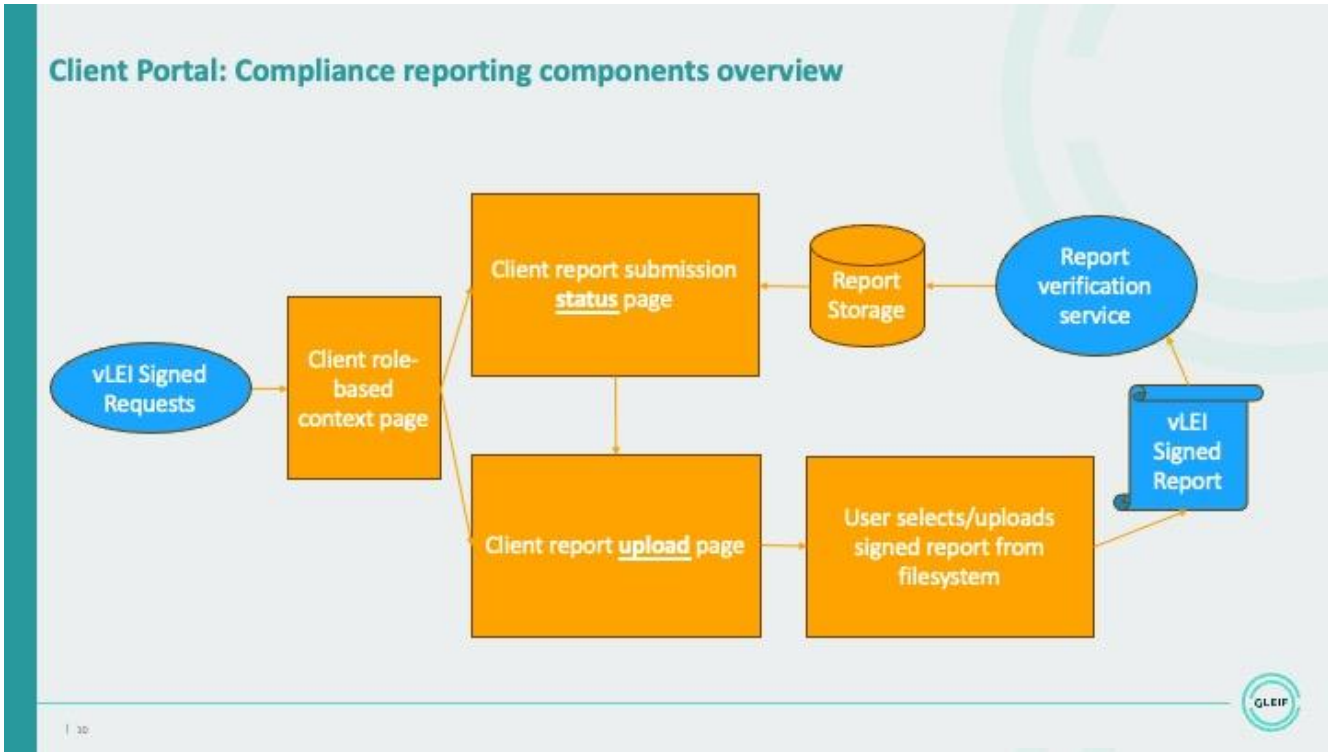


Check Status

File	Size	Status	Message
test_MetaInfReportJson_noSigs.zip	3059	Failed	5 files from report package not signed ('parameters.csv', 'FilingIndicators
test_ifclass3.zip	5662	Verified	All 9 files in report package have been signed by submitter (ECJLhLI1-xtrgi
test_ifgroup2023.zip	4467	Verified	All 6 files in report package have been signed by submitter (ECJLhLI1-xtrgi

Your Portal: Authentication overview diagram





Client Portal: Compliance reporting components overview

vLEI Signed Requests

Client role-based context page

Client report submission **status** page

Client report **upload** page

Report Storage

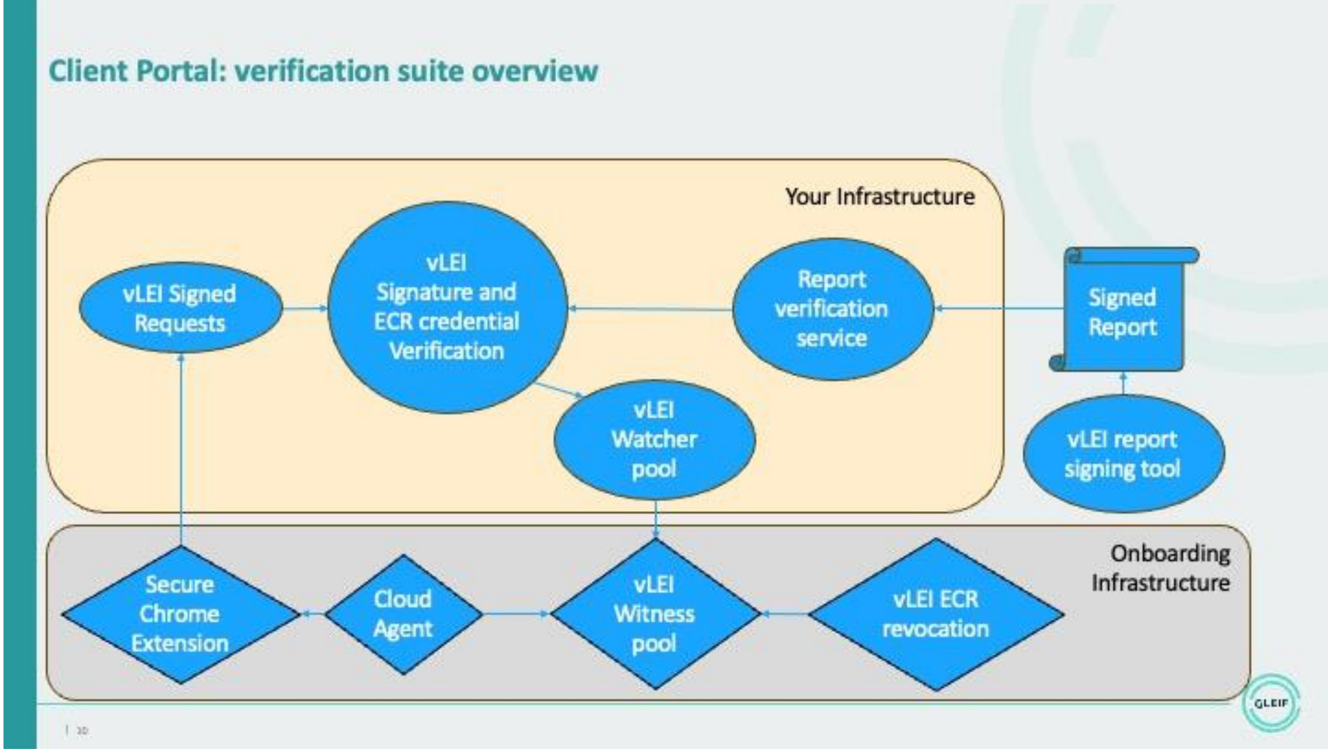
Report verification service

vLEI Signed Report

User selects/uploads signed report from filesystem

GLEIF

| 30



Client Portal: verification suite overview

Your Infrastructure

vLEI Signed Requests

vLEI Signature and ECR credential Verification

Report verification service

vLEI Watcher pool

Signed Report

vLEI report signing tool

Onboarding Infrastructure

Secure Chrome Extension

Cloud Agent

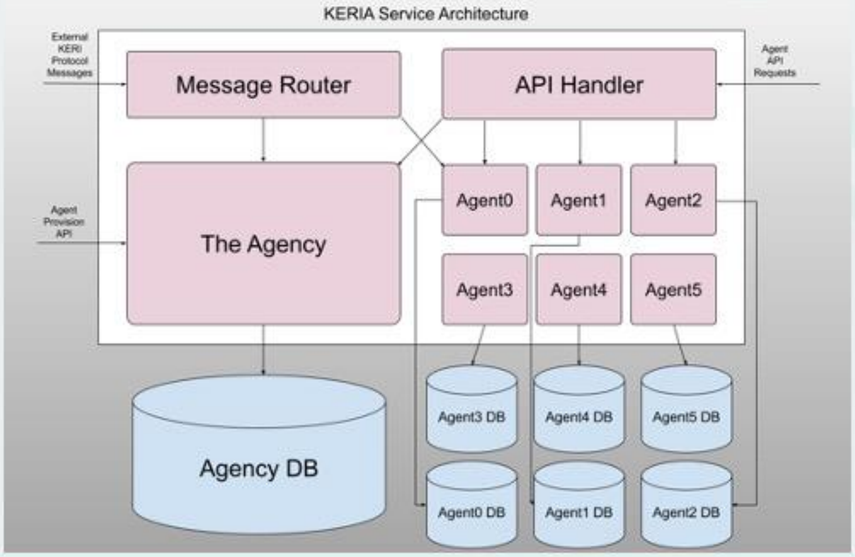
vLEI Witness pool

vLEI ECR revocation

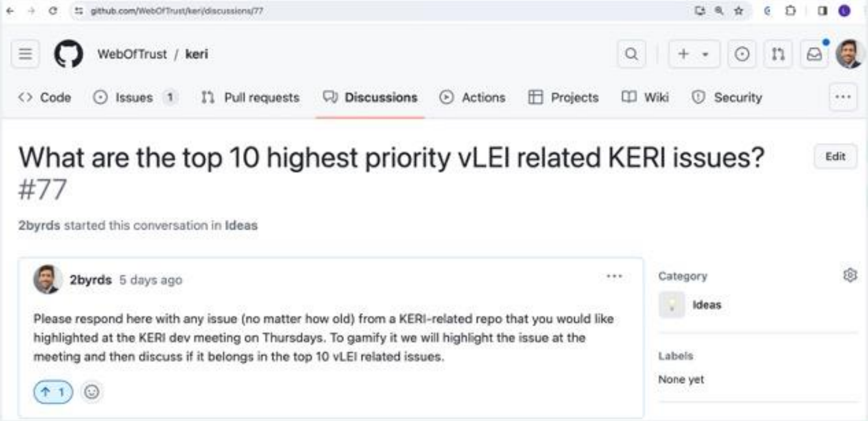
GLEIF

| 30

KERI community: verification suite overview using KERIA



KERI community meetings: vLEI Top 10 Issues



What are the top 10 highest priority vLEI related KERI issues? #77

2byrds started this conversation in Ideas

2byrds 5 days ago

Please respond here with any issue (no matter how old) from a KERI-related repo that you would like highlighted at the KERI dev meeting on Thursdays. To gamify it we will highlight the issue at the meeting and then discuss if it belongs in the top 10 vLEI related issues.

↑ 1

Category: Ideas

Labels: None yet

Limitations

- This presentation contains confidential and proprietary information and/or trade secrets of the Global Legal Entity Identifier Foundation (GLEIF) and/or its affiliates, and is not to be published, reproduced, copied, or disclosed without the express written consent of Global Legal Entity Identifier Foundation.
- Global Legal Entity Identifier Foundation, the Global Legal Entity Identifier Foundation logo are service marks of Global Legal Entity Identifier Foundation.

Authorization 101 - Intro to authorization concepts

Session Convener: Steve Venema
Session Notes Taker(s): he Rohit Khare

Tags / links to resources / technology discussed, related to this session:

Steve Venema's slides from the presentation
Google Photos album of slides
Cross-references from AuthZ meetup notes
Authorized Social & Unauthorized Unconference at IIW in April 2024

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

[[Rohit Khare: I loved the phrase "It's turtles all the way *up*!" as an explanation that there can be policies about who can join a group or be assigned an attribute; or a policy about who can administer policies; and so on.]]

Q: Explain more about the databases in your diagram for Attribute Store and Policy Store?

A: Oh yeah, so there was an attribute store and a policy store. So, the attribute store would typically be how your identity system lists users and those attributes with each user, either in that directory system or be passed by that system. So, it could be, for example, an LDAP directory.

So that's one side and then the other side is the actual policy. Statements, which are in some language. Um, those have to live somewhere and managed by the policy Administration. Access by the policy decision.

Q: Can you replace that database with a verified credentials.

A: Well, How Dynamic are the attributes? You typically think of verifiable credentials as a little bit longer lifetime. Now, there are situations where you can issue very quickly and have an ephemeral token lifetime.

[[Omri Gazitt: I loved using the term "Pre-authorization" to describe the practice of the AuthN ceremony embedding scopes in an access token, which the RP uses as "precomputed authorization". Also the callout to Vittorio's blog post explaining why this is a bad practice!]]

PDF - What to do about them?

Session Convener: No Name
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

Syper Persuasive Bots (NOT) Without using pseudonymity

Session Convener: No Name
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

SD - JWT (SD-JWTVC & SD-JWT VCDM)

Session Convener: Kristina & Oliver
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

SD-JWT, SD-JWT VC, SD-JWT VCDM

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

materials used are here:
https://drive.google.com/file/d/13AOxOp_eijY9UB_J32sSYKE68ZljC0L8/view?usp=sharing

**POKE HOLES * In our knowledge based authentication method.*

Session Convener: Matthew Vogel - Center Identity
Session Notes Taker(s): Matthew Vogel

Tags / links to resources / technology discussed, related to this session:
https://centeridentity.com/identity?api_key=MEQCIC7ADPLI3VPDNpQPaXAeB8gUk2LrvZDJIdEg9C12dj5PAiB61Te/sen1D++EJAcgnGLH4iq7HTZHv/FNByuvu4PrrA==&next=/authenticate&mode=auth&stage=signin

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

During the meeting, we discussed the implementation of secret locations selected on Google Maps and the use of AI to vet hints for these locations. We compared this method to the traditional use of standard passwords. Additionally, we explored various strengths and potential weaknesses of this approach.

Concerns about social engineering, the memorability of locations, and possible technical workarounds were among the top issues raised.

One participant suggested contacting a university to conduct an official experiment with a large group of participants, aiming to reach a definitive conclusion about the efficacy of this method.

Where Am I? How did I get here?

Session Convener: Jeff Orgel
Session Notes Taker(s): Jeff Orgel

Tags / links to resources / technology discussed, related to this session:

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps: **From @0 to @1 – Human Identity Extension Onto An Extra Worldly Realm**

For decades I have witnessed and participated in the Human Experience (HX) of human presence being extended into a realm of 0's & 1's via connected systems.

These definitions apply to the following review.

@0 *- this refers to human experience before the natural world had connected & social technology systems.*

***@1** - this refers to human experience after the natural world had connected systems. This is the sun-rising of connected system technologies into daily life: when and how this arrives is very idiosyncratic to each individual.*

From @0 to @1 - Extension from Real World/Human eXperience (RW/HX) <u>ONTO</u> Digital Landscape (DL)

In the natural world (**@0**), people are designed to occupy a world of convergent forces: hot-cold, wet-dry, light-dark. The intellect in play exists in the sentient creatures – not one bit in the environment they exist in. Perfectly able and intelligent creatures are designed with capability responsive to the real-world sensor package they were born with. This sensor package allows them to discern what is happening around them. The better they could assess the challenge-scape of moment-to-moment circumstances, the more likely they would survive.

On the digital landscape (**@1**) the human animal occupies a realm of intellectual design where nothing (two words - NO THING) is naturally occurring. Everything (two words again – EVERY THING) is designed by intellect. Further it is designed by us. Who knows how to game us better than ourselves?! Who knows how to exploit human vulnerabilities of voyeurism, self-aggrandisement, sex, power, “free” and on it goes - better than us?! It shows…

The discordance occurring around this fact is extraordinary. Perfectly able and intelligent creatures from the physical world of **@0** are hobbled by not having a sensor package equivalents like smell, touch, gut intuition to discern what is happening around them in **@1**. The **@1** environment around them is immature, if not plain malicious, at being clear as to use of caution, implications of presence in such a framework and delivering trust.

This presentation was designed to put handles on thoughts with words regarding awareness of this interplay. It will also work towards identifying that people are trying to bridge these realms without clarity on the transitional, translational and symbiotic connections they will meet with in use of these systems.

The portion of human intellect which is occurring in people is unique for the above-mentioned reasons. I am calling that intellectual layer of understanding and management the HumanOS^{Ô}.

Our Sessions covered ideas such as;

- Plato’s Allegory of the Cave – what we see on the wall vs what the wall sees of us (AK)

- Bi-directional interplay between Real World & Digital Landscape

- Framework structure: visual models (linear vs. stack model)

- Understanding the idea of building a Digital Twin from awareness of the implications of those ***Real-IT*** ® relationships – ***the relationship we chose to have, or not have, with connected technology systems***. This profile was identified as a variation of a Voo Doo Doll we make of ourselves.

- Identifying the impact of ***Real-IT*** ® choices, and reflection into, a person's reality

- Concepts of managing system forces "in the room" including social media, data collection and predation such that a person's intention is manifested with minimum to no risk of hazard or harm.

- Explored: Can we exist without identifiable presence? Can we be present without existing? The phrase "being in a place" where there is no actual "place" (BC)

Examples of Connected Social Systems (CSS) would be; Social Networks like Facebook, TikTok, Instagram, WhatsApp; Legal Records like State & Federal: Tax Filing, Personal Property Tax, Real Estate Tax, License Bureau; Knowledge & Discovery (YouTube search, etc.)

Operation on the DL (Digital Landscape): Extension eXperience (EX) occurs @2 >< @3 >< @4 creating feedback from EX INTO Real World RW/HX

@2* - **Real-IT** ®: understanding the presence of the relationship with technology as a symbiotic aspect/element in daily life to one degree or another. @2 is the layer where RW (Real World) & DL (Digital Landscape) are ever iterating. This is a critical layer.

@3 - **YouDoo Doll** - here you craft your VooDoo Doll (aka You Do Dollä): crafting (more or less so) of S.A.M. (Same As Me) This is where Real-IT® awareness meets with a variation of the martial art Aikido on the Digital Landscape. I call this Real-ITdoä. This is the idea that we are managing forces we often aren't in control of, or even aware of.

@4 - **YouX**: How is the Real-IT Yin Yang going? UI & UX experience feedback back returns to HX/RW more or less aligned with your intended outcomes (hope, expectation, trust)? Assess and go to @2 and iterate.

Presenting the same session once each day (an ***IIW Triple Play***) allowed for the following significant benefits;

- maximum opportunity for attendees to attend with minimum session conflicts regarding other valued sessions

- scaffolding refinement each day which elevated the model for the next day's attendees

- likely 3X the number of attendees during the particular IIW event

- great for advancing the pace of developing evolving edge space models as there is evolution at a higher rate since each day-group contributes to a revision one day after the next. IIW.38 r1, IIW.38 r2 IIW.38 r3

Other Notes regarding a ***IIW Triple Play***;

- calls for some presentation durability as it is an effort in triplicate

- reduces opportunities to attend one other session each day

Local First / SSI Fediverse UpDates Notes from the Field

Session Convener: Dmitri Zagidulin
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

Simple SSI - Attractive, intuitive, and easy-to-use SSI code for developers

Session Convener: Jonathan Rayback
Session Notes Taker(s): Jonathan Rayback

Tags / links to resources / technology discussed, related to this session:

https://drive.google.com/file/d/1EgVSJhV3wF52GAuDtxP9VzhEYXI8b1rY/

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

See slides: https://drive.google.com/file/d/1EgVSJhV3wF52GAuDtxP9VzhEYXI8b1rY/

Conclusion of group discussion was that smaller, more composable libraries are needed within the SSO ecosystem. Perhaps something like this might be an effort taken up by one of the foundations…

Provenance in an ML World

Session Convener: Matt Miller
Session Notes Taker(s): Eric Scouten & Tchaikawsky “Troy” Samuels

Tags / links to resources / technology discussed, related to this session:

Project to embed digital signature + DNS into media file header:
https://github.com/danielquinn/aletheia

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

Notes copied from Session 3M: Provenance in a ML World:

Discussion about image theft and appropriation of identity.
"Overwhelm with the positive (trust signal); ignore the negative."

Discussion about how to have trust in anonymous or pseudonymous content.
Some misconceptions I observed:

- There's a binary distinction between human and generative content. (Where does gen fill fit in?)
- There's a binary distinction between edited and unedited content. (What about photographer's/videographer's choice of what to include in the frame?)
- There's a binary decision to make: trust or not trust. But trust is on a spectrum from closest friend to barbershop hearsay.

"I think you just said it sucks to have to make our own (trust) decisions."

Alethia combines signature with DNS.
TurnItIn anti-plagiarism tool used in academia.

Troy:
How do we get the framework to work seamlessly with existing processes?
How do you verify its from the BBC vs. Not a fringe content creator or bot?
How does it also work in a way that has true meaning.
- Things like the padlock which isn’t shown in browsers anymore have lost the meaning they intended to communicate.
Standards, combining a signature and a DNS.
How can it be further tied to content?
Social FI Friend.Tech or XCAD.Social
2 issues, Provenance vs Reputation and Proof-of-source, Validate the originator/editor of a piece of media.
What comes from a machine vs a human?
More notes due.. Other devices died mid session.

The DEI Backlash & the Identity Profession

Session Convener: Heather Flanagan
Session Notes Taker(s): Elizabeth Garber

Tags / links to resources / technology discussed, related to this session:

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

Every year IDPro does a skills survey and collects a lot of data about identity practitioners - challenges, skills, demographics. At EIC in June, IDPro is going to do a workshop about the identity profession with a lens on diversity.

Thing 1: what are we seeing on the skills survey. The industry is top heavy, senior people rather than junior people. Limited junior level jobs. (It's possible that the respondents are self selecting)

Identity is too important to get wrong so hiring managers want experience… but this means young people may not be at the table.

Thing 2: Gen Z (and general cultural) backlash against DEI. Zero sum thinking. Feeling exclusion and pushing back. Political climate makes it feel more acceptable to be hostile to DEI.

IIW - all technical people. We are missing governance, policy, human components. OIX paper shows that the view of our industry from relying parties is "all I see is technical folks arguing about standards" Tech heavy as well as top heavy

Planning the session…
Are you looking to be controversial? A little bit, yeah…. But don't want to really

How do you get people to see that it's not a zero sum game. Debated whether you could argue it is zero sum. Lots of conversations with white men who feel that they are being excluded and marginalized. How do you make them feel heard to create pathways for change? So much power is still concentrated in that community however.

Diversity of thought is incredibly important. In the early days of the dotcom boom we were all better off for the diversity of degrees (not all computer science) innovating.

Is it an argument that needs to be had? In the midst of uncertainty, erosion of the American dream, people are struggling. Resentment is natural. It's probably only structural things that will fix it..perhaps this is cyclical and generational.

The markets will drive more success in this space. Maybe we need to re-frame the conversation as not trying to change minds and stop zero sum thinking but more about the argument for diversity in all its forms. So why does diversity lead to better outcomes.

The term DEI is being used as a slur in right wing circles. It's being used to devalue and demonize… the term itself might not have a bright future. Should we discuss the re-branding of our talk? Of the interventions themselves?

Spheres with their own power structures - all would require some form of intervention.
-Government
-Organizational
-Personal
- would also add cultural sphere

In the talk, we should discuss practical things that people can go bring into their organizations

Practical things inside orgs:

- Don't make minority group members to do the work of DEI
- Listen more than you talk

Example from transportation industry:
-Tried to improve hiring practices but realized that the internship program was causing the dynamic by only selecting top tier students from top tier schools
-Spend time together outside of work to breed inclusivity
-Inclusion has to be a value in order to unlock the benefits of diversity

How does an organization do this and how do we do this at an industry level? How can you as a hiring manager (since it is a top-heavy industry)?

How does our language of identity open or close doors for new entrants?

At EIC we think we're going to:
-Establish that DEI is important
-Include a debate
-Talk about practical ideas for organizations
-Talk about interventions at industry level - not dependent on organizational hiring / individual line manager practices. Things we can do to fill their pipelines

SESSION #4

WIGG Digital Credentials API

Session Convener: Lee Campbell, Sam Curren & Tim
Session Notes Taker(s):

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

No Notes Submitted

FIDO 101 and Passkeys - an IIW 101 Session

Session Convener: John Bardley
Session Notes Taker(s):

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

No Notes Submitted

OpenID AuthZEN: 0 to interop in 6 Months!

Session Convener: Omri Gazitt
Session Notes Taker(s): Omri

Tags / links to resources / technology discussed, related to this session:

- Omri's Slide deck
- Interop website
- Cross-references from AuthZ meetup notes

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

- Interop scenario: Todo app
- Interop payload document
- Results page - 4 interoperable implementations, and counting!
- Getting to interop in less than 6 months required adhering to KISS (Keep it simple, stupid!)

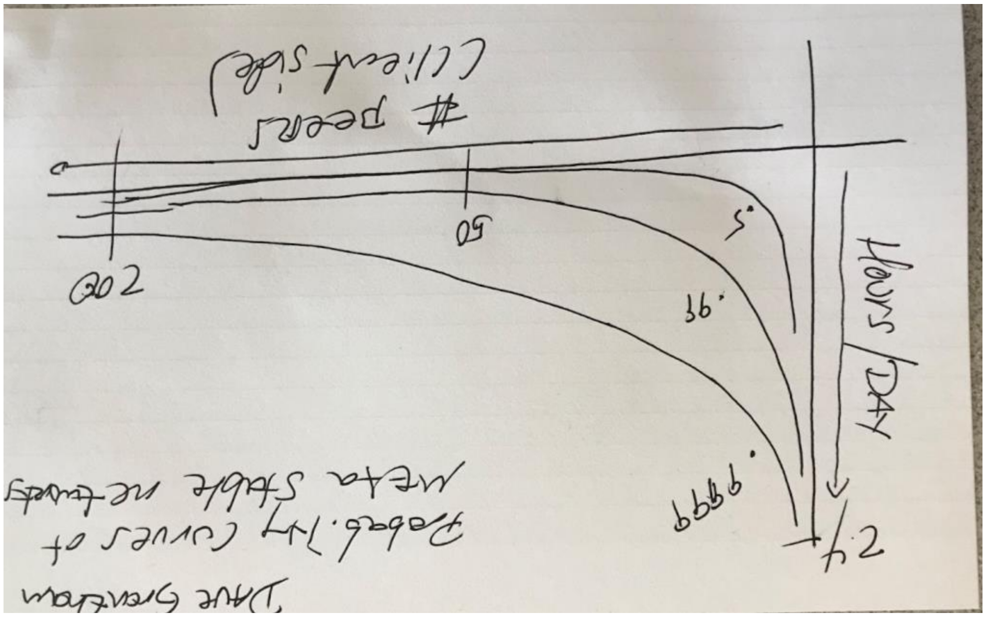
Latest Research in Metastable Networks - How did we get the web but NOT the web of trust?

Session Convener: Dave Grantham | https://www.linkedin.com/in/david-grantham-87207a265/
(formerly Huseby - cool story about how he took back his father's given surname just before his Dad died earlier this year)
Session Notes Taker(s): Cam Geer | https://www.linkedin.com/in/camgeer/

Tags / links to resources / technology discussed, related to this session:
https://github.com/cryptidtech/
https://www.cryptid.tech/

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

- Peer Behavior
  - connect / disconnect randomly (in time)
  - change IP randomly (in space / location)
  - change firewall status randomly
- Avg behavior of a peer
- Unit of time (Epoch)
  - research chose 24 hours as a
- A peer's behaviour determined to be average
  - ex. phones - 4 hours / day]
- 2 nodes live and running anf chaning packets
- sum of binomial curves
- Avg number _ same average number of contributors to an open source project



Graph

- y-Axis
  - hours / day
  - 24 hours
- x-Axis
  - # client side peers
  - ~ 200 - to all ways
  - Client Peers that you have an identifier for that I can send a message to

- Joe Andrieu
  - DNS helped to create the web because of centralized Authority
  - Web of Trust failed
    - because "Trust" is the wrong word
    - What people mean is verifiability with a high degree of certainty
- Cam Geer
  - Trust is a human emotion that is not quantifiable
  - Trust is informed as a function of time
- Reza
  - Internet was create asymmetrically

Example

---

did:key:a132fb....
Possible Link States

URL	PubKey
• valid > • https://www.amazon.com/some/thing/you/don't/need	• valid
• invalid Example Amazon 404 error	• invalid
• partially valid identifier ○ Go back to: ○ https://www.amazon.com/ and then do a search	

Asymetric Time Domain in Your Identifier
A Identifier lives less than (<<) **B**
A system that trends toward "THE" network.
large enough pool of entropy yet with a cryptographic commitment

Accumulation of all events identity, authentication

- cryptographically verifiable key history

fully programmable
Hash linked data structure not rpovledged storage

Log is append only
how append dine is lock and unlock scripts

next event in log

- signed by threshold key
- signed by pub key
- allows two entries to compete for the same sequence number in the provenance log

p.log

- entry 0 - previous point of Null
- lock
- unlock
- CID (content address)
    - first lock
- VLAD
    - very long lived address
    - digital signature over the CID of the first lock scriot
- VLAD: sig (CID)
- ephemeral key signs the entry in the provenance log
    - the private key is immediately

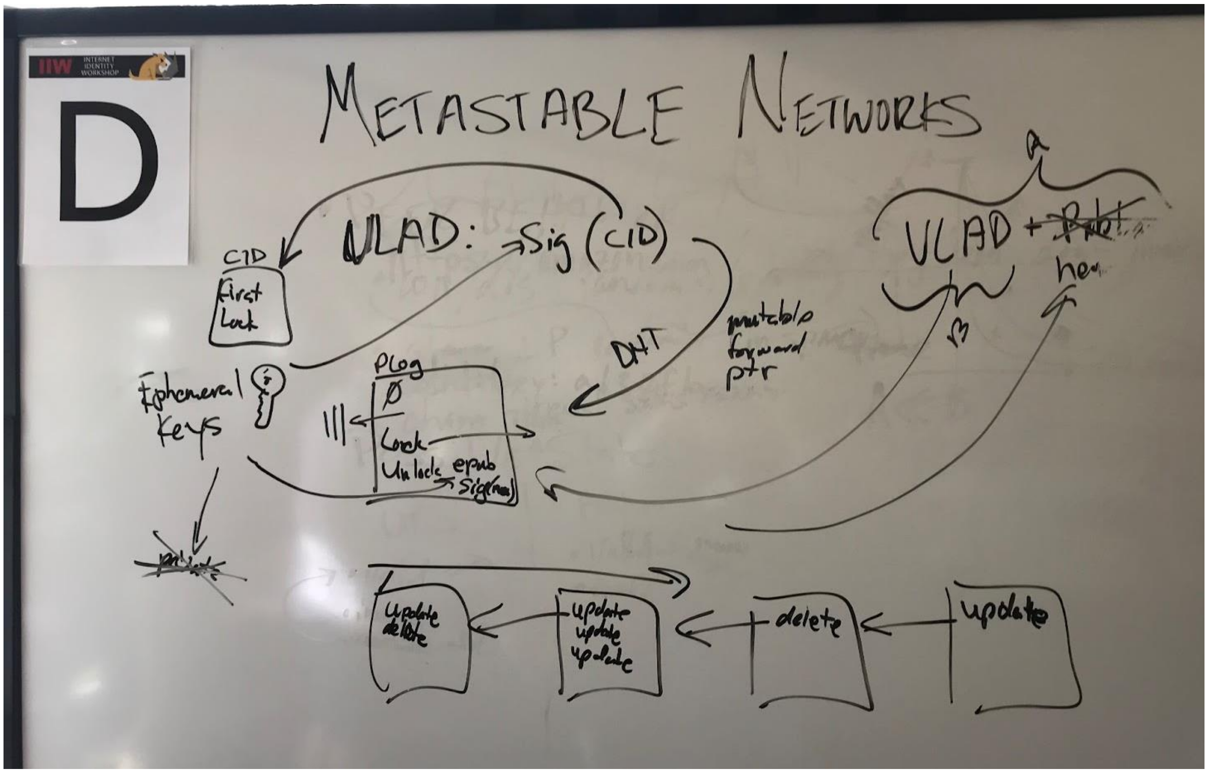
Dave G is proposing a New IPNS protocol

in P2P network there is no implied hierachy

Joe Andrieu > KERI does not solve the hard part.

events

- have an update or delete
- each event has a back link to the previous event



Joe Andrieu

- keep attributes & identifiers separately
- gave Dave Grantham a thumbs up

Product Name: **Better Sign**

Privacy Enhancing Mobile Credentials (PEMC) update

Session Convener: John Wunderlich
Session Notes Taker(s): John Wunderlich

Tags / links to resources / technology discussed, related to this session:

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

Link to deck:
https://docs.google.com/presentation/d/1r7-1wKoAjZXWGotAQlct6MqzhD8g6v-e/edit?usp=sharing&ouid=117540279191244887421&rtpof=true&sd=true

OpenIDIDComm

Session Convener: Sam Curren
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

OpenID, OpenID4VCI, OpenID4VP, DIDComm

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

We presented the work done by IDUnion that coordinates the OpenID4VC protocols with the creation of an associated DIDComm connection. We discussed the minimal additions required and showed the demo created by IDUnion to demonstrate the approach.

https://github.com/IDUnion/OpenIDIDComm

The work is under discussion for transfer to the DIF for further work.

An Intro to SSI - An IIW 101 Session

Session Convener: Limari Navarrete and Steve McCowen
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

Link to Intro to Presentation Slide Deck:
https://docs.google.com/presentation/d/1eTfLxCACvU7dYcDi6JrFVyruyOz2hEDO/edit?usp=sharing&ouid=112146186626842815936&rtpof=true&sd=true

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

Decentralized Storage and Bring Your Own Identity

Session Convener: Aaron Coburn
Session Notes Taker(s): Aaron Coburn

Tags / links to resources / technology discussed, related to this session:

https://solidproject.org/

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

This session provided a brief overview of the Solid project and the types of architectures that are made possible when storage, identity and application code are separated. In particular, this changes the economics of application development: apps are cheaper to build and require less infrastructure. This provides opportunities for portability while also introducing new challenges for data addressing.

There was a discussion of the current mechanisms for layering identity into this structure, in particular WebID with OpenID Connect, while also considering alternatives, such as key-based methods.

Empowerment Tech: the good, bad and ugly

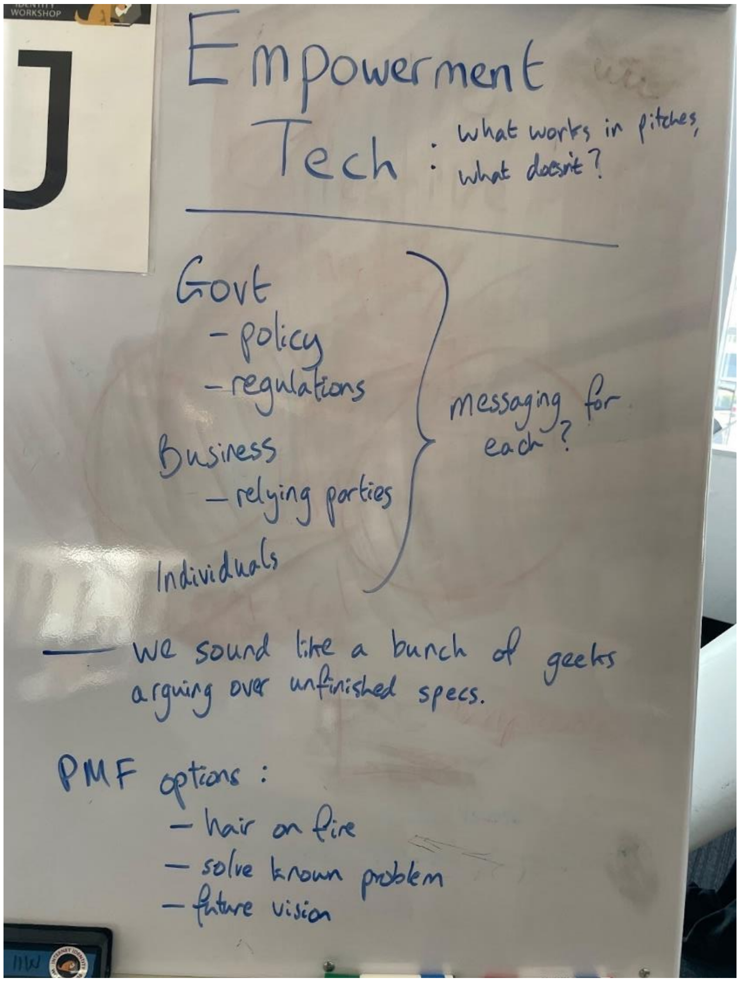
Session Convener: James Monaghan
Session Notes Taker(s): James Monaghan

Tags / links to resources / technology discussed, related to this session:

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

We talked about what goes well and what doesn't when discussing Empowerment Tech with potential buyers. This included a discussion about what we mean by "empowerment" and how much closer to the individual the balance of power should be, and what would be helpful when pitching it.

Photos of the whiteboard are below:



Empowerment Tech : what works in pitches, what doesn't?

Govt
- policy
- regulations

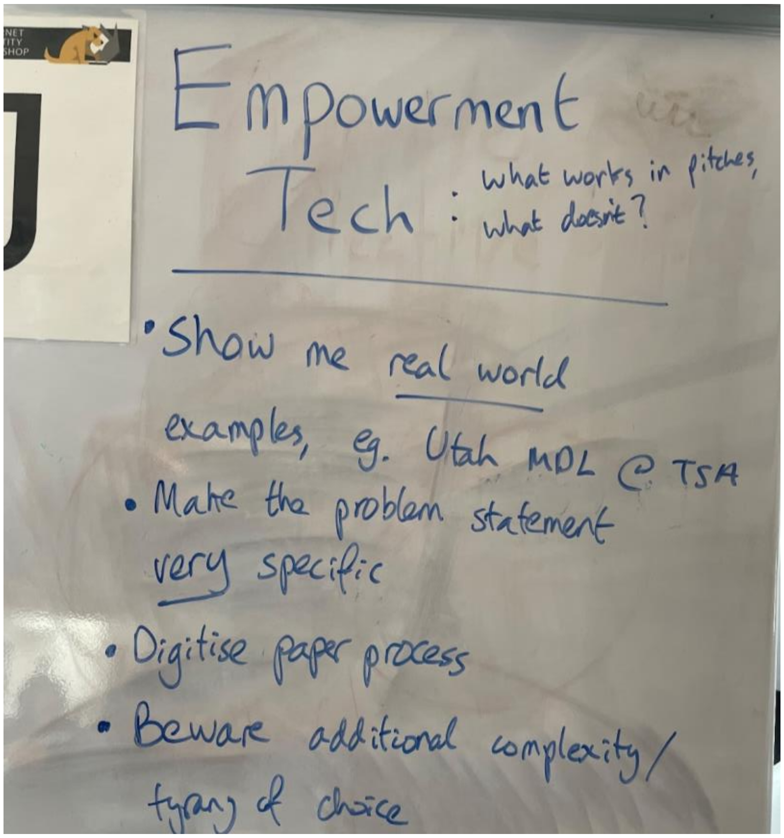
Business
- relying parties

Individuals

messaging for each?

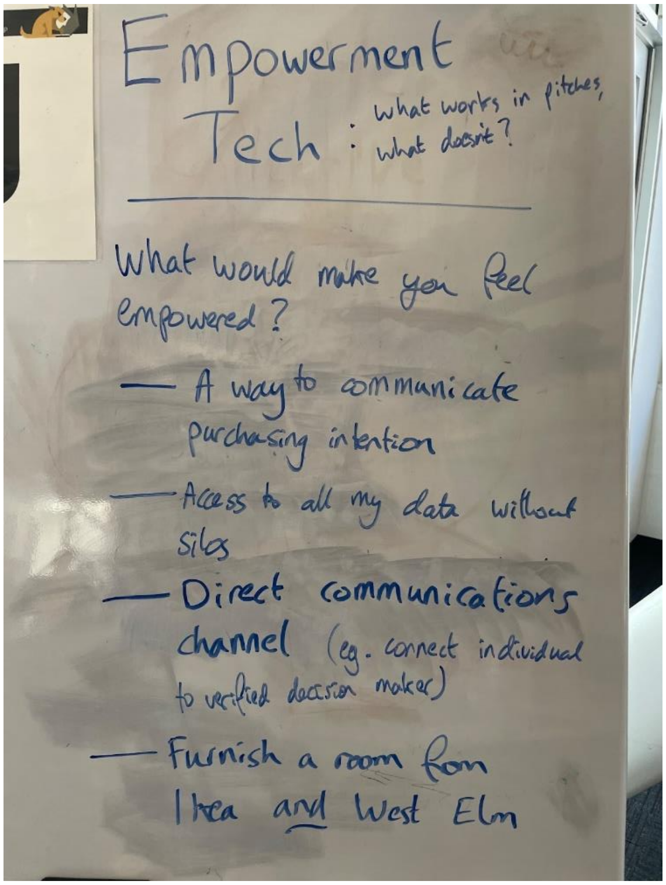
— we sound like a bunch of geeks arguing over unfinished specs.

PMF options :
- hair on fire
- solve known problem
- future vision



Empowerment Tech : what works in pitches, what doesn't?

- Show me real world examples, eg. Utah MDL @ TSA
- Make the problem statement very specific
- Digitise paper process
- Beware additional complexity/ tyrany of choice



Empowerment Tech : what works in pitches, what doesn't?

What would make you feel empowered?

— A way to communicate purchasing intention

— Access to all my data without silos

— Direct communications channel (eg. connect individual to verified decision maker)

— Furnish a room from Ikea and West Elm

Public verifiable data for websites, people, and organizations

Session Convener: Jan Christoph Ebersbach (JC) and Brian Richter
Session Notes Taker(s): Jan Christoph Ebersbach, amended by Samuel Rinnetmäki

Tags / links to resources / technology discussed, related to this session:

Presentation slides:
https://slidesdown.github.io/?slides=github.com/identinet/presentations/240417_IIW_linked-vp/SLIDES.md
DIF Linked Verifiable Presentation specification: https://identity.foundation/linked-vp/
identinet browser add-on for Chrome and Firefox that implements DIF linked-vp for websites: https://github.com/identinet/identinet-plugin

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

Feedback by participants:

- Software Bill of Materials is another potential use case that isn't mentioned in the slides.
- Public product data / product passports might not be the best use case for Linked Verifiable Presentations since the need for products to have a Decentralized Identifier (prerequisite for using the Linked Verifiable Presentation specification) isn't clear.
    - The presenters remarked that the verification of the business need for public verifiable data needs to be analysed on a case by case basis.
- A participant asked how Linked Verifiable Presentations are adding value beyond X.509 Extended Validation certificates (https://en.wikipedia.org/wiki/X.509#Extended_Validation_certificates) that are in use by organizations that require a high degree of trust, e.g. some bank.
    - The conversation turned into the direction of allowing third-party issuers to provide credentials to a holder who can combine multiple credentials with the Decentralized Identifizier and Verifiable Presentation approach. However, a clear business case was not established in the conversation.
- BC Gov's OrgBook was cited as a potential use case for Linked Verifiable Presentations https://orgbook.gov.bc.ca/
- Why use service endpoint and not a linked resource?
- An organization might want to have various Verifiable Presentations each including a set of logically linked credentials instead of just one VP containing all the company's credentials. The approach to have all credentials in a single VP is simpler (for example to the browser extension) but might not scale well.

Business of SSI and Authentic Data

Session Convener: Timothy Ruff
Session Notes Taker(s): Eric Scouten

Tags / links to resources / technology discussed, related to this session:

Authentic Data Economy
Session 4L: Business of SSI and Authentic Data Link to Timothy's slides: The Business of SSI.pptx

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

DTV founded in 2019 to launch new SSI businesses.
2022-2024 incubating more startups in health care, trade, securitization, and more.

Business model challenges:

- A use case isn't a business model.
- The tech is the easy part; making money is the hard part.
- Too focused on individuals. Re SSI: "We want this more for people than they want it for themselves."
- Get organizations on board, then the individuals will follow.
- Focused on identity at the expense of authentic *data.*
- Well-funded competitors and sensitive data.
- Web3, blockchain, etc. have a not-wonderful reputation in many circles. "It's lost it sizzle."
- The term "self-sovereign" causes allergic reactions esp. among governments.

Suggestions:

- Follow *Running Lean* by Ash Maurya (a student of Eric Rees)
- Look for problem-**solution** fit (not product-*market* fit)
- Read *The Mom Test*. (tl;dr: Everyone will lie to you even if they don't think they're lying to you. Work around this by asking about *existing* behavior, not to predict future behavior.)
- Spend more time understanding the problem, not the product. "Fall in love with your customer's problem. The solution will fall out when you really understand the problem."
- Look for multi-sided markets. In such an environment, find the "queen bee" who controls the overall ecosystem. Understand *their* problem and you move the market. (Example: European Banking Authority and managing login systems for 6000 banks and their regulatory filings.)
- Find minimum viable "route" for success. Show the solution in the small, then it will grow.
- Be prepared to pivot. Timothy's example:
    - Proprietary -> blockchain -> KERI
    - VCs -> ACDCs
    - DIDs -> AIDs
    - ZKPs -> graduated disclosure
    - SSI -> B2B (the "route" to adoption)
- Be a truth-seeker. "Strong opinions loosely held."

"The technology in this space has a half-life of about five years." 🎤 drop

Governance model that combines life cycle perspective and ToIP stack model

Session Convener: Ismael Avila
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

Unique Media ID to Fight Disinformation

Session Convener: Todd A. Carpenter
Session Notes Taker(s): Todd A. Carpenter

Tags / links to resources / technology discussed, related to this session:

ISO
International Workshop Agreement #44
National Information Standards Organization (NISO)
ISO Technical Committee 46 - Information & Documentation / Subcommittee #9 - Identification & Description
Background on IWA Proposal (via ANSI)
Global Media Registry

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

In January 2023, the ISO Technical Management Board approved a new International Workshop Agreement (IWA) to explore the creation of a new identifier for the media ecosystem. The IWA formed in February with a goal of creating a Global Media Identifier, which aims at enhancing the integrity of content indexation and recommendation by online platforms (e. g. search, streaming and social media). The discussion during Day 1 covered the background of the project, the goals the project seeks to achieve and how it interacts with other issues related to media identification.

This project is intended to be achieved by harmonising and improving the effectiveness of respective signalling along the distribution chain by means of a unique identifier of channels and brands. In addition, the deliverables of the IWA will be used by all other stakeholders that engage with mass media and content distribution online such as providers/operators of advertising technology and public sector actors (e. g. regulatory authorities).

For the avoidance of doubt, the project participants have agreed that this indicator is about the means of distribution of media only, not about individual pieces of content. Thus, its purpose is to unambiguously identify the respective source, for example in order to trace back and identify its ultimate beneficial owner. Accordingly, it will be designed to provide signal transparency and integrity in a neutral way, not a value judgement about the trustworthiness of the content itself.

It is also acknowledged that ethical concerns about so-called “inclusion” or “exclusion” lists (i.e., “white” or “black” lists), that might be misused for the purpose of censorship and of which the project group is fully aware, are not applicable to this project. Such an identifier might help to mitigate related risks by preventing mismatches and mix-ups that are rampant in this space. This is a result of the fact that all stakeholders concerned (such as social media platforms and search engines, the advertising sector and public actors, like regulators, and academia) each separately already are using identifiers, to index media companies, channels and their assets, but that those are not harmonized yet.

Which Problem is addressed by the IWA?
The functioning of our shared information space depends on digital infrastructure and platforms. Their protocols and algorithmic-driven recommender systems determine how we see the world online. Accordingly, authoritative and credible information deserves prominence, while harmful or even illegal content must be demoted or deleted. This project aims at harmonising and improving the effectiveness of respective signalling along the distribution chain of content and thus, to enhance the integrity of services. In order to work properly, recommender systems require up-to-date criteria by which content is included, promoted or even excluded based upon inclusion lists of trustworthy sources of content, or exclusion lists of bad actors.

Currently, the datasets upon which these decisions are based are provided in real time by an increasing number of external actors, such as NGOs and ad-tech providers, but are also compiled internally by platform owners. A problem occurs when these different lists result in ambiguities or mismatches. This might be the case with brands of the same name (there are several dozens of media outlets called ‘Phoenix’), or with affiliates, syndicated channels or sister-brands of the same origin, but with different editorial lines (e. g. Al Jazeera, Phoenix or Fox). Even when a web-domain or social media account is always distinct, it might not be immediately clear to which media outlet or company it belongs. This could lead to conflicting or wrong signals, misleading algorithmic indexation and negatively impacting site integrity and user experience.

Bad actors could even capitalise on this deficiency and try to game the recommender systems with similar sounding names of channels, accounts or brands.

The conversation highlighted a variety of existing media identification projects, notably the C2PA project. Discussions also focused on the potential application of distributed identifier systems as a potential solution. Whether the UMID project should pursue a distributed or centralised approach was discussed. The ethical issues of anonymity and security were also discussed.

SESSION #5

SSI didn’t work, we are Pivoting! Ask me anything

Session Convener: Riley Hughes
Session Notes Taker(s):

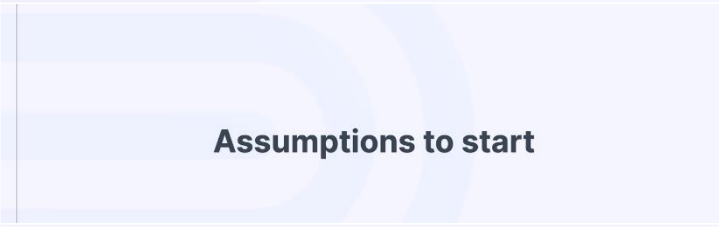
Tags / links to resources / technology discussed, related to this session:

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

No notes - just slides

trinsic

Why Trinsic is pivoting + lessons learned from 5yrs as an SSI platform

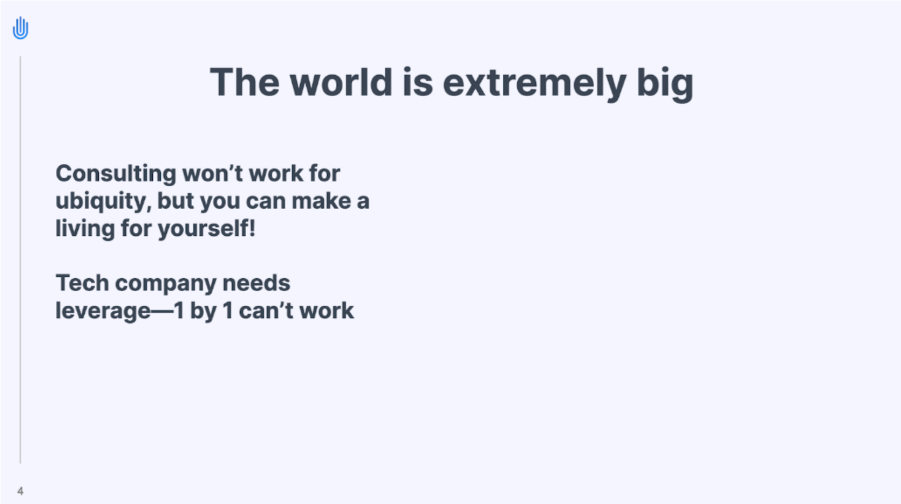


Assumptions to start

We all want the same thing

Walls down, safe space 😊

3

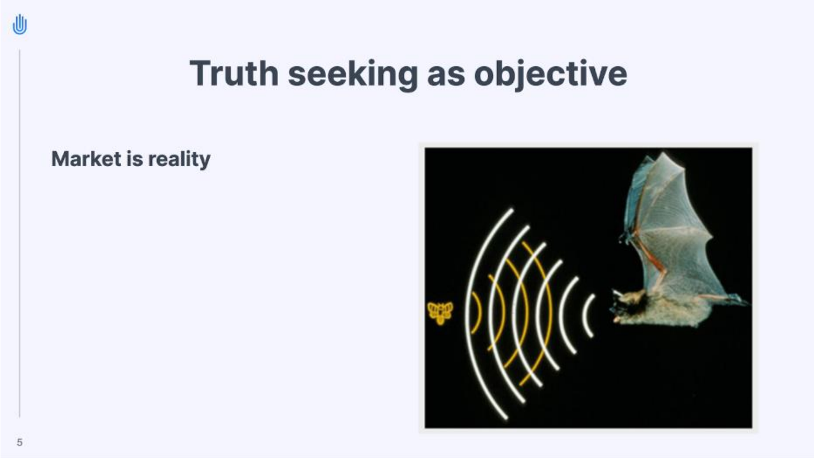


The world is extremely big

Consulting won’t work for ubiquity, but you can make a living for yourself!

Tech company needs leverage—1 by 1 can’t work

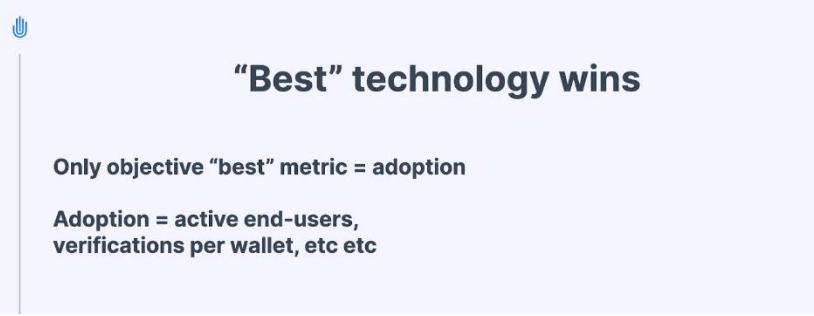
4



Truth seeking as objective

Market is reality

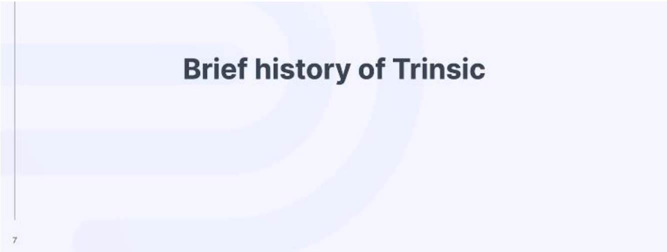
5



“Best” technology wins

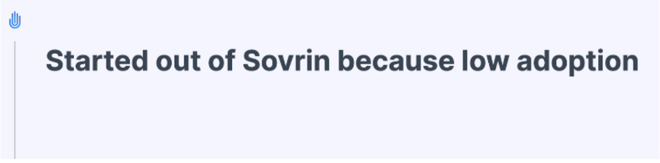
Only objective “best” metric = adoption

Adoption = active end-users, verifications per wallet, etc etc



Brief history of Trinsic

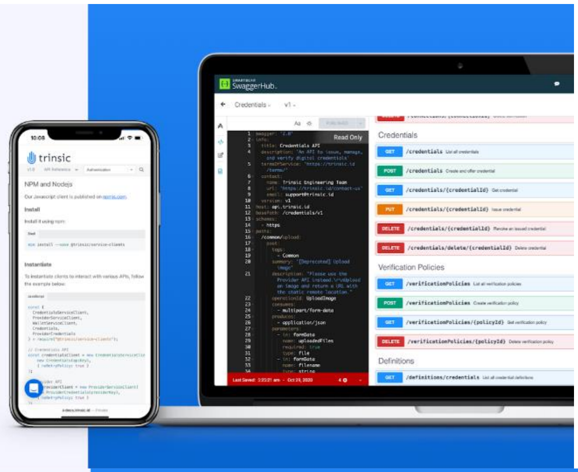
7



Started out of Sovrin because low adoption

VC Infra

- Launched at IIW 5yrs ago
- "Stripe for VCs" won't work until VCs are widely adopted
- "250k consulting deals OR big bet on adoption"



NPM and Nodejs

Our Javascript client is published on npmjs.com.

Install

Install it using npm:

```
npm install --save @trinsic/service-clients
```

Instantiate

To instantiate clients to interact with various APIs, follow the example below:

```
const {
  CredentialsServiceClient,
  ProviderServiceClient,
  WalletServiceClient,
  Credentials,
  ProviderCredentials
} = require("@trinsic/service-clients");

// Credentials API
const credentialsClient = new CredentialsServiceClie
    new Credentials(apiKey),
    { noRetryPolicy: true }
);

    ovider API
    roviderClient = new ProviderServiceClient(
    new ProviderCredentials(providerKey),
    { noRetryPolicy: true }
```

```
swagger: '2.0'
info:
  title: Credentials API
  description: 'An API to issue, manage,
    and verify digital credentials'
  termsOfService: 'https://trinsic.id
    /terms/'
  contact:
    name: Trinsic Engineering Team
    url: 'https://trinsic.id/contact-us'
    email: support@trinsic.id
  version: v1
host: api.trinsic.id
basePath: /credentials/v1
schemes:
  - https
paths:
  /common/upload:
    post:
      tags:
        - Common
      summary: '[Deprecated] Upload
        image'
      description: "Please use the
        Provider API instead.\r\nUpload
        an image and return a URL with
        the static remote location."
      operationId: UploadImage
      consumes:
        - multipart/form-data
      produces:
        - application/json
      parameters:
        - in: formData
          name: uploadedFiles
          required: true
          type: file
        - in: formData
          name: filename
          type: string
```

Credentials

- GET /credentials List all credentials
- POST /credentials Create and offer credential
- GET /credentials/{credentialId} Get credential
- PUT /credentials/{credentialId} Issue credential
- DELETE /credentials/{credentialId} Revoke an issued credential
- DELETE /credentials/delete/{credentialId} Delete credential

Verification Policies

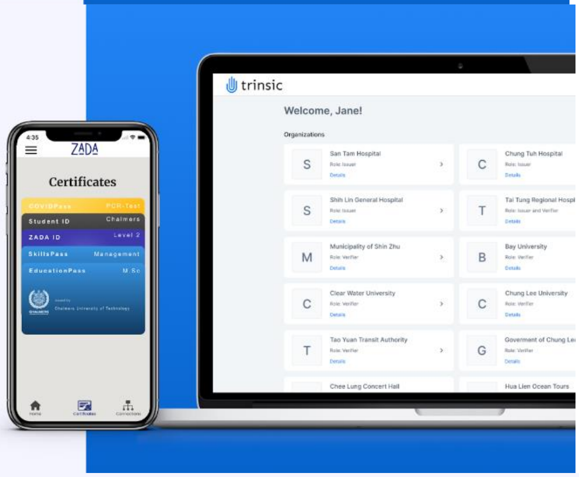
- GET /verificationPolicies List all verification policies
- POST /verificationPolicies Create verification policy
- GET /verificationPolicies/{policyId} Get verification policy
- DELETE /verificationPolicies/{policyId} Delete verification policy

Definitions

- GET /definitions/credentials List all credential definitions

IDtech platform

- Shifted because everybody building the same thing
- IDtech startups not succeeding enough



Welcome, Jane!

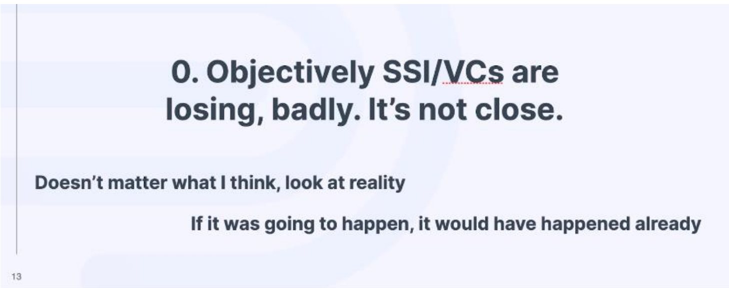
Organizations

San Tam Hospital Role: Issuer Details	Chung Tuh Hospital Role: Issuer Details
Shih Lin General Hospital Role: Issuer Details	Tai Tung Regional Hospi Role: Issuer and Verifier Details
Municipality of Shin Zhu Role: Verifier Details	Bay University Role: Verifier Details
Clear Water University Role: Verifier Details	Chung Lee University Role: Verifier Details
Tao Yuan Transit Authority Role: Verifier Details	Goverment of Chung Le Role: Verifier Details
Chee Lung Concert Hall	Hua Lien Ocean Tours

After 4 years of Trinsic?

itsme 8m	YOTI 7m	ID.me 53m
CLEAR 17m	persona 1m	incode 4m

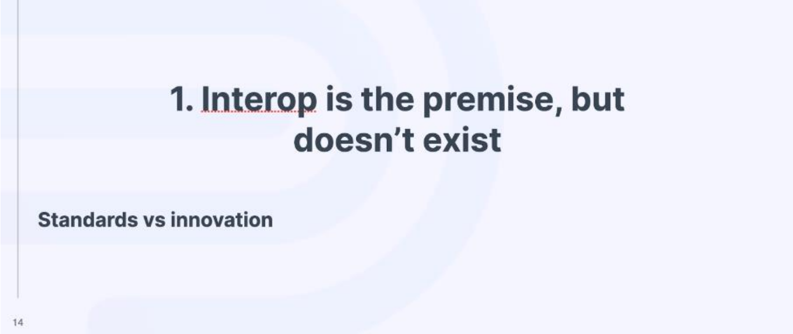
Why my bets are no longer on VCs in the short- to mid-term



0. Objectively SSI/VCs are losing, badly. It’s not close.

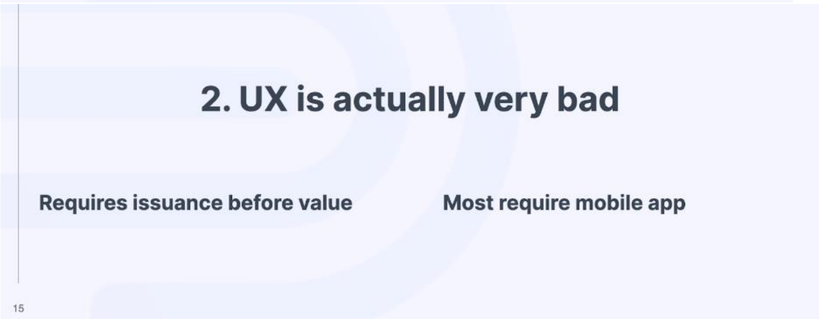
Doesn’t matter what I think, look at reality

If it was going to happen, it would have happened already



1. Interop is the premise, but doesn’t exist

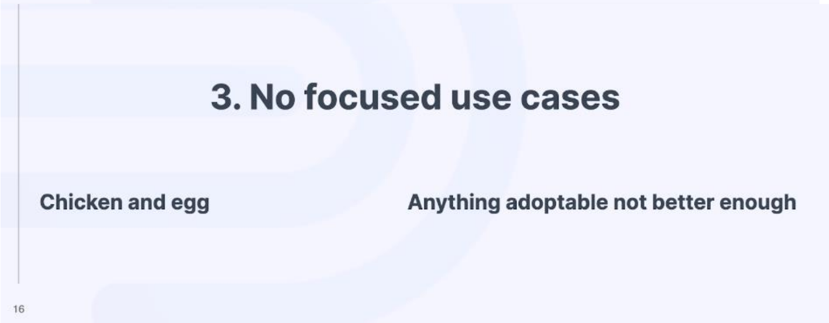
Standards vs innovation



2. UX is actually very bad

Requires issuance before value

Most require mobile app



3. No focused use cases

Chicken and egg

Anything adoptable not better enough

Zero Trust with Zero Data (Verifiable Credentials)

Session Convener: Phil Windley
Session Notes Taker(s):

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

Extremely informative session. Zero Trust is The Key component to identify for Credentials and Verifiabels.

OpenWallet Foundation Overview

Session Convener: Sean Bohan, OWF
Session Notes Taker(s): N/A

Tags / links to resources / technology discussed, related to this session:

That is a link to the deck
https://drive.google.com/file/d/1ANgJli2hkQVm6wnavePF3h_f1-Seboyk/view?usp=sharing

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

What is required to trust A.I. with your Personal ID?

Session Convener: Marc-Aurèle Besner
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

- Limit Access / Fine Grain Access Control
- Training
- Insurance on mistakes
- Fear of missing out / Peer validation
- Identifier/Identity for A.I. Agent
- Layering A.I. agent to protect against prompt engineering
- Trustless system

Functional Privacy

Session Convener: Joe Andrieu
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

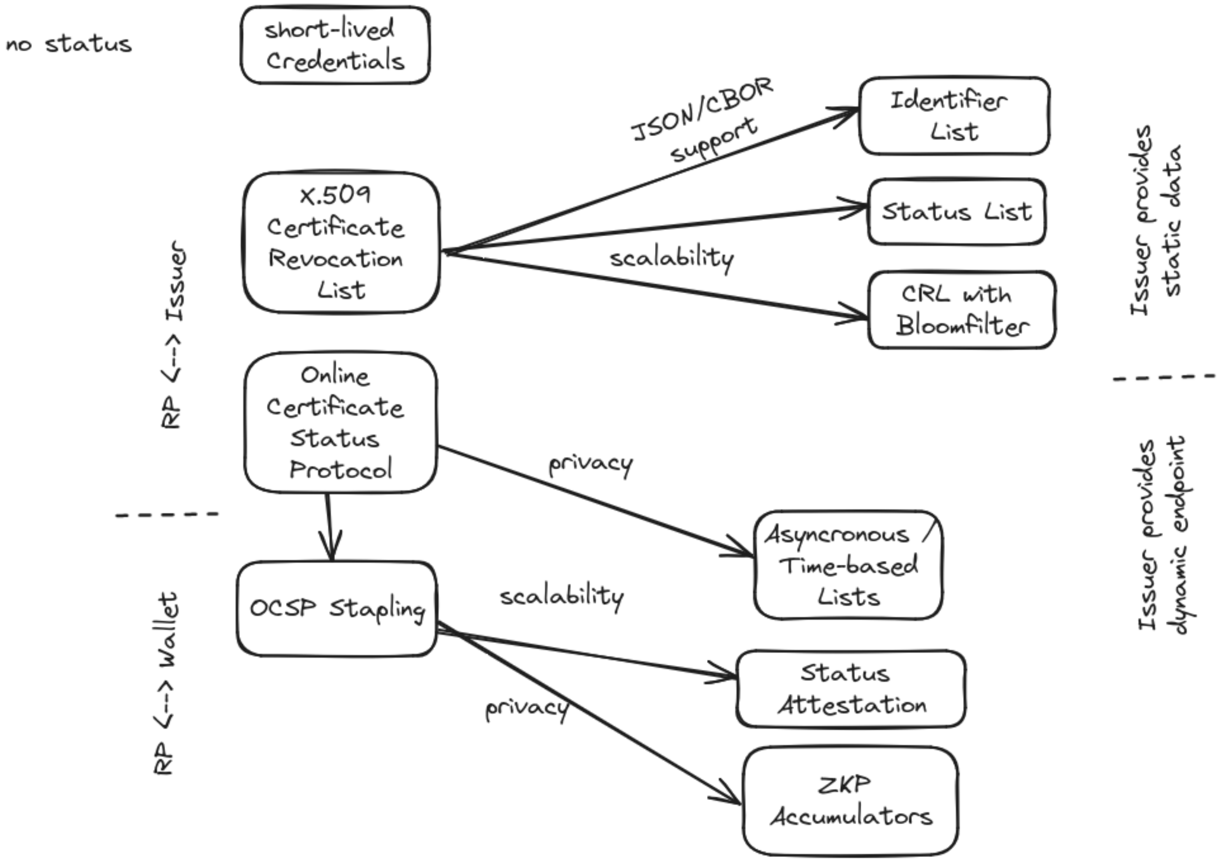
Status/Revocation Mechanisms Comparison

Session Convener: Mirko Mollik, Paul Bastian
Session Notes Taker(s): Kai Wagner, Mirko Mollik

Tags / links to resources / technology discussed, related to this session:
Revocation Lists/Status Lists, Comparison Matrix

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

- Different Credential revocation approaches were discussed, from accumulators to lists, bittrings and also status credentials.
    - Mentioned were
        - Bitstring Status List
        - Linked Validity Verifiable Credentials https://eprint.iacr.org/2022/1658.pdf & https://www.linkedin.com/pulse/privacy-preserving-scalable-revocation-done-why-so-andreas-freitag-yvxkf/?trackingId=yI4CJJKqQxiUC73Ovl76Zw%3D%3D
        - https://mailarchive.ietf.org/arch/msg/oauth/3iWsiAa2iaoGdmIiB_Hjhx-h7NA/
        - other methods researched by Mirko were also discussed
- Trying to go from the “current used solutions” from the PKI world to the new one introduced in the SSI space.



After listing the different approaches, Paul and Mirko presented the different criterias they want to use for a comparison matrix:

- Scalability
  - Does the efficiency suffer for the issuance or the verifier when adding new elements
  - Option for Third Party Hosting/CDN?
- Privacy
  - Observability from Issuer (Traceability)
  - Observability from Verifier (Profiling)
  - Observability from Outsiders
- Complexity
  - Algorithm (is it easy to understand?), is the Specification publically available (for free)
  - Implementation (is it hard to implement? How many libraries exist to support it?)
  - Communication requirements
  - during issuance
  - during presentation
- Efficiency (costs/time, required resources)
  - Efficiency for Issuer
  - (how many resources are required to update one credential)
  - providing the information
  - Efficiency for Holder
  - Efficiency for Verifier

- Feature
  - Historical data
  - Third Party hosting as a privacy feature
  - reversible status changes
- Offline capability and Caching
  - Scenario Holder is offline
  - Scenario Verifier is offline
- Dependency
  - Bound to specific algorithms (e.g. crypto agility)
  - Bound to a specific system (DLT)

The audience agreed that these could be objective criterias. However the relevance for each of them can depend on the specific use case. The work will continue in the credential profile comparison SIG at the Open Wallet Foundation: https://github.com/openwallet-foundation/credential-format-comparison-sig

Verifiable Presentation as a Signature

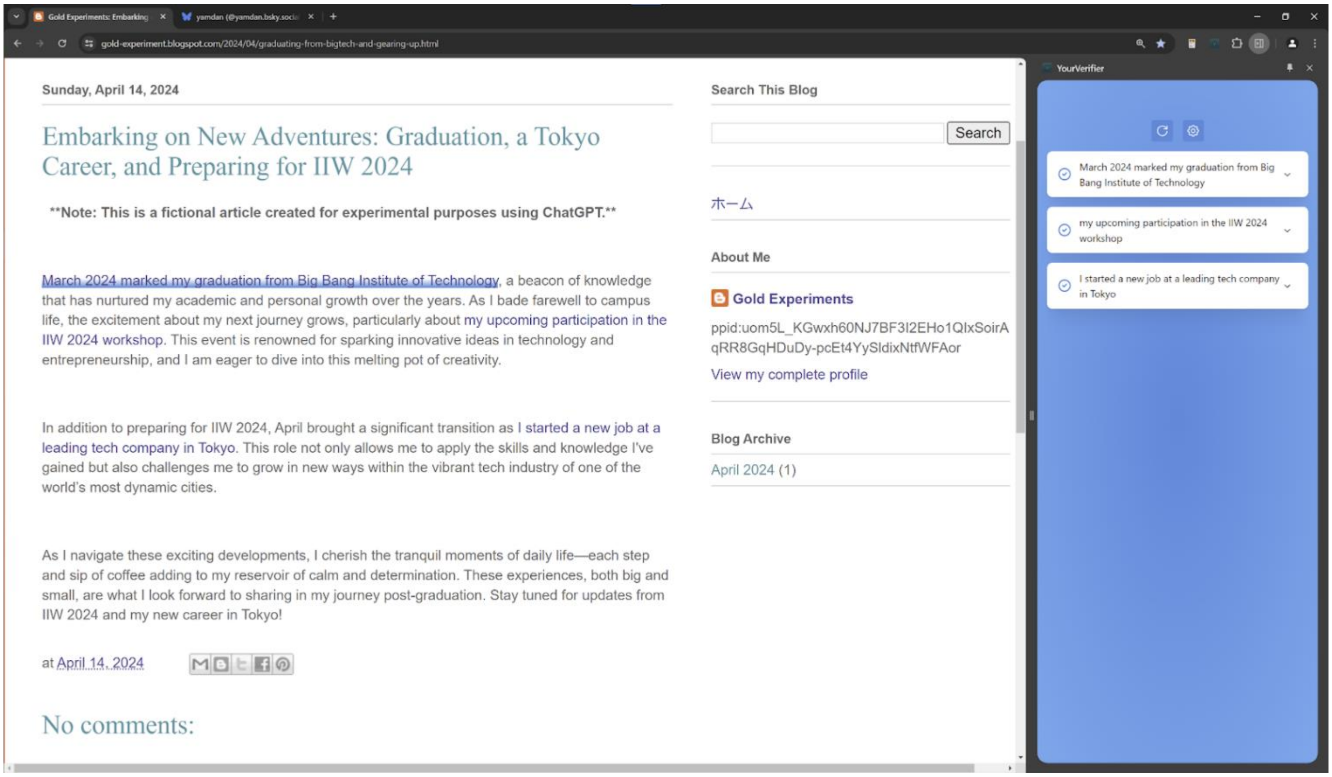
Session Convener: Dan Yamamoto
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

- Tags: Verifiable Credentials, Verifiable Presentations, BBS+ Signatures, Zero-Knowledge Proofs, Pairwise Pseudonymous Identifier (PPID), Chrome extension
- Related session: Verifiable Credentials with BBS+ and zk-SNARKs for Predicate Proofs (Day 3 / Session 14 / Space G)
- The extension is published at https://github.com/zkp-ld/web-verifier (work in progress, not officially packaged)
- The demo website for the extension is https://gold-experiment.blogspot.com/2024/04/graduating-from-bigtech-and-gearing-up.htm

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

The convener presents a prototype Chrome extension that can verify Verifiable Presentations embedded in or externally attached to webpages, e.g., blog and bluesky.



Gold Experiments: Embarking
yamdan (@yamdan.bsky.soci
gold-experiment.blogspot.com/2024/04/graduating-from-bigtech-and-gearing-up.html
YourVerifier

Sunday, April 14, 2024

Embarking on New Adventures: Graduation, a Tokyo Career, and Preparing for IIW 2024

Note: This is a fictional article created for experimental purposes using ChatGPT.

March 2024 marked my graduation from Big Bang Institute of Technology, a beacon of knowledge that has nurtured my academic and personal growth over the years. As I bade farewell to campus life, the excitement about my next journey grows, particularly about my upcoming participation in the IIW 2024 workshop. This event is renowned for sparking innovative ideas in technology and entrepreneurship, and I am eager to dive into this melting pot of creativity.

In addition to preparing for IIW 2024, April brought a significant transition as I started a new job at a leading tech company in Tokyo. This role not only allows me to apply the skills and knowledge I've gained but also challenges me to grow in new ways within the vibrant tech industry of one of the world's most dynamic cities.

As I navigate these exciting developments, I cherish the tranquil moments of daily life—each step and sip of coffee adding to my reservoir of calm and determination. These experiences, both big and small, are what I look forward to sharing in my journey post-graduation. Stay tuned for updates from IIW 2024 and my new career in Tokyo!

at April 14, 2024

No comments:

Search This Blog

Search

ホーム

About Me

Gold Experiments

ppid:uom5L_KGwxh60NJ7BF3I2EHo1QIxSoirAqRR8GqHDuDy-pcEt4YySldixNtfWFAor

View my complete profile

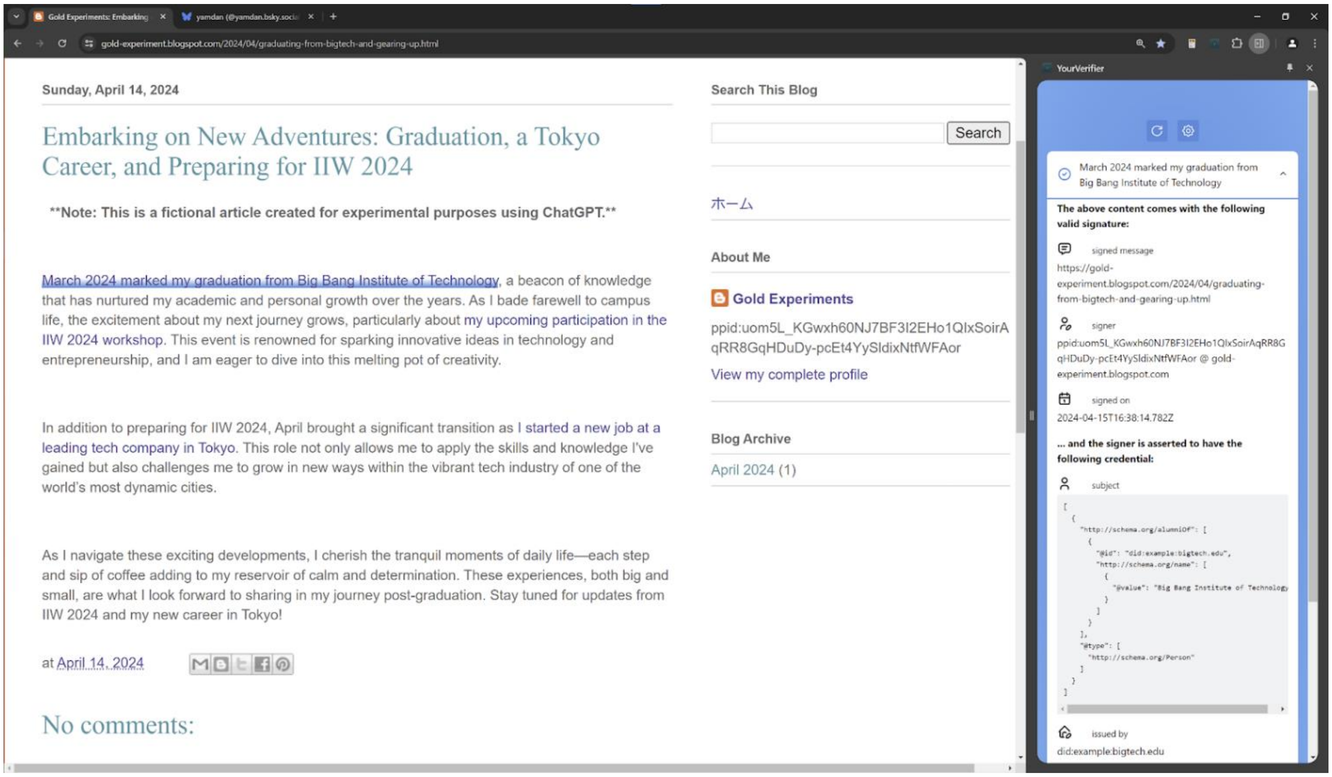
Blog Archive

April 2024 (1)

March 2024 marked my graduation from Big Bang Institute of Technology

my upcoming participation in the IIW 2024 workshop

I started a new job at a leading tech company in Tokyo



Sunday, April 14, 2024

Embarking on New Adventures: Graduation, a Tokyo Career, and Preparing for IIW 2024

Note: This is a fictional article created for experimental purposes using ChatGPT.

March 2024 marked my graduation from Big Bang Institute of Technology, a beacon of knowledge that has nurtured my academic and personal growth over the years. As I bade farewell to campus life, the excitement about my next journey grows, particularly about my upcoming participation in the IIW 2024 workshop. This event is renowned for sparking innovative ideas in technology and entrepreneurship, and I am eager to dive into this melting pot of creativity.

In addition to preparing for IIW 2024, April brought a significant transition as I started a new job at a leading tech company in Tokyo. This role not only allows me to apply the skills and knowledge I've gained but also challenges me to grow in new ways within the vibrant tech industry of one of the world's most dynamic cities.

As I navigate these exciting developments, I cherish the tranquil moments of daily life—each step and sip of coffee adding to my reservoir of calm and determination. These experiences, both big and small, are what I look forward to sharing in my journey post-graduation. Stay tuned for updates from IIW 2024 and my new career in Tokyo!

at April 14, 2024

No comments:

Search This Blog

Search

ホーム

About Me

Gold Experiments

ppid:uom5L_KGwxh60NJ7BF3I2EHo1QIxSoirAqRR8GqHDuDy-pcEt4YySldixNtfWFAor

View my complete profile

Blog Archive

April 2024 (1)

March 2024 marked my graduation from Big Bang Institute of Technology

The above content comes with the following valid signature:

signed message

https://gold-experiment.blogspot.com/2024/04/graduating-from-bigtech-and-gearing-up.html

signer

ppid:uom5L_KGwxh60NJ7BF3I2EHo1QIxSoirAqRR8GqHDuDy-pcEt4YySldixNtfWFAor @ gold-experiment.blogspot.com

signed on

2024-04-15T16:38:14.782Z

... and the signer is asserted to have the following credential:

subject

```
[
  {
    "http://schema.org/alumniOf": [
      {
        "@id": "did:example:bigtech.edu",
        "http://schema.org/name": [
          {
            "@value": "Big Bang Institute of Technology
          }
        ]
      }
    ],
    "@type": [
      "http://schema.org/Person"
    ]
  }
]
```

issued by

did:example:bigtech.edu

Hyperlinks in the above demo blog are anchored to VPs hosted on a GitHub page (e.g., https://yamdan.github.io/vc-example/public/vp/gold-experiment.blogspot.com/JohnSmithBigTechAlumni.jsonld#verifiable-presentation). The extension picks up all the hyperlinks ending with `#verifiable-presentation` and fetches them to get VPs, which are then verified using the issuers' public keys.

The VP includes the holder's PPID rather than its unique identifier to avoid interdomain linkability. PPID is deterministically generated from the holder's secret key and the identifier of the website that is indicated as `domain` in VP.

TODOs: spec documents, standardization, official extension for Chrome and Firefox, …

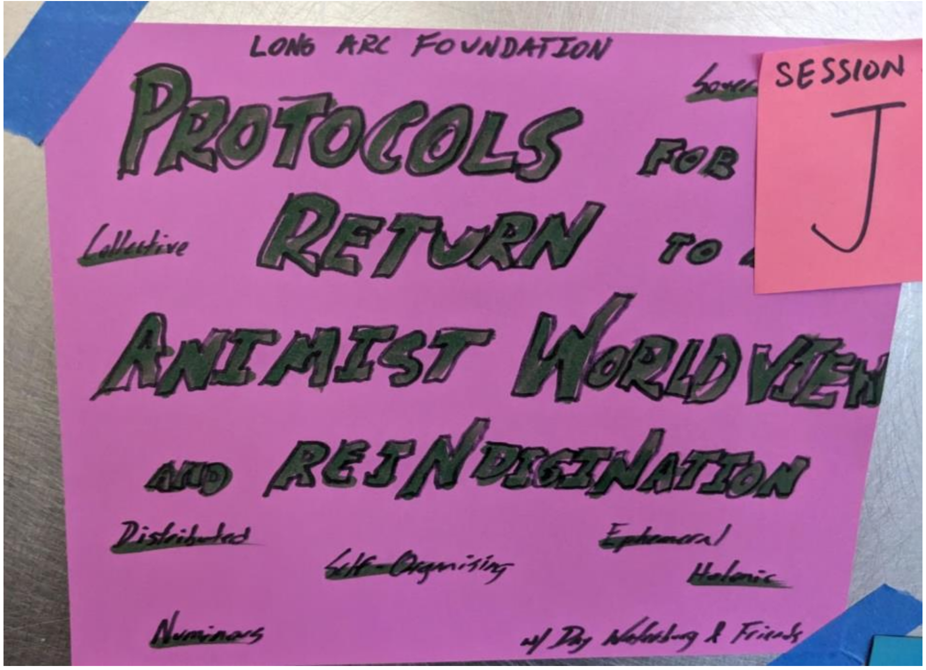
Protocols for a Return to an Animist Worldview and reiNdigenNation

Session Convener: Day Waterbury
Session Notes Taker(s): Day Waterbury

Tags / links to resources / technology discussed, related to this session:

Not the same, but close enough (ways of seeing, human processes, and culture as protocols): https://forum.summerofprotocols.com/t/pig-rfc-arc-regenerative-communities-protocol/1140

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



Linking notes to all our woven session here (Proton Drive PW: Share->IIW38 or Signal me @deiim.69 in case I change the PW) to save time. If I can I'll pull the session-specific transcripts in.

State of Adoption - bring your real world use case

Session Convener: James Monaghan
Session Notes Taker(s): James Monaghan

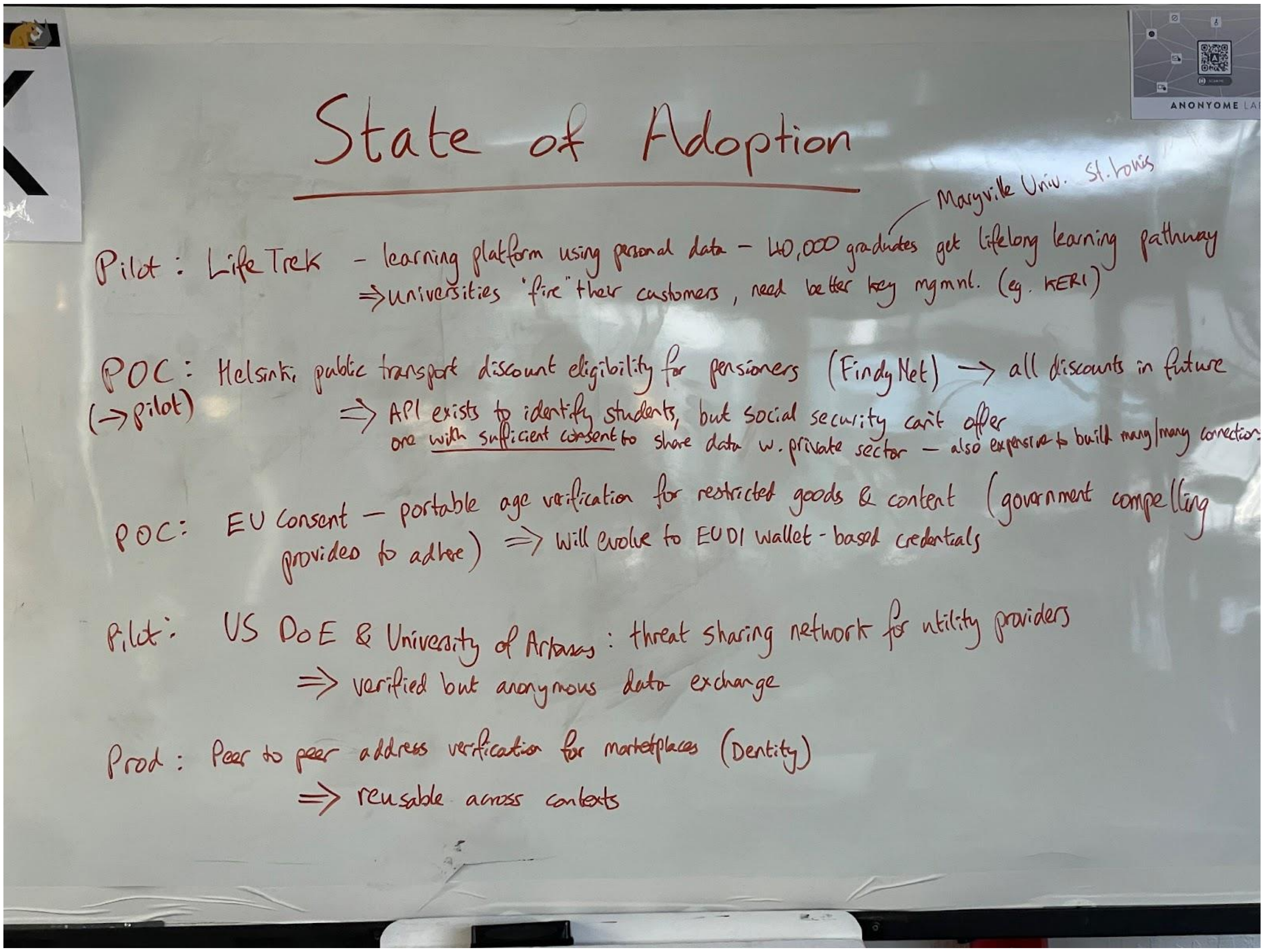
Tags / links to resources / technology discussed, related to this session:

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

The intention was to build a list of cool examples where decentralised ID is adopted in the real-world, so we can all be more persuasive when describing this to people.

We ended up with a list of cool use cases, and although most were in POC or Pilot stage rather than Production there was also a great discussion about some of the blockers to that adoption.

Photos of the whiteboard are below:



State of Adoption

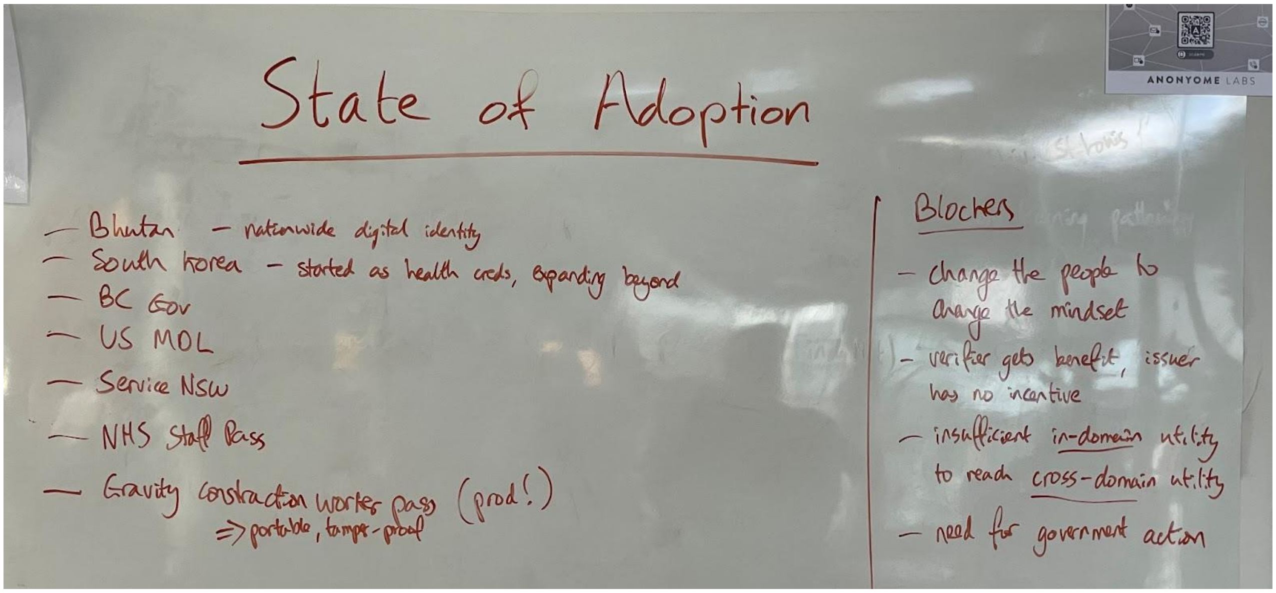
Pilot : LifeTrek – learning platform using personal data – 40,000 graduates get lifelong learning pathway
Maryville Univ. St. Louis
⇒ universities 'fire' their customers, need better key mgmnt. (eg. KERI)

POC : Helsinki public transport discount eligibility for pensioners (Findy Net) → all discounts in future
(→ pilot)
⇒ API exists to identify students, but social security can't offer one with sufficient consent to share data w. private sector – also expensive to build many/many connections

POC: EU Consent – portable age verification for restricted goods & content (government compelling providers to adhere) ⇒ Will evolve to EUDI wallet - based credentials

Pilot: US DoE & University of Arkansas : threat sharing network for utility providers
⇒ verified but anonymous data exchange

Prod : Peer to peer address verification for marketplaces (Dentity)
⇒ reusable across contexts



State of Adoption

- Bhutan – nationwide digital identity
- South Korea – started as health creds, expanding beyond
- BC Gov
- US MDL
- Service NSW
- NHS Staff Pass
- Gravity construction worker pass (prod!)
  ⇒ portable, tamper-proof

Blockers

- change the people to change the mindset
- verifier gets benefit, issuer has no incentive
- insufficient in-domain utility to reach cross-domain utility
- need for government action

OID4VCI Event Signalling

Session Convener: Oliver Terbu
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

materials used are here:
https://docs.google.com/presentation/d/1eIFywGwRp3Kqk35hiSTLlkZzRCmF1QC0N382u2ldMJI/edit?usp=sharing

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

We spoken about different use cases of event signalling in the context of OID4VCI to enable the following:

- The ability to notify the wallet of specific credential issuance process-related events, e.g., to reduce polling requests at the deferred issuance endpoint.
- The ability to inform the wallet or its backend about certain risk-related events, e.g., fraud, key compromise.
- The ability to notify the wallet of specific credential lifecycle-related events, e.g., a credential has been revoked independently from the status mechanism and associated TTL windows, new credential types can be requested, or the underlying credential dataset has changed, which is relevant for many credential types such as age-over-18, marriage, etc.

A potential solution could be based on the OIDF Shared Signals and related IETF standards work as presented at IIW. The slides can be found here.

It was generally considered to be a good idea and required to scale digital identity systems.

A solution should support both push and pull notification mechanisms. While the pull mechanism is easier to implement, it has certain limitations. For example, if a wallet must maintain relationships with several issuers, polling event endpoints from those issuers introduces a significant load on the mobile device.

Next steps are proposing event signalling to the OIDF DCP WG.

Introduction to TSP (Trust Spanning Protocol) Draft (Part I)

Session Convener: Wenjing Chu
Session Notes Taker(s): Wenjing Chu

Tags / links to resources / technology discussed, related to this session:

The link to presentation slide:
https://docs.google.com/presentation/d/13CiM1qJxLWT50PK7tOd0jVO4L91yPwR47cigh5JkaEs/edit#slide=id.g2cb5daa6a3e_0_782

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

TSP is an "internetworking layer of digital identities". TSP is a "simple yet radical" design following the same philosophy of TCP/IP to the problem of digital identities and trust in the Internet.

This is the first part of "Intro to TSP" - we covered:

- TSP's overall goals, why a spanning layer, why focus on inter-networking or interoperability.
- Verifiable IDs
- How two peers discover each other
- How two peers verify each other's ID. TSP only uses IDs after verification.
- Verifiable IDs associated with public key pairs.
- TSP Relationship formation
- TSP message structures
- TSP public key based authenticated encryption: HPKE, Sealed Box
- TSP signatures, why
- Summary: we covered the TSP Direct Mode that enables authenticity and confidentiality.

- Tomorrow in Part II, we will cover Routed Mode, nesting, and metadata privacy. https://docs.google.com/document/d/1VkT6Cc5_dFfxjMTYON-INzLBZud3lV7vM6bio5_JHYw/edit
- On Thursday in Part III, we will cover implementation of TSP in Rust and how one may adapt TSP in their software environments.

TSP Draft Spec:
https://trustoverip.github.io/tswg-tsp-specification/
Github: https://github.com/trustoverip/tswg-tsp-specification

W3C Federated Identity WG + WICG Digital Credentials

Session Convener: Heather Flanagan
Session Notes Taker(s): Wendy (assistance welcome!)

Tags / links to resources / technology discussed, related to this session:
[Notes from the WICG session]

Issues regarding adding Digital Credentials to the FedID WG charter:
https://github.com/w3c/strategy/issues/450

Draft charter revision under discussion: https://w3c.github.io/charter-drafts/2024/wg-fedid.html?rand123

Current charter (chartered March 2024) :
https://www.w3.org/2024/03/wg-fedid-charter.html

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

Heather: Intro, W3C Process;
W3C Community Group, incubation. Working Group, formal standardisation.
WG chartered, during chartering, suggestion (not formal objection) was made to include Digital Credentials work from WICG. So a proposed recharter discussion has begun. This session is part of that discussion!

A previous session demoed the Identity Credentials selection as in WICG, digital-credentials.dev

Areas of open discussion in the proposed recharter: privacy and harms considerations. How to include privacy considerations on a pace matched to the API development.

Questions:

- How familiar are you with Digital Credentials work?
- When it's ready, is this WG the right home?
- What does "ready" mean?

Dean: Passkeys Q. If Digital Credentials work is identification, not authentication, does it belong with FedCM? Or should we consider similarities with passkey selection? (WebAuthn group is not working on selection.)
DW: business logic not defined at W3C, passing of information to enable the selection interface.
Rick: help user understand the difference between signing up and signing in.
George: previous session showed identity provider selection, FedCM is lots more. Can they be merged, across the on-device, in-cloud divide?
Sam: That's a reason I'm excited to have both APIs in one WG. invite the communities to collaborate.
Sameera: extend wallet selection to IDP
George: I'd like to see language about synergies, potentially driving toward a single IDP discovery model
Pam: presentation of a VC has a time element, similar to SAML assertion or request/response
George: Neither passkeys nor VCs can obtain authZ token. another set of use cases to keep in mind

Wendy: whose perspectives are we missing?
Sam: we've heard privacy advocates concerned about bringing sensitive documents (drivers' licenses, birth certificates) to the web. Not fostering a "papers-please" web, surveillance. Make sure we hear from multiple browsers
Dean: get a broad array of RPs into the room. Understand their issues, concerns, and what they like, need to do. (cf FIDO and passkey rollout). Shouldn't just be browsers setting the terms for the ecosystem.
: Should those interested in wallet-based credentials be here?

Heather: What does interoperability look like? what are we testing against? if we want to be protocol agnostic, what do we test?
Pam: are you chartering to solve a problem, or to produce specific deliverables?

Takeaways

1. Should we be explicit about a goal to see the APIs converge?
2. Add to entities represented in WG: wallet issuers and verifiers?
3. Interop story

Notes Day 2 / Wednesday April 19 / Sessions 6 - 10

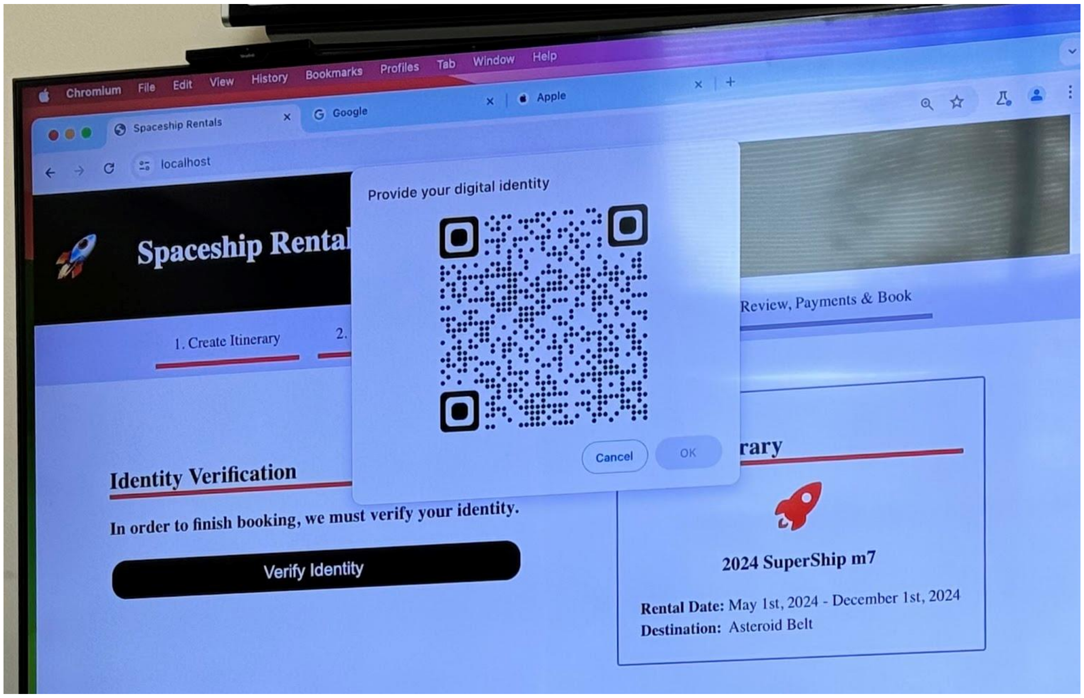
SESSION #6

Cross Platform Digital Credentials API

Session Convener: Eric M, Helen, Andreas, Lee
Session Notes Taker(s): Albert Wu (screenshots)

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

- Cross Platform Digital Credentials API
- Apple / Google demo
- using CTAP as starting point
- still prototype to demonstrate progress
- W3C NYCG?
- Supports any device supporting Passkeys
- transparent to relying party (website)
- sample app on OWF github https://github.com/openwallet-foundation-labs/identity-credential
- MacOS / iPhone



Provide your digital identity

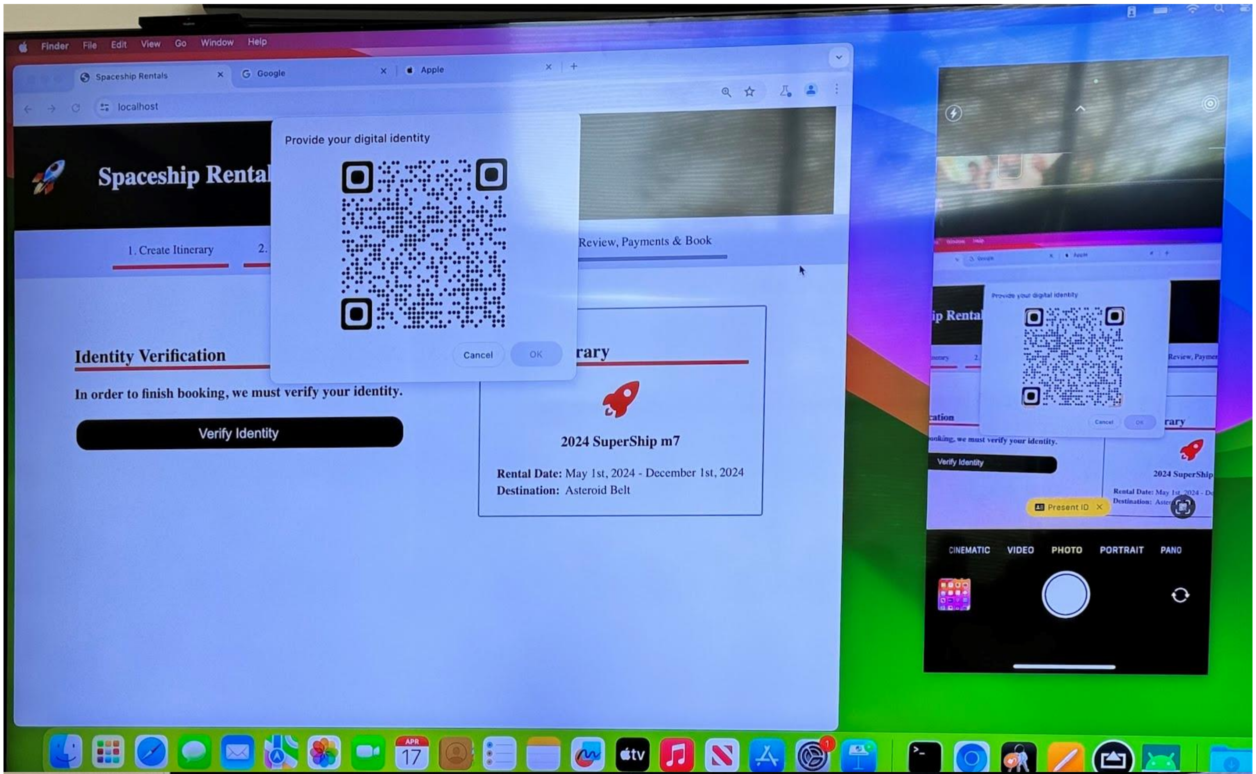
Identity Verification

In order to finish booking, we must verify your identity.

rary

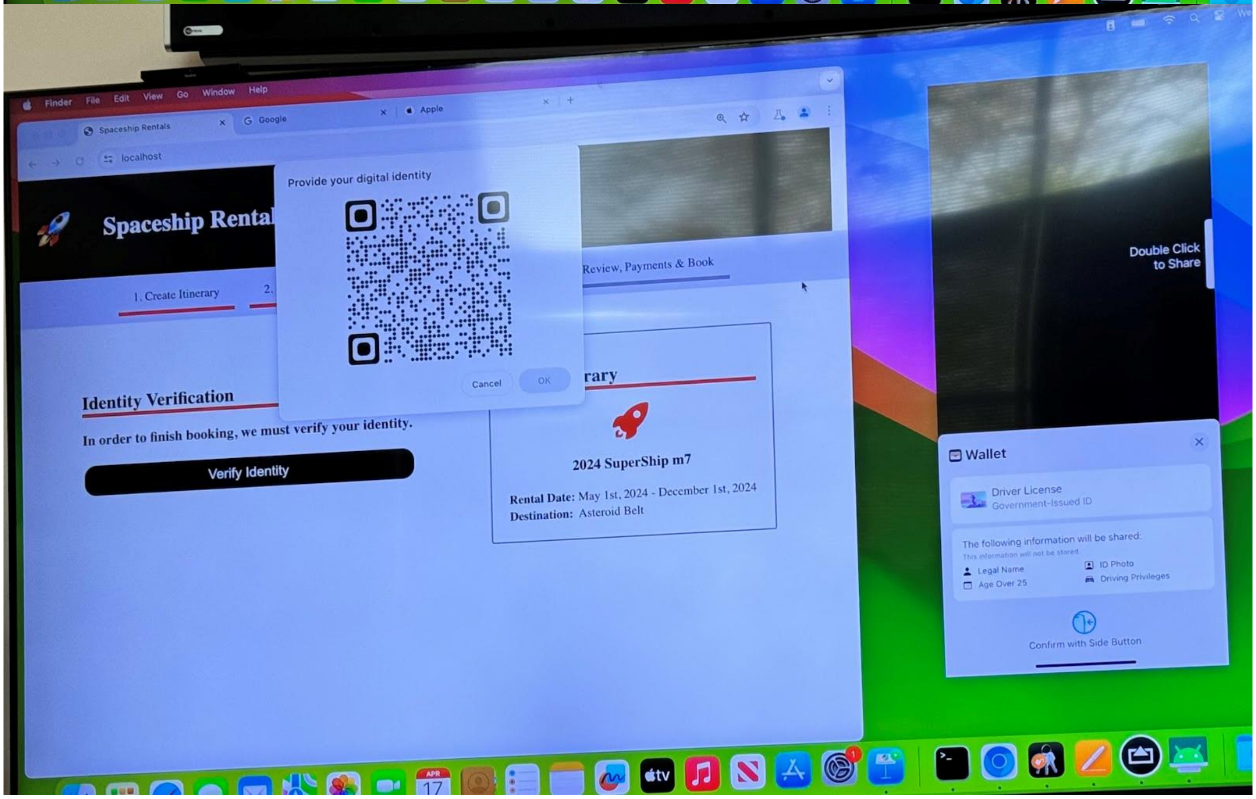
2024 SuperShip m7

Rental Date: May 1st, 2024 - December 1st, 2024
Destination: Asteroid Belt



In order to finish booking, we must verify your identity.

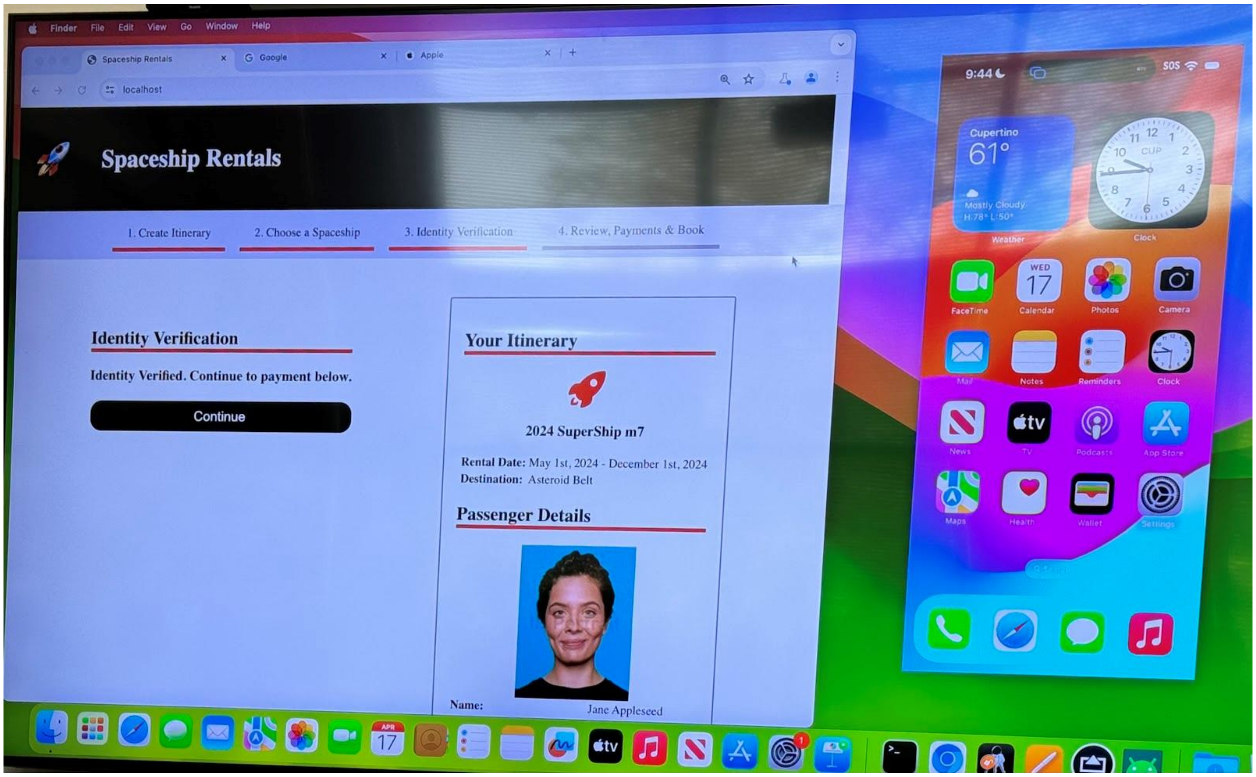
Rental Date: May 1st, 2024 - December 1st, 2024
Destination: Asteroid Belt



In order to finish booking, we must verify your identity.

Rental Date: May 1st, 2024 - December 1st, 2024
Destination: Asteroid Belt

The following information will be shared:
This information will not be stored.
Legal Name
Age Over 25
ID Photo
Driving Privileges



Spaceship Rentals

1. Create Itinerary | 2. Choose a Spaceship | 3. Identity Verification | 4. Review, Payments & Book

Identity Verification

Identity Verified. Continue to payment below.

Your Itinerary

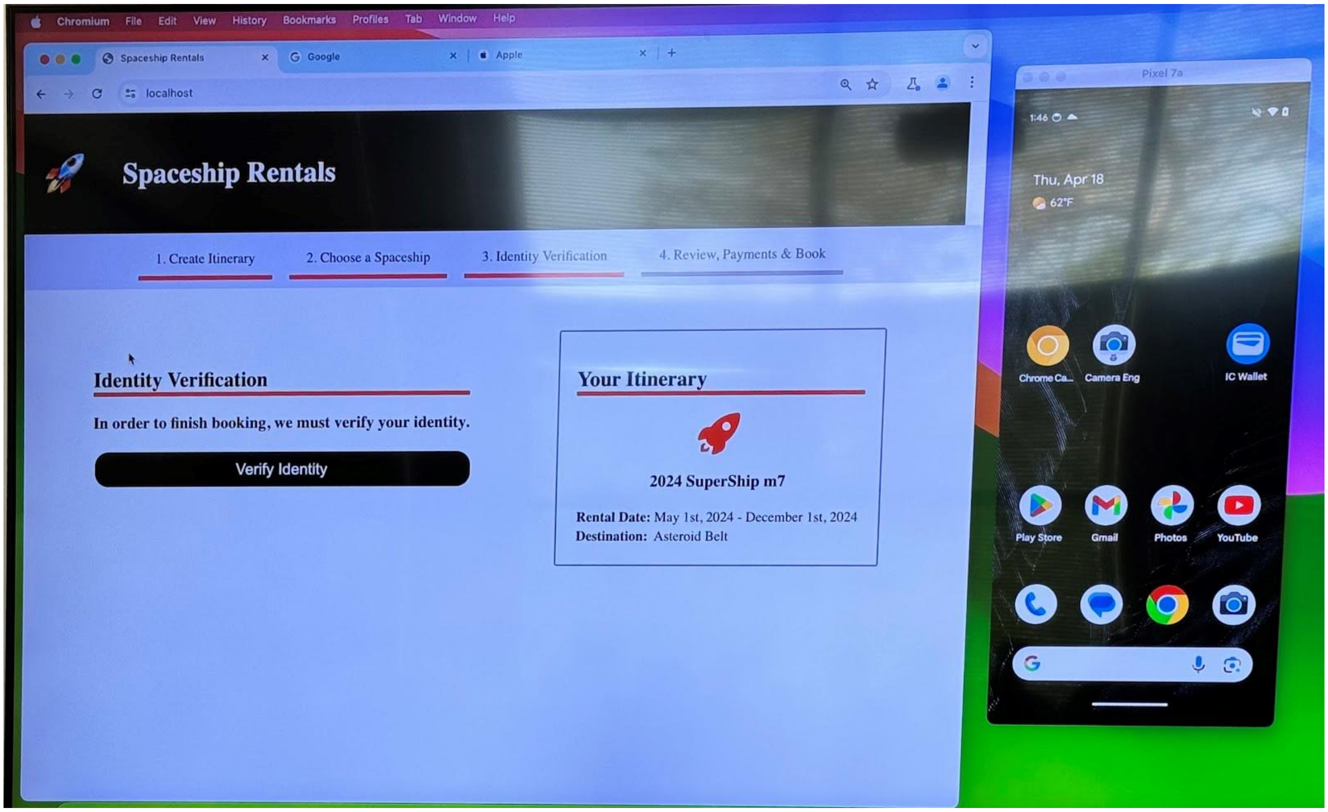
2024 SuperShip m7

Rental Date: May 1st, 2024 - December 1st, 2024
Destination: Asteroid Belt

Passenger Details

Name: Jane Appleseed

MacOS / Android



Spaceship Rentals

1. Create Itinerary | 2. Choose a Spaceship | 3. Identity Verification | 4. Review, Payments & Book

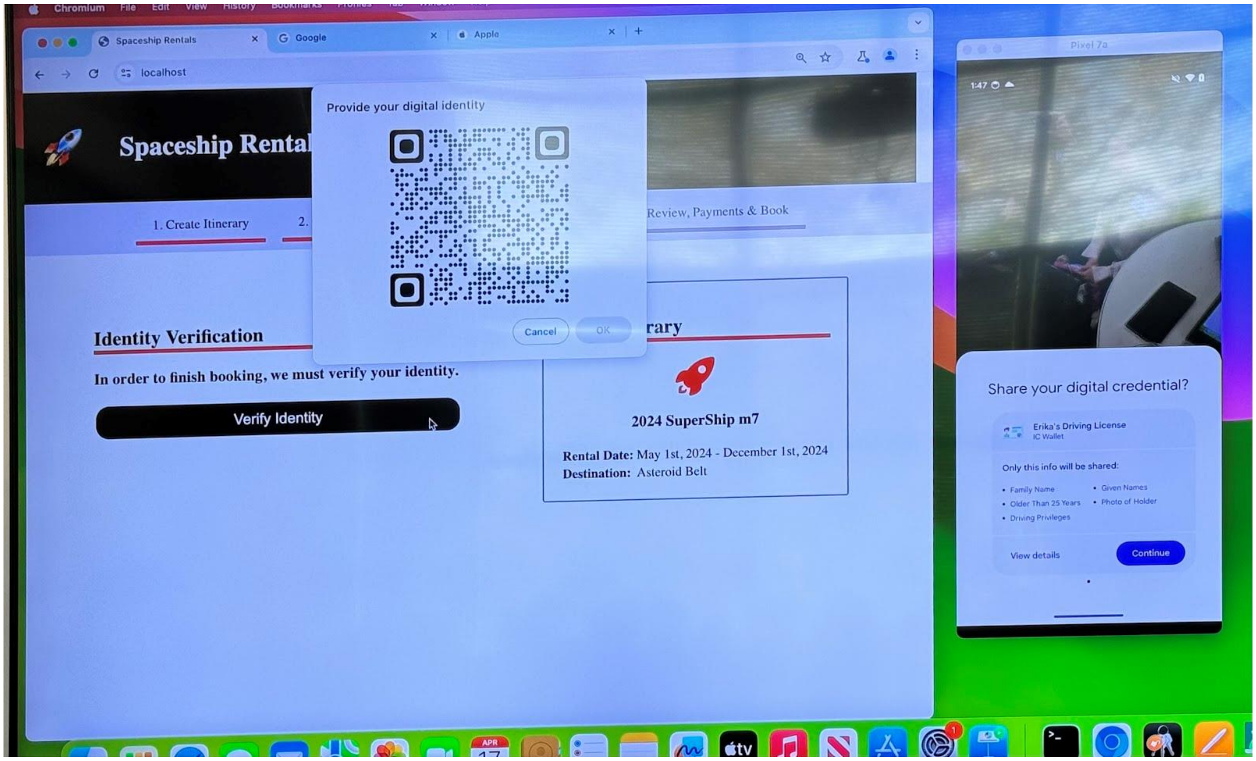
Identity Verification

In order to finish booking, we must verify your identity.

Your Itinerary

2024 SuperShip m7

Rental Date: May 1st, 2024 - December 1st, 2024
Destination: Asteroid Belt



Provide your digital identity

Identity Verification

In order to finish booking, we must verify your identity.

rary

2024 SuperShip m7

Rental Date: May 1st, 2024 - December 1st, 2024
Destination: Asteroid Belt

Share your digital credential?

Erika's Driving License
IC Wallet

Only this info will be shared:

- Family Name
- Given Names
- Older Than 25 Years
- Photo of Holder
- Driving Privileges

This provides plumbing and is wallet format agnostic.

See OpenID4VP session next hour (same room) to learn more about the payloads that might be transported through the pipes

KERI for Dummies

Session Convener: Timothe Ruff. Phil Fearheller
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

Content Authenticity 201

Session Convener: Eric Scouten, Adobe
Session Notes Taker(s): Jin Wen

Tags / links to resources / technology discussed, related to this session:

Eric's slide deck · Eric's comments (based on these notes – thank you, Jin!)

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

Follow up with yesterday's 101 session which is from here: IIW38_S1C_Content Authenticity 101

Eric's Content Authenticity 101: https://ericscouten.dev/2024/content-authenticity-101/

Focus on

- C2PA data model Assertions
- CAWG Identity Assertion Working Group

Note: The Content Authenticity 101 talk (Tuesday) or similar knowledge is a recommended prerequisite for two other sessions that Eric is leading on Wednesday or Thursday:

- CAWG identity assertion technical working session
  - More detailed walkthrough of identity assertion
  - "Interesting challenges" using VCs in a broadcast media context
- CAWG identity assertion user experience working session
  - Co-led with Pia Blumenthal, UX lead for CAI at Adobe

Continue on the C2PA data model assertions

Open Source HERESY Functional Source Licence and Other Approaches to Designing for Sustainability

Session Convener: Dave Grantham
Session Notes Taker(s): Sean Bohanm, Cam Geer

Tags / links to resources / technology discussed, related to this session:

Functional Source License | https://fsl.software/

https://www.linkedin.com/in/david-grantham-87207a265/
https://www.linkedin.com/in/seanbohan/
https://www.linkedin.com/in/camgeer/

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

- Hardest part of open source is funding
- Mozilla, LF as examples
- Web3 different, more bottom up
- Explicitly designed for sustainability
- Quadratic funding
- Staking revenue commitments
- Donor advised funding - example?
- Retroactive public goods funding - Dave example
- Compatible with F/OSS licences
- How to design a block bolted to floor
- Source available licences
- Open source understanding
- Number of functions to build sustainability to lower X factor
- Good Ed materials
- Engaging Unis
- Biz dev
- Funding needed
- What happens to people who depend on it
- Explore how to sell insurance to companies who want to use open source
- Ways to make sure expertise is paid for
- Long term
- Consider a non open licence (bsl fsl)
- Fsl with a commitment to public funding?
- Fsl
- Source available
- Starts clock
- 2 years - non profit, individual

- Used in dev of products internally
- Need to get commercial licence or reverts to open source licence
- Idea of fsl being rev generator
- Come with commit from commercial entity
- Designed to fund the open source side of the project
- Maybe we need a new licence or not
- Are public benefit vehicles the right thing?
- Sustainability
- Code availability is integrated in the market
- Polyform licences - attempt to be CC for software licences
- Distinction being osi approved is helpful
- Customers worry about source availability
- Compare to alternatives
- Similar to gitlab licence
- Benefits sales enablement
- Sean Bohan / Seanbohan@gmail.com

Defend Against ENSHITTIFIACATION Brainstorm: How can we build safeguards (governance) against the hostile spiral of anti-individual extraction?

Session Convener: Wendy Seltzer
Session Notes Taker(s): Rohit Khare, Drummond Reed

Tags / links to resources / technology discussed, related to this session:

Elinor Ostrom / commons

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

Utopian communities / Free usage as a sign of future risk

Drummond's notes:
Facilitated by Wendy Seltzer
Wendy started by explaining the term as coined by Cory Doctorow.

Marten brought up how large markets like Amazon

Todd Carpenter talked about portability of data, using "leaving Twitter" as an example. It is a huge challenge.

Harold Carr from Oracle Labs talked about incentives.

Kim Duffy from DIF talked about one of Cory's books that talked about how platforms can become almost sinister. In terms of how we get out of this current state, there are just a lot of questions.

Nara Lau from FISE Tech has a platform built on blockchain (Ethereum) and the user controls their own keys. Both companies and individuals are KYC'd.

Drummond spoke in favor of protocols not platforms. But that doesn't solve the incentives problem.

John Pritchard talked about Web 1.0 and Web 2.0 and security. His mother was a mystery writer, so he tends to plan for the worst, look for the best. He has eternal hope that we can do things right if we start to approach it from a systems perspective. He is inspired by Tristan Harris and his Center for Humane Technologies. Tristan advocates that when new technologies appear, we need to plan ahead for how they will be abused.

Marten said that can be a real problem, because it's hard to plan ahead. He used the example of when movies were invented, they showed trains crashing together and people ran out of the theatre.

Doc Searls believes an Intention Economy (name of his book) would be free of enshittification. He believes that the latter starts often starts with "freemium".

Jim Fenton pointed out that freemium is typically funded by VCs, and if the platform does not know how it will end out making money, then it will tend to go towards advertising and selling data.

Rohit Khare said that every time you share a link, you are "sharecropping".

John asked if it would be possible to have identity as a public good, so it is not within a commercial context. Something like Wikipedia or the eIDAS 2.0 initiative. So it could be something like public libraries, which are supported via taxes. Also public parks.

The same applies in some countries to healthcare. It eliminates the perverse incentives.

An anonymized encrypted AI agent that is double sided. One side is private, and one is public. And the public side can get spam but it is smart enough to filter it out.
The question then was asked: who owns the personal AI agent? What would be the incentive for someone to be able to build it. What's the business model. Nara would like it to become a non-profit.

"The very moment you outsource your rolodex to a social media service, you're in trouble."

Jim Fenton pointed out that public libraries are in trouble.

Wendy asked whether folks are interested in the platform cooperatives model. Can we build into the organizational structure of a platform the self-governance.

Harold said that in the end it comes down to good government and good people. He gave the example of Social Security coming out of a bad situation.

“You will get there through ‘good disasters’ that give us the motivation to make those changes.”

Enshittification is a natural outcome of profit maximization. It will continue until it collapses.

How can you incentivize people to look long-term?

How do we get away from KPIs that constantly get people to focus on short-term profits.

“Are we doomed as humans because we are being taken out of the loop in capitalist structures?”

There was discussion of DAOs that require constant attention and voting. That’s not necessarily the best way to have humans in the loop.

Wendy noted that, “Her notepad was enshittified from above.”

Rohit pointed out that there can be creative destruction. Enshittification is something that happens in many industries: cable TV, airlines, etc. Various different solutions can be brought to bear. One suggestion is regulation.

Rohit talked about envisioning a more positive future. “Cargo cult” is finding the right shape of change.

Doc said you can think of enshittification as “cancer”, progressing through stages.

Wendy asked Doc if there were examples from the Ostrom thinking about commons. However Doc pointed out that Ostrom studied the physical world, whereas we’re talking about the digital world. It is a very different state.

Wendy pointed out that the physical world has a “useful friction” that helps prevent many of the problems of the digital world. Jim used an example of postage for a letter. But he was NOT advocating “paid email”.

Samuel from Findynet considered two kinds of protection against enshittification:

1. protection against other companies being enshittified
    a. vote with your feet
    b. voicing your opinions on social media may make a difference
    c. you can try to create alternatives, Signal instead of a WhatsApp
2. protecting our own organizations, products, and efforts
    a. choose the right corporate structure
        i. Co-operative

   ii. [Kickstarter is a Public Benefit Corporation]
   iii. [MyDex is a Community Interest Company]
   iv. [ShareTribe has a steward-ownership structure]

b. perform periodic interventions to see whether your company is headed towards enshittification

Kim suggested a counterfactual analysis that could figure out what hasn't been enshittified and what that could teach us.

Mark brought up "stewardship" as a model.

Nara brought up a non-profit trust.

Rohit brought up the utopian communities and the process of "voice vs. exit". You can either speak up or leave. Those are the two options. The "leaving" option digitally is "homesteading".

Identity Dynamics 0 to 1 - Born w/out to Born w/in Human OS

Session Convener: Jeff Orgel
Session Notes Taker(s): Jeff Orgel

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

From @0 to @1 – Human Identity Extension Onto An Extra Worldly Realm

For decades I have witnessed and participated in the Human Experience (HX) of human presence being extended into a realm of 0's & 1's via connected systems.

These definitions apply to the following review.

@0 *- this refers to human experience before the natural world had connected & social technology systems.*

@1 *- this refers to human experience after the natural world had connected systems. This is the sun-rising of connected system technologies into daily life: when and how this arrives is very idiosyncratic to each individual.*

From @0 to @1 - Extension from Real World/Human eXperience (RW/HX) ONTO Digital Landscape (DL)

In the natural world (**@0**), people are designed to occupy a world of convergent forces: hot-cold, wet-dry, light-dark. The intellect in play exists in the sentient creatures – not one bit in the environment they exist in. Perfectly able and intelligent creatures are designed with capability responsive to the real-world sensor package they were born with. This sensor package allows them to discern what is happening around them. The better they could assess the challenge-scape of moment-to-moment circumstances, the more likely they would survive.

On the digital landscape (**@1**) the human animal occupies a realm of intellectual design where nothing (two words - NO THING) is naturally occurring. Everything (two words again – EVERY THING) is designed by intellect. Further it is designed by us. Who knows how to game us better than ourselves?! Who knows how to exploit human vulnerabilities of voyeurism, self-aggrandisement, sex, power, “free” and on it goes - better than us?! It shows…

The discordance occurring around this fact is extraordinary. Perfectly able and intelligent creatures from the physical world of **@0** are hobbled by not having a sensor package equivalents like smell, touch, gut intuition to discern what is happening around them in **@1**. The **@1** environment around them is immature, if not plain malicious, at being clear as to use of caution, implications of presence in such a framework and delivering trust.

This presentation was designed to put handles on thoughts with words regarding awareness of this interplay. It will also work towards identifying that people are trying to bridge these realms without clarity on the transitional, translational and symbiotic connections they will meet with in use of these systems.

The portion of human intellect which is occurring in people is unique for the above-mentioned reasons. I am calling that intellectual layer of understanding and management the HumanOSô.

Our Sessions covered ideas such as;

- Plato’s Allegory of the Cave – what we see on the wall vs what the wall sees of us (AK)

- Bi-directional interplay between Real World & Digital Landscape

- Framework structure: visual models (linear vs. stack model)

- Understanding the idea of building a Digital Twin from awareness of the implications of those ***Real-IT*** ® relationships – ***the relationship we chose to have, or not have, with connected technology systems***. This profile was identified as a variation of a Voo Doo Doll we make of ourselves.

- Identifying the impact of ***Real-IT*** ® choices, and reflection into, a person’s reality

- Concepts of managing system forces “in the room” including social media, data collection and predation such that a person’s intention is manifested with minimum to no risk of hazard or harm.

- Explored: Can we exist without identifiable presence? Can we be present without existing? The phrase “being in a place” where there is no actual “place” (BC)

Examples of Connected Social Systems (CSS) would be; Social Networks like Facebook, TikTok, Instagram, WhatsApp; Legal Records like State & Federal: Tax Filing, Personal Property Tax, Real Estate Tax, License Bureau; Knowledge & Discovery (YouTube search, etc.)

Operation on the DL (Digital Landscape): Extension eXperience (EX) occurs @2 >< @3 >< @4 creating feedback from EX INTO Real World RW/HX

@2* - **Real-IT** ®: understanding the presence of the relationship with technology as a symbiotic aspect/element in daily life to one degree or another. @2 is the layer where RW (Real World) & DL (Digital Landscape) are ever iterating. This is a critical layer.

@3 - **YouDoo Doll** - here you craft your VooDoo Doll (aka You Do Dollä): crafting (more or less so) of S.A.M. (Same As Me) This is where Real-IT® awareness meets with a variation of the martial art Aikido on the Digital Landscape. I call this Real-ITdoä. This is the idea that we are managing forces we often aren't in control of, or even aware of.

@4 - **YouX**: How is the Real-IT Yin Yang going? UI & UX experience feedback back returns to HX/RW more or less aligned with your intended outcomes (hope, expectation, trust)? Assess and go to @2 and iterate.

Presenting the same session once each day (an ***IIW Triple Play***) allowed for the following significant benefits;

- maximum opportunity for attendees to attend with minimum session conflicts regarding other valued sessions

- scaffolding refinement each day which elevated the model for the next day's attendees

- likely 3X the number of attendees during the particular IIW event

- great for advancing the pace of developing evolving edge space models as there is evolution at a higher rate since each day-group contributes to a revision one day after the next. IIW.38 r1, IIW.38 r2 IIW.38 r3

Other Notes regarding a ***IIW Triple Play***;

- calls for some presentation durability as it is an effort in triplicate

- reduces opportunities to attend one other session each day

Digital Identity Landscape (World Bank)

Session Convener: Christian Gray
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

NOSTR

Session Convener: Max Webster
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

The State/Role of Academic Research in Identity - open discussion

Session Convener: Evan Krul
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

Kaliya was not able to make the session but does have an annotated bibliography on digital identity that covers a lot of academic and non-academic sources.

https://docs.google.com/document/d/1uyvM9aIhVMJJ6Bl4jzFa9b6lO8Y_inSEN8Sd0W1TTQY/edit

Healthcare - Data, SSI, ID, Etc..

Session Convener: Leah Houston with Susan Stroud
Session Notes Taker(s): Susan Stroud

Tags / links to resources / technology discussed, related to this session:

HITECH
TEFCA
Kantara Initiative

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

Leah Houston, founder of HPEC, shared a view of American healthcare from the perspective of a Physician. After her physician credentials were stolen and used to commit healthcare fraud, she began her journey to create self-sovereign credentials for physicians with direct engagement and support from physicians.

Under U.S. Intellectual Property laws, health data created by a physician about a patient is owned by the physician.

The HITECH Act requires providers to make new patient medical data immediately available to patients in a 'useful' manner, but 'useful' is subject to interpretation and doesn't mean easy to use.

Susan Stroud, founder of Lifequipt, shared a view from the patient and caregiver perspectives. U.S. government mandates make patient data for Medicare, Medicaid, and VA health plans participants available via the Blue Button API (FHIR standard). Commercial health plans are exempt from the FHIR mandates so adoption is slow.

Physicians are demanding control over their medical credentials. Solutions, such as HPEC's credentialing platform, benefit the physician community, medical expenses, and the reduction of medical theft, waste, and abuse.

Patients and caregivers need tools to make sense of their health data, currently exposed via a myriad of disconnected patient portals, and share health data about themselves at their discretion. Digital wallets, like Lifquipt's Vault app, can make progress towards equipping patients with their full medical history.

DDID ecosystem development - Two Years of Lessons Learned

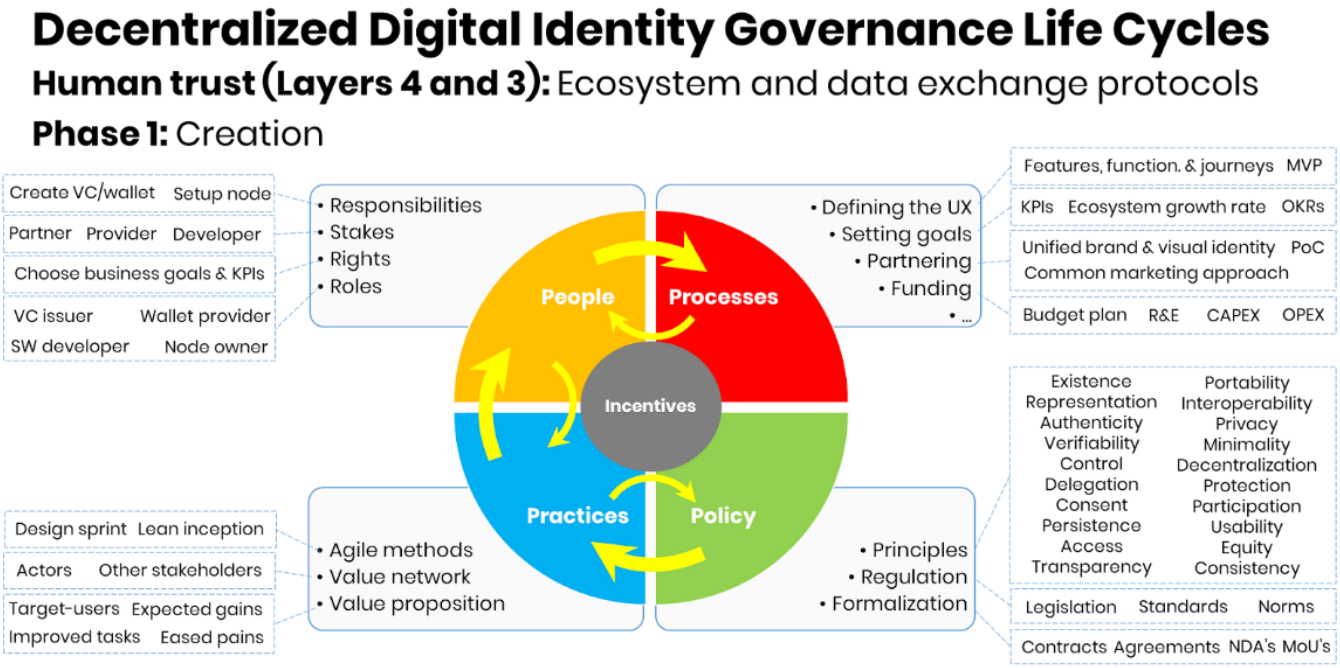
Session Convener: Ismael Ávila
Session Notes Taker(s): Ismael Ávila

Tags / links to resources / technology discussed, related to this session:

Decentralized digital identity governance frameworks; ToIP; IEEE working group.

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

The presentation covered the practical use of the governance frameworks from Trust over IP (ToIP) and IEEE to create and customize a governance model for real world decentralized identity initiatives in the areas of e-commerce and banking in Brazil. The created models combined the governance stack from ToIP with the life cycle view from the IEEE framework, so as to guide the sequencing of activities in four very distinct phases: creation, growth, operation and repositioning, and two rather different layers: human trust and technical trust. In the presentation, each life cycle phase was described in terms of the topics of policies (DDID principles, legislations, contracts, etc.), practices (agile methods, value proposition, etc.), people (roles, responsibilities, rights, etc.) and processes, as illustrated below. During the presentation the kinds of incentives applicable to each of the mentioned topics were discussed.



Decentralized Digital Identity Governance Life Cycles

Human trust (Layers 4 and 3): Ecosystem and data exchange protocols

Phase 1: Creation

Create VC/wallet Setup node
Partner Provider Developer
Choose business goals & KPIs
VC issuer Wallet provider
SW developer Node owner

- Responsibilities
- Stakes
- Rights
- Roles

- Defining the UX
- Setting goals
- Partnering
- Funding
- ...

Features, function. & journeys MVP
KPIs Ecosystem growth rate OKRs
Unified brand & visual identity PoC
Common marketing approach
Budget plan R&E CAPEX OPEX

Existence
Representation
Authenticity
Verifiability
Control
Delegation
Consent
Persistence
Access
Transparency

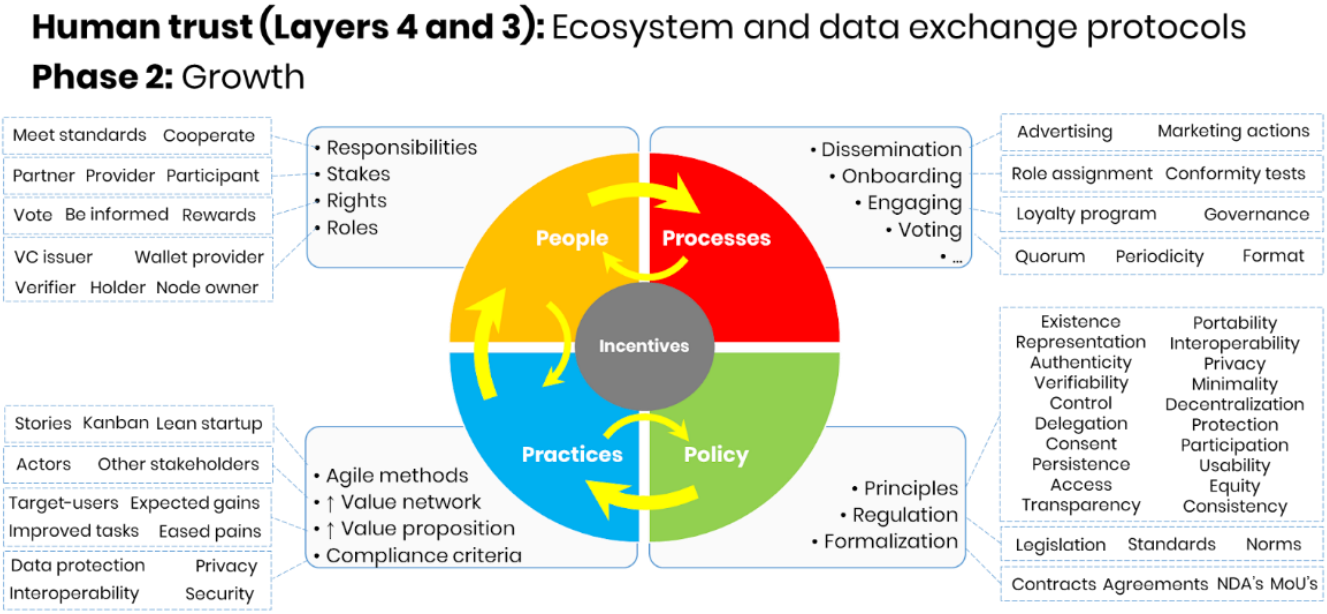
Portability
Interoperability
Privacy
Minimality
Decentralization
Protection
Participation
Usability
Equity
Consistency

Legislation Standards Norms
Contracts Agreements NDA's MoU's

Design sprint Lean inception
Actors Other stakeholders
Target-users Expected gains
Improved tasks Eased pains

- Agile methods
- Value network
- Value proposition

- Principles
- Regulation
- Formalization



Human trust (Layers 4 and 3): Ecosystem and data exchange protocols

Phase 2: Growth

SESSION #7

OpenID4VP and OpendID4VP over Browser API

Session Convener: Joseph Heenan, Kristina and Torsten
Session Notes Taker(s): Jin Wen; Albert Wu (screen shots)

Tags / links to resources / technology discussed, related to this session:

- Digital Credentials API explainer

- Digital Credentials (This document specifies an API to enable user agents to mediate access to, and presentation of, digital credentials such as a driver's license, government-issued identification card, and/or other types of digital credential. The API builds on Credential Management Level 1 as a means by which to request a digital credential from a user agent or underlying platform.)

- Digital Credentials API Web Platform and App Platform Layering / Interactions

- Linkedin Livestream

Slides: OID4VC_20240410_OSW.pptx-2.pdf

PR to review in OIDF DCP WG: https://github.com/openid/OpenID4VP/pull/155

work in W3C: https://github.com/WICG/digital-identities/blob/main/resources/DigitalCredentialsAPI-Layering-v20240301.pdf

OpenID for Verifiable Presentations (Highlights)

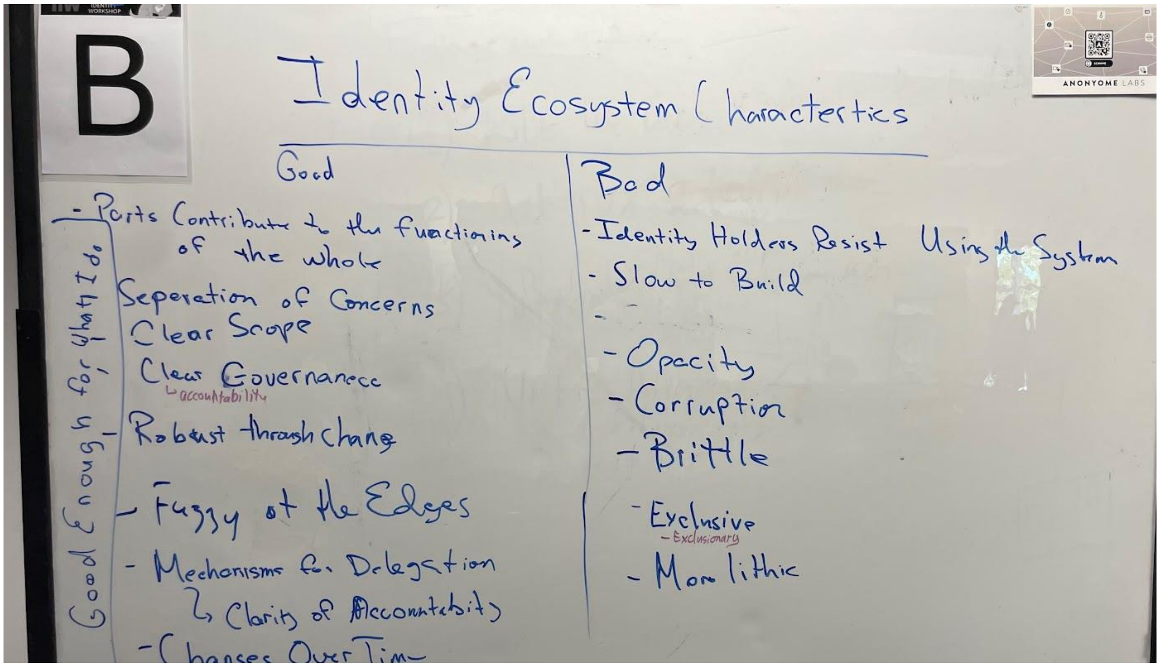
Same Device

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

Characteristics of a healthy identity ecosystem

Session Convener: Justin Richer, John Wunderlich
Session Notes Taker(s): John Wunderlich

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



Good Identity Ecosystem Characteristics

- Ports Contributor to the functioning of the whole
- Separation of Concerns
- Clear Scope
- Clear Governance
- Robust through change
- Fuzzy at the edges
- Mechanism for Delegation
- Change over time (evolution)

Bad Identity Ecosystem Characteristics

- Identity Holders resist using the system
- Slow to Build
- Opacity
- Corruption
- Brittle
- Exclusive
- Monolithic

Report Our + Winners Demo = DIF Hackathons

Session Convener: Limari @DIF, Ken Watanabe from WasedaU
Session Notes Taker(s):

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

The coining of Digital Innovation Lab and the experimentation to Digital initiatives were key to WIP.

How Might we… Normalizing Wallet Interactions - Open Discussion

Session Convener: Matthew Miller (Cisco)
Session Notes Taker(s): Matthew Miller + attendees

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

- Wallet interactions quickly extend beyond users accepting credentials into their wallets, and selectively disclosing information contained within.
- Training will be needed to educate consumers of VCs (e.g. a bouncer at a bar who needs to verify that someone is old enough to enter)
- What solution would help the bouncer do their job in a VC world? Separate scanner? Screenshot-deterrence features on the holder's wallet?
- Unclear which credential formats are "winners" to head off issues with holder's and verifier's apps not supporting the same document formats
- Look at what's been possible to achieve without VCs - why might they need to be injected into these processes?
- Stronger verification of supply chain qualities by nature of cryptographic signatures
    - Where is liability in this system?
    - Does liability transfer if someone doesn't catch a discrepancy somewhere along the line?
    - Interesting legal challenges are sure to come from this
- Also unclear how introducing tech into these existing processes support those without access to the tech
    - Perhaps quickly solving the problem with tech will leave more time for addressing scenarios in which tech is unavailable to the holder
- Hard to imagine a lot of the eIDAS stuff going on gaining traction in the US because of our resistance to a "national identifier"
    - Platforms implementing to EU regulations will probably transmit similar capabilities to e.g. US users by virtue of it becoming a platform capability
- Do people even think of "first-party platform wallets" as wallets in the way IIW attendees do?
- Not a lot of easy answers here, just more problems to solve

Autonomous Identity: Digital Identity for Humans & AI

Session Convener: Jeremy Frank
Session Notes Taker(s): Colby Anderson

(Apologies if the notes are incoherent, I'm just jotting things down as I hear them, not using correct grammar or providing enough context consistently)

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

The following notes are organized chronologically. Warning, these notes may be incoherent.

- Autonomous Identity = identities for both humans and AI agents
- Do they need "identities" or rather simply "identifiers", or even, "identifiers + asym. key pair". A consensus was reached here
- The precursor to autonomous identity seems to be "AI Authorization on Human's Behalf". And, perhaps it is out-of-place to talk about "autonomous identity" as such, and instead talk about "AI Authorization on Human's Behalf", and only touch on "Autonomous Identity" if it comes up as a valid solution to "AI Authorization on Human's Behalf". A consensus was reached here
- When do I care about "Autonomous Identities"? What is the scope? It is a bit unclear and vague. A consensus was reached here
- If "autonomous agents" require identifiers, perhaps they can be disposable. However, sometimes you might need correlation between an identifier.
- An "identifier" is a unique number within a group/set, whereas an "identity" is the collection of "identifiers, attributes/credentials, relationships" that belong to a single entity. An identifier is concrete whereas an identity is not. The discussion on the difference here was talked about for a bit.
- "An identity is only good for one thing — knowing who to put in jail" (aka accountability) - Alan Karp
- AI is just a tool. It doesn't have an identity.
- Every use-case is different. Sometimes, AI shouldn't have identifiers in some cases, and perhaps should in other cases only insofar as it is correlated to me-the human controller. A consensus was reached here
- Perhaps there should be an identifier for AIs, simply to know the kind of AI we are dealing with, aka the model, or perhaps whether it passed "certain safety checks"
- We still want to preserve anonymity. And identifiers for AI (that connect you the human to it) may compromise this.
- Instead of proving you are human, prove that you (the AI) are representing a human
- What about accountability? What if an AI car hits a human? Perhaps this issue can even be extended into regular software? What if a bank, through my unintentional or accidental doing, transfers money from someone else's account into my account? The discussion was talked about for a while.

- Lots of people may be accountable. There is a chain. The AI, the human controller, the provider of the AI, the software that the AI provider used, etc. Analogy — a car accident and everyone blames the car in front of them until the end of the line is reached.
- Another interesting use case for accountability is AI that is used to develop production code.
- Access-tokens can be assigned to roles. Roles can be generalized perhaps to include many access-tokens per role.
- How can you develop trust in AI? Is trust ever possible? Is it possible to build trust?
- An analogy to the rate of growth of AI is — AI (in reasoning capabilities) is growing at the rate of a child. Perhaps it is 8 years old now.
- What kind of infrastructure would be relevant to giving AI identifiers? Perhaps, KERI, perhaps TrustOverIP,
- If we were using DIDs, my DID document would have a method for information on how to sue me, or else you wouldn't do business with me
- DIDPeer can be a DID identifier that only be used between two people
- Intentionally sharing a private key. This should be considered when using DIDs for accountability. People should only give their private key to an AI, if they have a way to hold the AI accountable or transfer liability in a delimited capacity to the AI.
- DIDWebS could be an alternative to KERI that is relative to this discussion
- As a business strategy, perhaps the development of standards should be avoided

The “LAWS” of Externalized Authorization

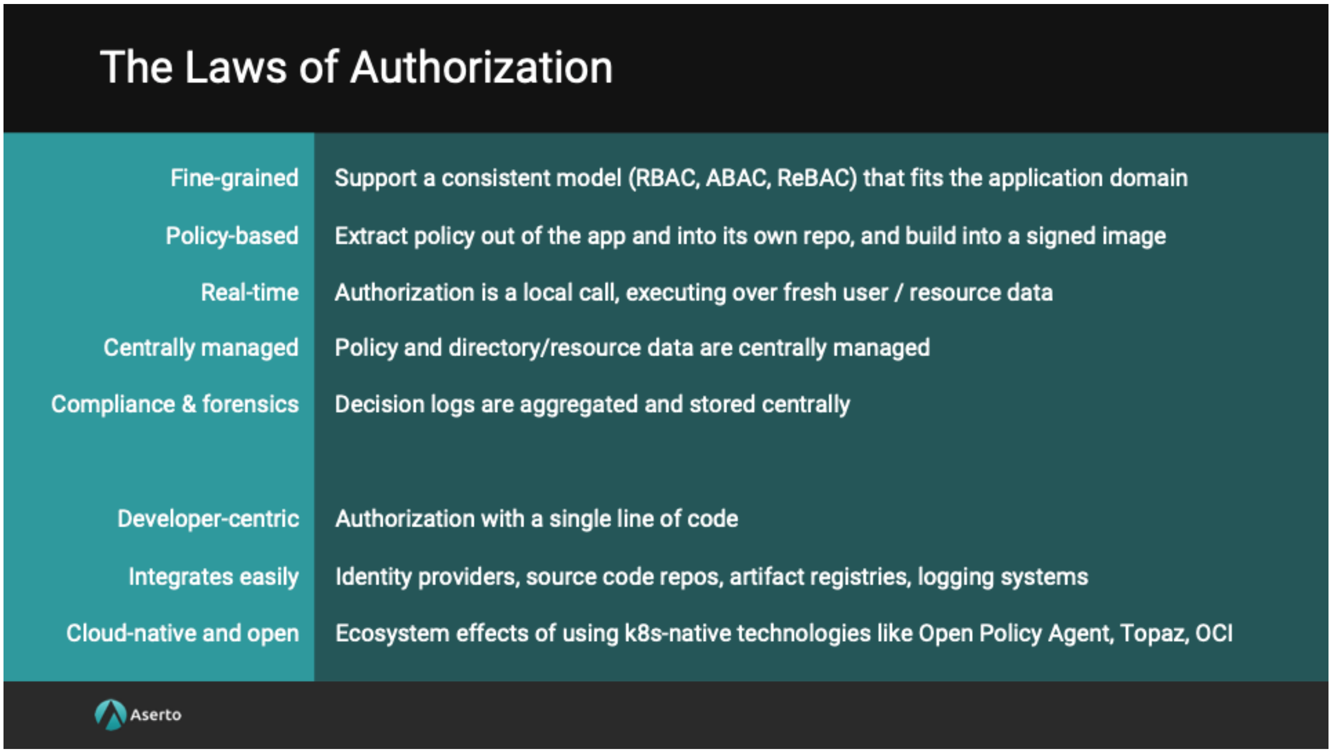
Session Convener: Omri Gazitt
Session Notes Taker(s): Omri

Tags / links to resources / technology discussed, related to this session:

- Omri’s Deck
- Cross-references from AuthZ meetup notes

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

- We had a good discussion about the motivations behind externalized authorization
- Deeper dive into “fine grained”, “policy-based”, and “real-time”
- Proposed “Laws of Externalized Authorization”



The Laws of Authorization

Fine-grained	Support a consistent model (RBAC, ABAC, ReBAC) that fits the application domain
Policy-based	Extract policy out of the app and into its own repo, and build into a signed image
Real-time	Authorization is a local call, executing over fresh user / resource data
Centrally managed	Policy and directory/resource data are centrally managed
Compliance & forensics	Decision logs are aggregated and stored centrally
Developer-centric	Authorization with a single line of code
Integrates easily	Identity providers, source code repos, artifact registries, logging systems
Cloud-native and open	Ecosystem effects of using k8s-native technologies like Open Policy Agent, Topaz, OCI

Aserto

DID DHT 6 months later

Session Convener: Gabe Cohen (Block/TBD)
Session Notes Taker(s): Gabe Cohen

Tags / links to resources / technology discussed, related to this session:

Covered content present in: https://did-dht.com/ and https://developer.tbd.website/blog/did-dht

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

Identity of Media - Channels & Brands +PART II+

Session Convener: Olaf Steenfadt and Todd A. Carpenter
Session Notes Taker(s): Todd A. Carpenter

Tags / links to resources / technology discussed, related to this session:
ISO
International Workshop Agreement #44
National Information Standards Organization (NISO)
ISO Technical Committee 46 - Information & Documentation / Subcommittee #9 - Identification & Description
Background on IWA Proposal (via ANSI)
Global Media Registry

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

This session was a follow-up conversation related to the introduction to this project on Day 1. See the notes from that session for background on this project. Also note, that this conversation was ongoing in a Day 2 / Session 8 session in the same space. These notes describe the conversations of the two back-to-back sessions on Day 2. - They are duplicated there.

The discussion began with a description of the value of media identification. Why might we want to understand who owns a company or media channel. There is a lot of ambiguity in the media landscape. For example, consider Al Jazeera. A lot of people know what it is, yet they own 18 different channels, which are quite different. Other examples include “What is Phoenix”? or the number of companies that are named “ABC” is nearly limitless. Nothing stops organisations from (or bad actors) creating an online channel and how do we manage this flood of entities. Can we

build a systematic approach that helps to address the problem of impersonation, Information integrity
and brand integrity.

In February of 2024, an ISO project was launched to develop a unique media identifier (UMID). The project aims to create a new identification structure to identify media channels and brands. This project includes three active subgroups looking at:

Group 1 - Syntax - Use cases
Group 2 - Governance
Group 3 - Validation and security & safety

The project aims to connect to existing identifier systems. In those different domains. such as the C2PA project. To distinguish the two efforts, for example, C2PA identifies the actual content object. In the C2PA data model, the source identity tag is missing guidance on what to include. It might or might not be a legal identity. We've also discussed the role of GLEIF - VLEIF, which produces its own sub-entity identification model However, this project isn't looking at corporate entities, it is exploring brands and channels.

The session described a number of potential use cases, including:
Trust Networks - based on verifiable identity
Business/Analytics/Tracking
Research - academic study
Regulation development and enforcement
Civil Society analysis and study

A critical aspect of this project will be to accurately describe the referent, that is the entity being referenced by the identifier, and the level of assignment in the corporate hierarchy of a media entity.

The conversation also covered set of ways that the identifier might be modelled. We're presently envisioning three assignment paths for the identifier. The first is Observed assignment, which is a model where 3rd Paries may assign a UMID, where a publisher has been observed as creating some content but has not yet been identified. The second is Declared assignment, which is where the Corporate entity registers (self-asserts), where the publisher declares itself owner of an outlet/ a channel/a brand. The third approach is Confirmed/Validated in which an Accredited issuer assigns the identifier. In this model, a publisher is verified by an issuing body, such as a regulator or agency. For each of these different types of assignment models, there would be different types off metadata, vetting, or possibly validation (such as signing certificates may be associated with these different levels. There could be different issuing pathways for each type. The benefits and challenges of each of these approaches were discussed in detail and the convenors appreciated the feedback, which will be brought back to the IWA team.

Further discussions included AEGIS - issuing tokens that are looking to deploy telecommunications IM systems. Solutions such as Cryptid - Cam, were also discussed as well as the problem of bad actors. The complexity of medical IDs was also considered. Methods of verification, certification and validation were also considered.

The business and advertising use cases were also discussed in detail. The regulatory environment in the EU and the US were discussed and compared. The existing work of the C2PA and the Creative assertions community group - CAI (Creative Assertions) were discussed and it was noted that there are ties between the IWA and the C2PA, LEIF and GS1 were noted, but it was acknowledge that better information sharing is welcome and the suggestion on how to improve communication would be brought back to the IWA group.

Additional use cases were discussed and scenarios were considered. The convenors appreciated the feedback and suggestions from all the participants in the sessions. Advances related to the project will be shared with the IIW community moving forward.

Trust Registry FACE OFF!!

Session Convener: Andor K, Mathieu Glaude, Sam Curren
Session Notes Taker(s): ??, Martina Kolpondinos

Tags / links to resources / technology discussed, related to this session:

A later session in IIW 38 on OpenID Federation: https://docs.google.com/document/d/16-E9M32jPqkdKJebiqxoJq2u05Uq9z7E4jSqOhHX_gg/

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

Overview Of Conversation

x509	**IETF**	Common and works but not flexible and not context specific.
Northern Block		Working implementation leveraging DNSSec for higher trust assurances.
DIF Credential Trust Establishment	**DIF**	Decentralized Data Model.
EBSI Trust Chains		Presented by cheqd with an implementation. Long term persistent layer for trust infrastructure.

OIDF	**OpenID**	Good penetration in some countries. x509 compatible.
Trust over IP Trust Registry Protocol v2	**ToIP**	RESTFul API based approach with Governance and Requirements Information. 80/20 rule.
did/whois		
TRAIN		
W3C Verified Issuer / Verifier Verifier List Data Model	**w3c**	

Introduction

- Brief discussion about what a trust registry is and why it's important
    - After the cryptographic verification happens the question comes to how do you trust an issuer (and verifier) => binary decision on whether we accept a credential or not.
- Trust over IP list of requirements for trust registries is useful for evaluating implementations

Implementations

x509

- Used for global drivers licence authority
- Pros
    - Common and works
- Cons
    - Not flexible
    - Not context specific

Northern Block (https://trustregistry.nborbit.ca/)

- A webapp that stores DIDs in a centralized database.
- Correlates trust registry DIDs with domain names using DNSsec
- Authorized issuers, verifiers, and wallets
- Includes a registry of registries
    - Creating a new trust registry creates a public website for the trust list
- Lists are exportable (csv, json)
- Roadmap includes interactions via DIDComm to interact with the trust registry in a privacy preserving way

DIF Credential Trust Establishment

- Credential Trust Establishment 1.0
- Data model, not a protocol or interaction model
- Create the document, and host it behind a URI
- No centralization: gets distributed with the credential with no phone home of any kind
- Built on DIF Trust Establishment specification, but has specific items for credentials

- Allows roles for each participant
- Can provide synonym DIDs, e.g., when using several DID Methods
- Very lightweight (create the file, sign it, host it)
- File has a versioning in it
- no "phoning home" as the entire file is downloaded
- is being applied with slight variations by Indicio (i.e., it's not just theory)

EBSI Trust Chains

- Tracks “Verifiable Accreditations”
- Used by cheqd (i.e., it's not just theory)
- Governing authority for the ecosystem has a DID on a blockchain, and tracks DIDs that are authorized for specific actions
  - Uses DID Linked Resources: Verifiable Accreditation => Session 9, C
- Optional root of trust via X.509
- Only (?) for organisations due to privacy considerations

Trust over IP Trust Registry Protocol v2

- Version 2 is in implementor’s review: April 2024
- ToIP Trust Registry Protocol v2 TF DRAFT (trustoverip.github.io)
- RESTful API
- Query API that standardizes how to query which entities are authorized to do what in which context
  - No write or update operations
- Some concerns with Trust Registry lookups requiring a “phone home” depending on the implementation
  - Trust Registry could track which credentials are used by which verifiers
  - Could cache queries
- Anything that is in the trust registry can be issued as a credential—complimentary with VC based decentralized trust

OpenID Federation Trust Registries

- OpenID Federation 1.0 - draft 34
- OpenID Federation 1.0 presentation
- Already used in systems around the world
  - University network
  - 2 identity networks in Italy
  - Brazil open banking
- Each entity can provide trust lists, including common trust anchors with other lists
- Accreditor provides trust marks
- Going up the trust chain

Train

- train.trust-scheme.de/info
- EU SSI work: Fraunhofer Institute
- DNS Based

W3C Verified Issuer / Verifier Verifier List Data Model

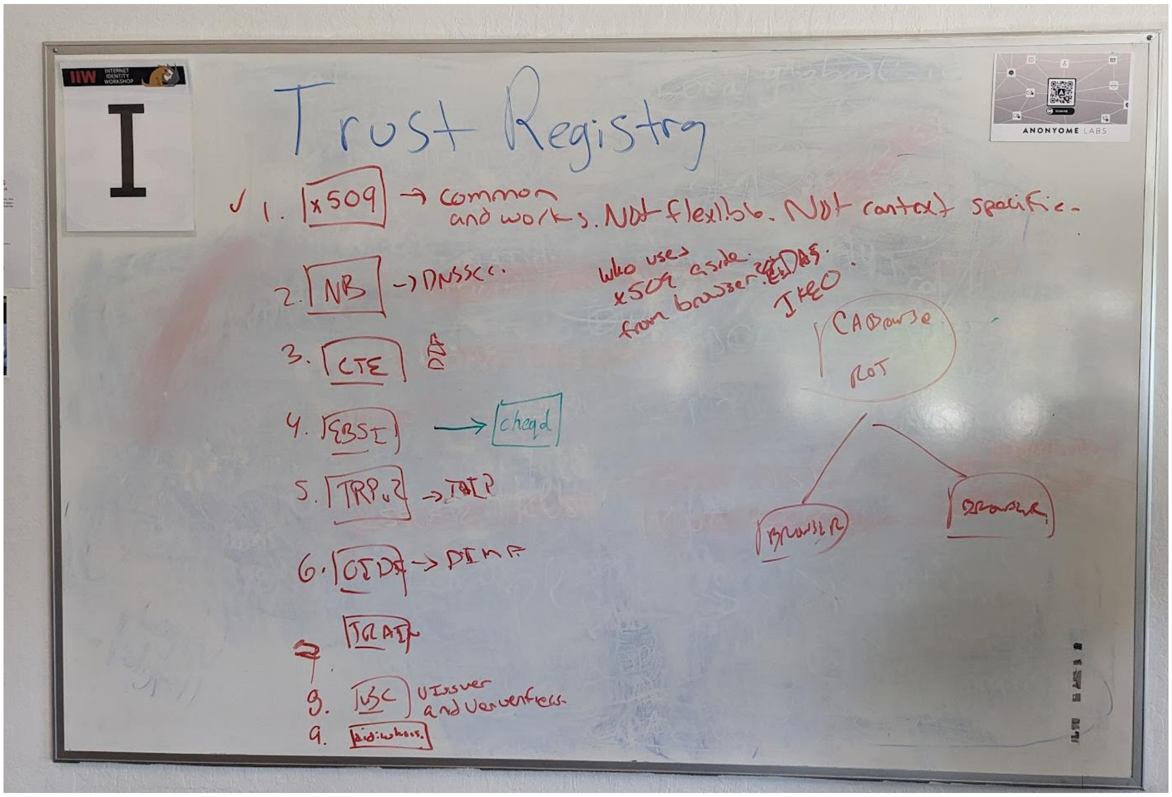
- https://w3c-ccg.github.io/verifiable-issuers-verifiers/

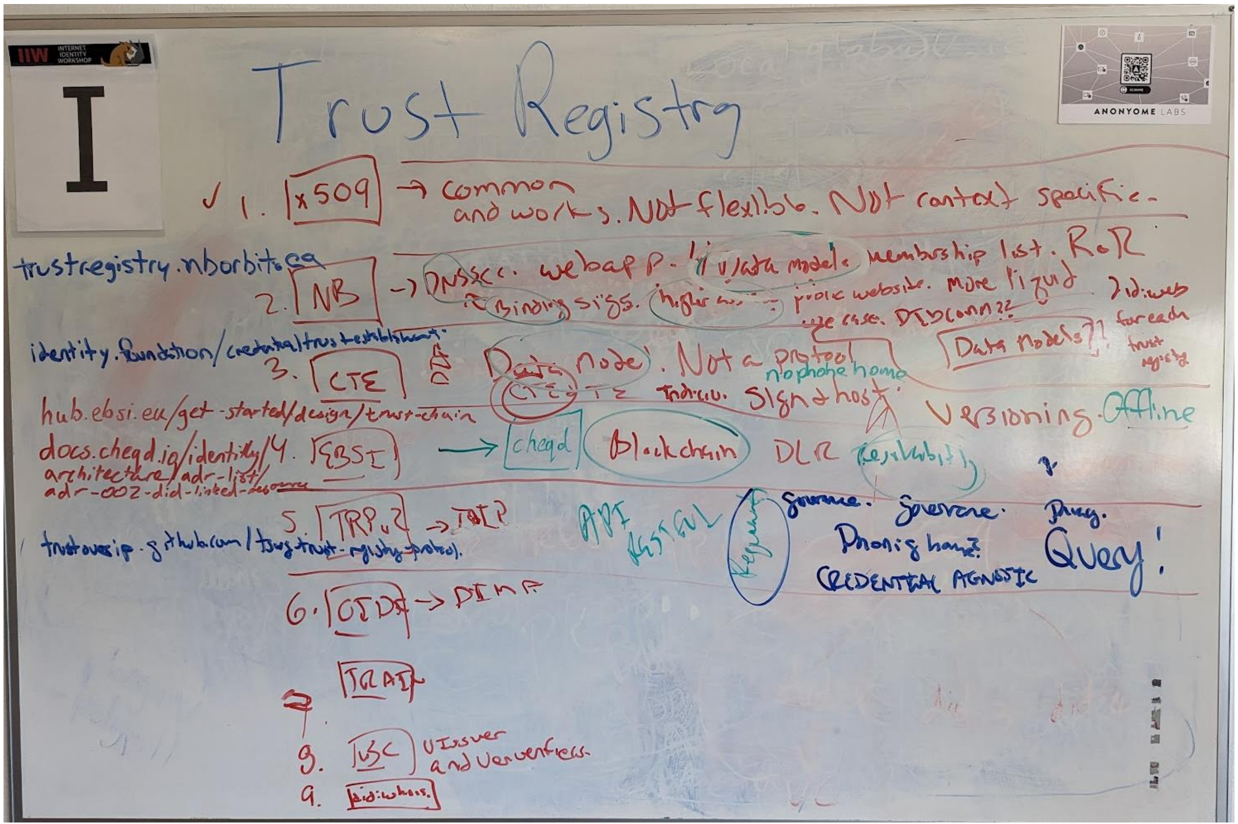
did/whois

- endpoint (in DIDDoc)

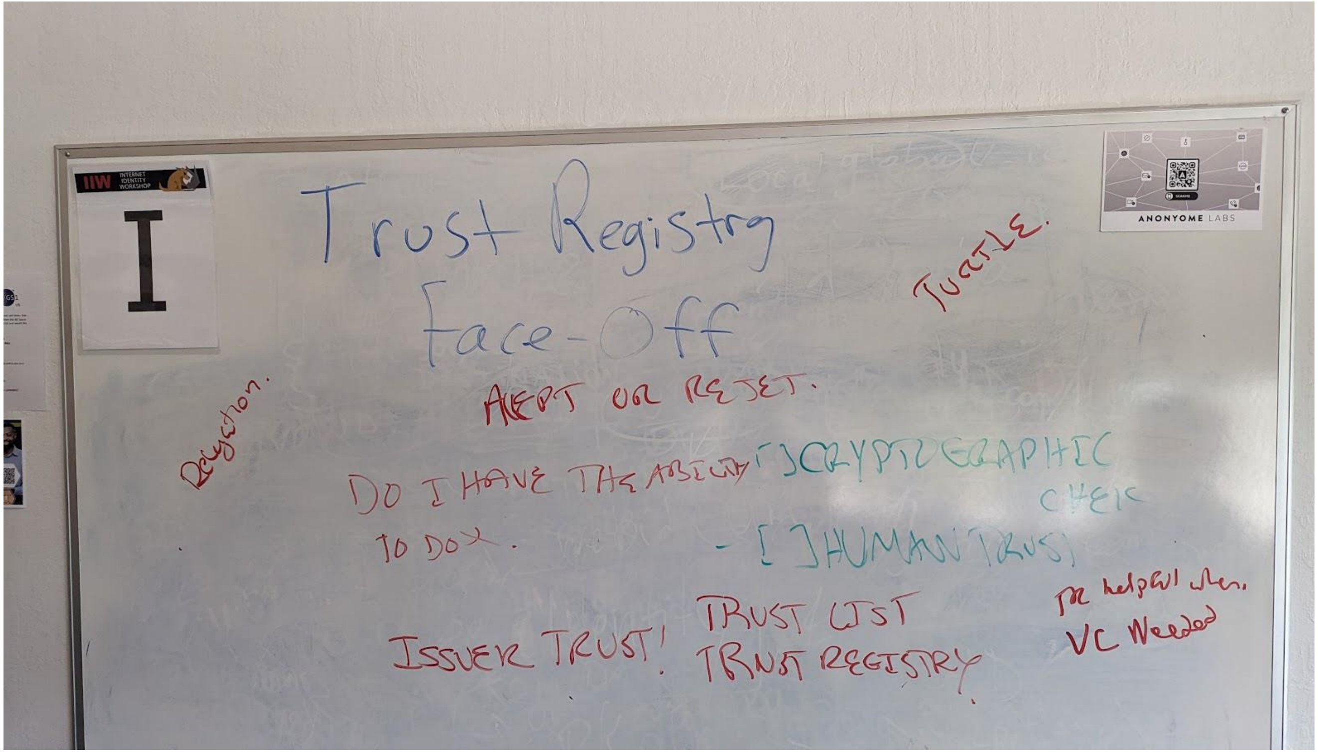
Discussion

- Do these approaches replace x509 or compliment it?
  - Designed to replace in functionality, but allows implementations to compliment x509
- Queries have to be sensitive to dates of queries: who is trusted today versus previously
- Each implementation targets a different part of the solution. Would be good to map how they fit together.

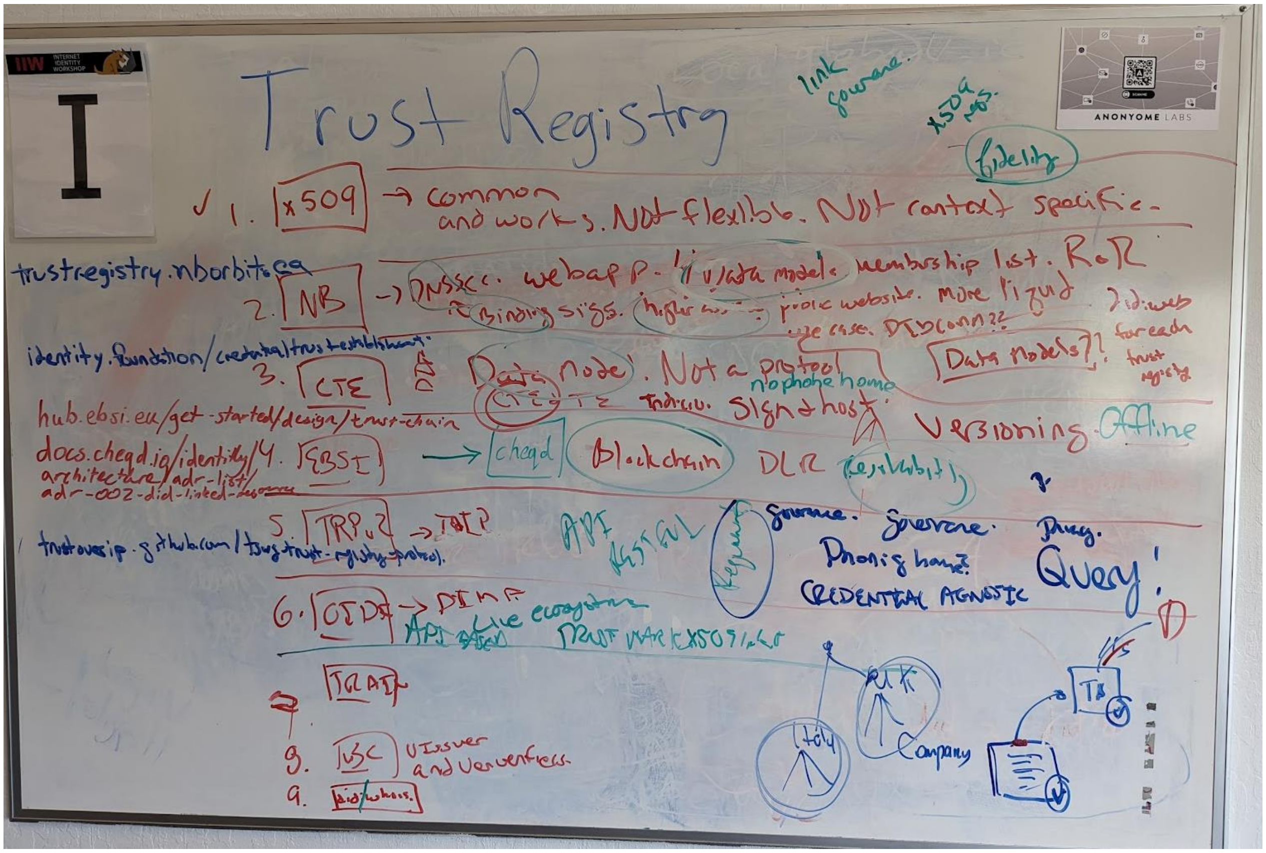

I
Trust Registry
✓ 1. x509 → common and works. Not flexible. Not context specific.
2. NB → DNSSEC.
3. CTE
4. EBSI → cheqd
5. TRP v2 → TAP?
6. OIDF → DIMA
TRAIN
8. VISC VIssuer and Verifiers.
9. did:whois.
who uses x509 aside from browser? eIDAS. ICAO.
CA Browse ROT
Browser
Browser
ANONYOME LABS



IIW INTERNET IDENTITY WORKSHOP
I
Trust Registry
✓ 1. x509 → common and works. Not flexible. Not context specific.
trustregistry.nborbit.ca
2. NB → DNSSEC. webapp. v data model. membership list. RoR
Binding sigs. higher ... public website. More liquid use case. DIDComm??
?did:web for each trust registry
identity.foundation/credential-trust-establishment.
3. CTE Data node. Not a protocol
CTE TE Individ. Sign & host.
no phone home
Data models??
Versioning. Offline
hub.ebsi.eu/get-started/design/trust-chain
docs.cheqd.io/identity/architecture/adr-list/adr-002-did-linked-resource
4. EBSI → cheqd Blockchain DLR Resolvability
5. TRP v2 → ToIP?
trustoverip.github.com/tswg-trust-registry-protocol.
API RESTful
Request
Governance. Governance. Query.
Phoning home?
CREDENTIAL AGNOSTIC
Query!
6. OIDF → DIMP
TRAIN
7.
8. TVSC v Issuer and Verifiers.
9. did:whois.
ANONYOME LABS



IIW INTERNET IDENTITY WORKSHOP
I
Trust Registry
Face-Off
TURTLE.
Delegation.
ACCEPT OR REJECT.
DO I HAVE THE ABILITY TO DO X.
[ ] CRYPTOGRAPHIC CHECK
- [ ] HUMAN TRUST
ISSUER TRUST! TRUST LIST TRUST REGISTRY
Be helpful when VC Needed
ANONYOME LABS


IIW INTERNET IDENTITY WORKSHOP
I
Trust Registry
link governance.
x509 roots.
fidelity
ANONYOME LABS
✓ 1. x509 → common and works. Not flexible. Not context specific.
trustregistry.nborbit.ca
2. NB → DNSSEC. webapp. data model. membership list. RoR
Binding sigs. higher ... public website. More liquid use case. DIDComm??
did:web for each trust registry
identity.foundation/credential-trust-establishment
3. CTE Data model. Not a protocol. no phone home
Data models??
Individ. Sign & host.
hub.ebsi.eu/get-started/design/trust-chain
docs.cheqd.io/identity/architecture/adr-list/adr-002-did-linked-resources
4. EBSI → cheqd Blockchain DLR Resolvability
Versioning. Offline
5. TRP v2 → TAP?
trustoverip.github.com/tswg-trust-registry-protocol
API RESTful
Request
Governance. Governance. Privacy.
Phoning home?
CREDENTIAL AGNOSTIC
Query!
6. OIDF → DIMP
API BASED Live ecosystems
TRUST MARK X509 like
TRAIN
7.
8. VSC VIssuer and Verifiers.
9. did:whois
Italy
Company
TR

MOSIP - Modular Open Source Platform - An Exploration & Report from Their Connect Conference

Session Convener: Kaliya Young
Session Notes Taker(s): Kaliya Young

Tags / links to resources / technology discussed, related to this session:

Key Differences Between the U.S. Social Security System and India's Aadhaar System

https://identitywoman.net/wp-content/uploads/Aadhaar-MOSIP-for-IIW-38.pdf
MOSIP, the Unneglectable Force in the Global South
A bumpy road to becoming an open identity infrastructure: MOSIP Connect 2024 in retrospect

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

Kaliya travelled to India in 2019 to Study Aadhaar as an India-US Public Interest Technology Fellow.

Key Differences Between the U.S. Social Security System and India's Aadhaar System

She wrote a paper coming back from that trip. And also did some presentations about the overall system.

These were the slides she presented at the session.

- the first ½ the deck is about Aadhaar.
- the second ½ the deck is about MOSIP.
- https://identitywoman.net/wp-content/uploads/Aadhaar-MOSIP-for-IIW-38.pdf

There were also key developments that MOSIP is actively integrating with two other open source projects that provide real value to resident/citizens.

The Integration with OpenCRVS

- The Open CRVS team was at MOSIP and presented extensively
- Here is a video demoing the integration (similar demos were shared on stage and at their booth) -https://www.youtube.com/watch?v=1dtM5ve0qA8

Integration with OpenG2P which is focused on getting money from the government to specific people (They could be employees or they could be just residents in a social benefit program).

OpenG2P is now a sister project with IIIT Bangalore next to MOSIP.

Lucy and I wrote two different pieces about MOSIP one before I went to MOSIP Connect and one I wrote after the conference for PAYPERS.

MOSIP, the Unneglectable Force in the Global South
A bumpy road to becoming an open identity infrastructure: MOSIP Connect 2024 in retrospect

The Five Rights of Secure Health Data Exchange

Session Convener: healthKERI (Jared J., CEO & Phil Feairheller, CTO)
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

Slides for this presentation can be accessed here:
https://docs.google.com/presentation/d/1W0hzEKJYJKV8641UJQta3yE0K3D0m_rC0mNwCJrUMtk/edit?usp=sharing

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

SESSION #8

Discussion on USER/HOLDER BINDING Mechanisms & Proposal for CLAIM BASED BINDING

Session Convener: Paul Bastian
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

https://docs.google.com/presentation/d/1Vjr71kiXkfktj_gkMlRd-sAjU9UGKYET4F1dUREcMSE

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

Four Categories of User Binding
Biometric Binding

Process
- Issuers embed biometric reference as a claim in the credential
- Verifiers compare biometric probe with reference

Challenges
- privacy and impact of leaked biometrics
- security and authenticity of the biometric data (low assurance)
- compatibility of biometric components
- lacking standardization for VCs

Benefits
established, well-understood mechanism from analogue world
Primary Use Cases
- proximity use cases, e.g. visual check with mDL
- closed loop use cases (issuer = verifier), e.g. physical access to gym with face biometry

Primary Use Cases
- proximity use cases, e.g. visual check with mDL
- closed loop use cases (issuer = verifier), e.g. physical access to gym with face biometry

Claim-based Binding

Process
- Issuers embed comparable data into credentials as claims (usually PII)
- Verfiers compare these claims with Identity Credentials or existing
master data/registry

Challenges
- requires disclosing many claims (privacy issue)

• lacking standardization and semantics
=> automatic Comparison may be prone to errors

Primary Use Cases

• majority of all existing analogue and digitized processes

Privacy-enhancing Variation

• Usage of dedicated linking attributes instead of PII data
→> current research topic within IDunion project

Cryptographic Binding with proof-of-procession

Process

1. Issuers bind Credential to asymmetric key pair
• public key embedded as attribute in credential
• private key under control of the user inside WSCD
2. proof-of-possession for presentation of the credential

Security-relevant Factors

• Storage and execution of the private key
→ Exportability and Duplication
• Unlocking of key usage through user authentication
• PIN, local biometrics, retry counter

Challenges

• Level of Assurance (LoA) => increasing security requirements to WSCD
• Credential is bound to the Lifecycle of the WSCD
• Portability / Change of Wallets is difficult

Cryptographic Binding with proof-of-association

Process

• The process works similar to proof-of-possession, additionally:
o various credentials are bound to keys from the same WSCD
• WSCD can create a proof during issuance and presentation that two or more keys belong to the same cryptographic device (proof-of-association)
• Issuer of an Attestation Credential proofs first the PID of the user and issues credential bound to key associated to the PID

Challenges

• Even higher requirements to the WSCD
o not compatible with native smartphone key stores (no association)
• CloudHSM/JavaCard on Secure Element is possible
• requires governance strategy to make this an efficient user binding
o high degree of implicit assumptions
• Backup & Recovery strategy may be difficult

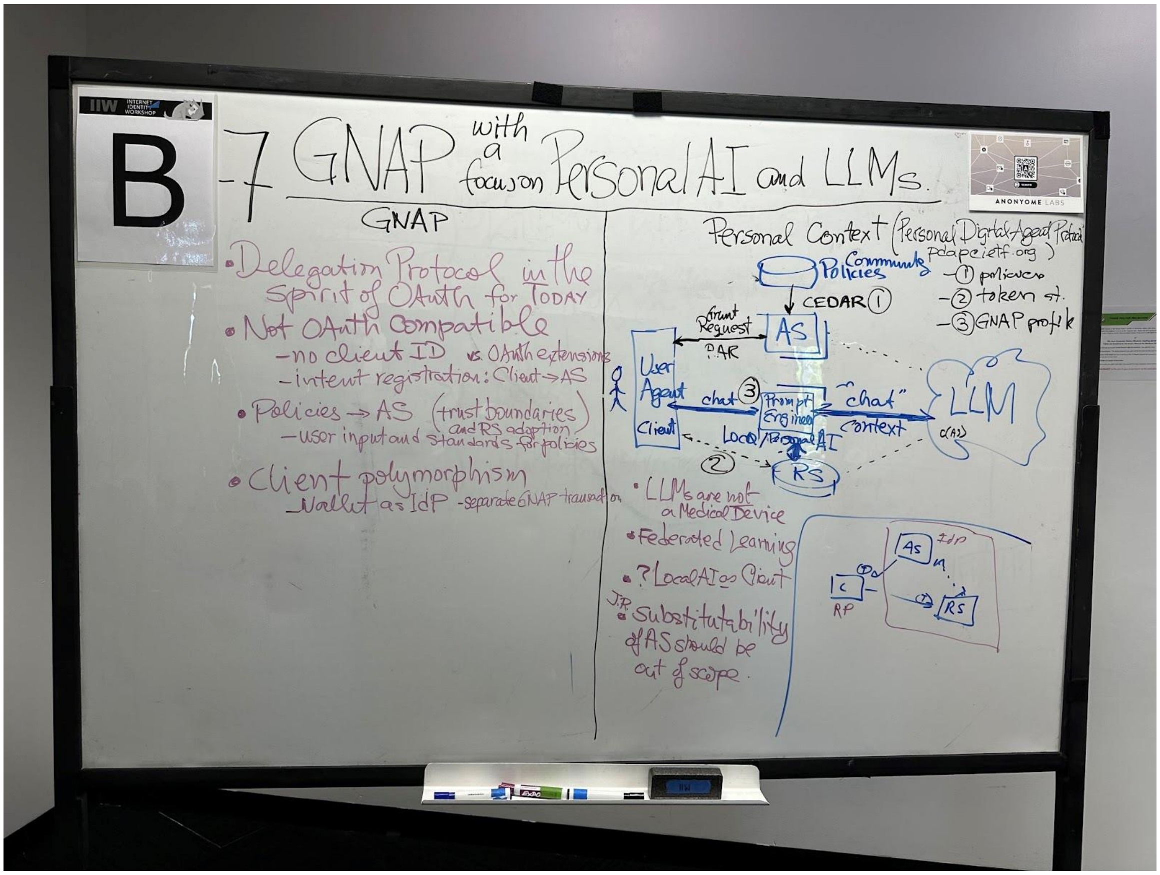
=== START Transcript via OpenAI Whisper and Perplexity summarise===================
Omitted: the tools are not intelligent enough to understand this conversation to our satisfaction.
=== END Transcript via OpenAI Whisper and Perplexity summarise===================

GNAP with a focus on Personal AI and LLMs

Session Convener: Justin Richer and Adrian Gropper
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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



B-7 GNAP with a focus on Personal AI and LLMs.

GNAP

- Delegation Protocol in the Spirit of OAuth for TODAY
- Not OAuth compatible
  - no client ID vs. OAuth extensions
  - intent registration: Client → AS
- Policies → AS (trust boundaries and RS adaption)
  - user input and standards for policies
- Client polymorphism
  - Wallet as IdP - separate GNAP transaction

Personal Context (Personal Digital Agent Protocol pdap@ietf.org)

- ① policies
- ② token st.
- ③ GNAP profile

- LLMs are not a Medical Device
- Federated Learning
- ? Local AI as Client
- J.R. Substitutability of AS should be out of scope.

- The request processing RO-AS must pass a request to the RS-AS as an extension to GNAP requests
- The token format between RS-AS can be out of scope for PDAP
- CEDAR is useful for substitutability of the RS-AS should be in-scope
- Profiling GNAP should include sequential use of two GNAP flows

SSI?VCs Not Dead (yet) : Hot takes and lessons learned from assi/VCs Consulting

Session Convener: Lucy Yang
Session Notes Taker(s): Kaliya Young

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

The “business person” working with Kaliya in a consultancy.
Lucy is a business operator.
Many skills to help shape business, Marketing, Sales.

Helped a Friend with their outdoor business Development over Christmas to re-work membership model and it doubled.

Strategic Collaborations.

Who are our clients?
Interested decentralised identity - help you succeed.
Way selecting clients.

We want to take our whole industry forward.
Clients we think are critical to the industry.

Starting third year - sustainable recurring revenue.

How define going well - “knowing what does not work for them”
Hypothesis - with different clients.

Large Enterprise Client - market research.

Lucy challenges working with Kaliya.
Representative of the general community.

Advocate -> have strong opinions.

Sit and listen to the clients to meet where they are today.

Pulled Kaliya out of the working group participation.
Step out - figure out what is going on in the Market.

- Reilly - venture-capital-backed product company, you are not going to survive by selling SSI/VC

- While SSI/VC companies are spending time in community groups and fighting over interoperability and ideals proprietary solution providers, such as Clear, Persona, Yoti etc. capturing market shares because they are focusing on addressing today's pain points using whatever works.

SSI/VCs community has a problem understanding how normal human mind works
<3 engaging with emerging technology -
Positive thing - so many intelligent people - so many things in your mind.
How many ideas do you want to communicate in one presentation?

Communicate one compelling idea - not need to get into so many things.
How communicate complicated technology simply.

Important to understand where our clients are coming from.

Covid Credentials - this is our chance to grab the market - reasons. I don't think the tech was ready enough.

Kaliya led Good Health Pass Collaborative - so complicated…could not digest it.
AT linux foundation - took one piece of that entire comprehensive - try to take it to market - foundational infrastructure.
Took into UNDP - supporting WHO - took over all the work over government - will interoperate on health credentials.
Challenge explaining to policy makers to get them to give us money.

SSI/VC community has a problem understanding how capital/money works.
Related to first challenge.
Must listen to folks about where they are at.
There is a sliver lining.
Bigger clients are coming - interested because this seems like it is coming.
Need to have a clear problem to link technology too.
Very simple specific problems.
They don't give you a lot of money because it is a small problem so far - research.
Come with a vague problem - work on job description.
Go through the procurement.

Industries that can't afford not to use standards.
eIDAS 2.0 - legislation in place
Money will be in the market that we can grab as consultants.

Is there a problem? <- core question

If we don't have companies that reach a billion dollar valuation.

Few community roles would be good for us - looking for companies to sponsor us.
So we get bigger as an industry give back

Deliver things that create value for people today - we need to be able to get the money for this.

SSI/VC community has problem with talent.
I will make a lot more money not in this space.
Business generalist - don't have to be into this space.
I'm mission driven and like solving hard problems
Can we attract business talent?
Understanding the community and working directly with developers.
Wrap heads around
Lucy is lucky to work with Kaliya - because she knows so much and so many people.
Highly intelligent folks - create a high barrier to entry.

Ecosystem building.
Can we find consultants on our consultants' projects.
Senior technical architect - who is also a very good communicator - coordination with clients.
Want technical expertise.

Find people who know technology - know good enough.
So many conversations with stakeholders at big companies. Somebody in a department can't sell it up the chain to business stakeholders.

Consultant - She is getting into the space - and is working on

How do we train people?
Tied into the money problem.
If as an industry we don't capture enough market share how do we capture talent?

Q&A
Do the hot takes reflect the challenge

A: "Community organisation"
More tech driven then business organisations.

Tech leader leaning - have lack of lack of strategic thinking.
How use resources to move the conversation and industry forward with limited strategic resources.

Our clients can bring so much value.
Should work with us to help us execute.

Community organisations unwilling to do strategy.
Lets get a newsletter/article out.

We did our sponsorship projects - writing.

Community organisations - should be run as a startup.

Organization and Community
Community open
Organisation must have a preferred child.

Put one article - must talk about one thing - must matter more to audience - value to audience and build momentum.

Build tech and build interop.
Ecosystem work.

Interoperability - who do you want to connect to.
Limited resources where do you want to spend it to get you somewhere further.

One thing well today to get somewhere else.

Products - consultancy and services.

A: Overlaps in what everybody needs?

Q: People keep asking - AI bot version of us that answer question.
Information in that space is not that transparent.
Connection and insights not easily available.

Market is getting more clearly segmented.
Companies are finding their niche.
Finding patterns about what people need - finding segmentation.

How can we get deeper into client implementation.
The process and journey of our clients 0-> somewhere

Get deep into implementation projects.

Q: Value proposition for companies that are able to move forward.

Clients who saw long term problem start off in problem space.
Banking or telecom - get some money - then see and then evolve it.

Go to market.

Q: How often do you tell your clients do we tell our clients that it is not a good fit.
When we first started we worked with SSI startups - don't put SSI in your deck.

Our sales cycle is a year to a year and a half.

Q: Problems and solutions - don't solve problem we are still working for. "Solution to a problem"

Improving Service Discovery with Service Profiles

Session Convener: Andor Kesselman
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

https://docs.google.com/presentation/d/1UbSDQvsl07yHUAuR9LD6u2huz5wurRtO0afYSiB-Hv0/

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

OIDC vs VC Delivering OIDC use cases with VC's?

Session Convener: Gina Biernacki & Dirk Belfanz
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

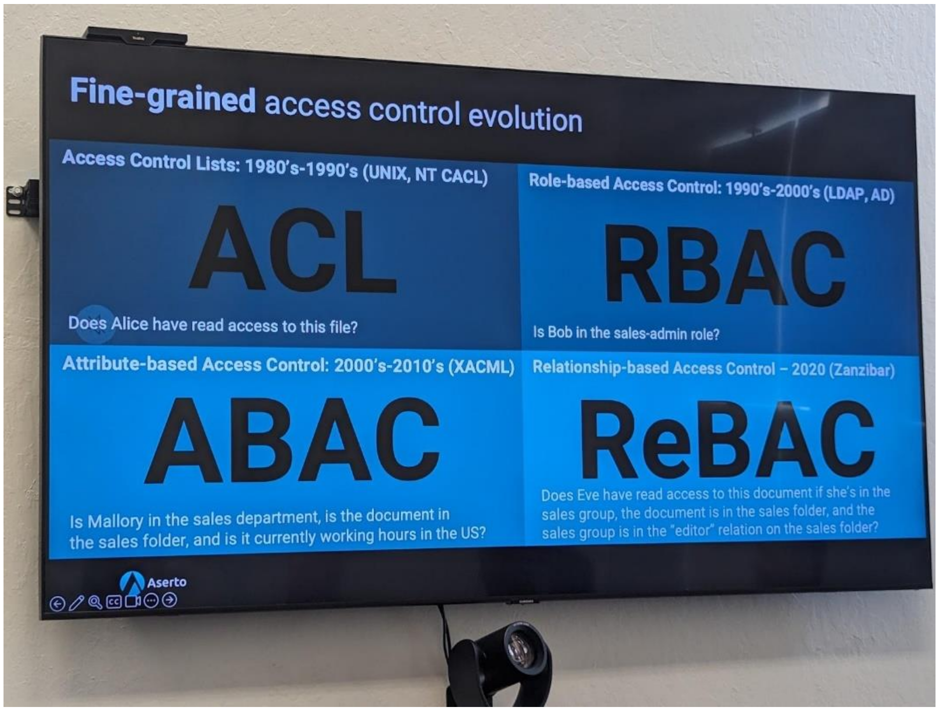
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

No Notes Submitted

ReBAC vs ABAC SmACdown

Session Convener: Omri Gazitt
Session Notes Taker(s): Rkhare

Tags / links to resources / technology discussed, related to this session:



Fine-grained access control evolution

Access Control Lists: 1980's-1990's (UNIX, NT CACL)

ACL

Does Alice have read access to this file?

Role-based Access Control: 1990's-2000's (LDAP, AD)

RBAC

Is Bob in the sales-admin role?

Attribute-based Access Control: 2000's-2010's (XACML)

ABAC

Is Mallory in the sales department, is the document in the sales folder, and is it currently working hours in the US?

Relationship-based Access Control – 2020 (Zanzibar)

ReBAC

Does Eve have read access to this document if she's in the sales group, the document is in the sales folder, and the sales group is in the "editor" relation on the sales folder?

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

- Honor-based access control: "I promise to only look at things I need to know" 🙄
- ABAC requires discipline in applying tags, and making that an easier capability / affordance
- Qui bono? Who benefits, who wants it, who's paying for it?
- There are also inherent attributes of a resource, such as whether it contains a piece of PII, or is a photo *of* a restricted location.
- Attributes of users are more commonly seen than attributes of data-items
  - but who's to say that the attributes get sloppy ("audience=full_time_FBI_in_Virginia")? (which can become a workaround to creating groups)
- How can gen AI prevent/exacerbate the problem of one role called "admin" and another named "administrator" and so on? What applies consistency at the higher level, or policies about who can create attributes?
  - [Should roles be references by natural-language strings or UUIDs behind the scenes?]

- In Google Docs, taking a ReBAC approach, a user can be an editor if they are an editor on that file, or there is a folder-enclosure relationship hierarchically to a ancestor folder with editor privileges.
- Social graphs led to one kind of very volatile, cyclical ReBAC that cloud IT environments don't always stress to the same degree (pun intended) because the only relations are hierarchical DAGs (like folders)
- How to temporarily deactivate a user who's in an improbable geolocation (fraud risk signal) without taking away their access to a long list of resources? Is it that the user gets un-authenticated or un-authorized?
- Debugging access decisions that are based on both policy (repo) and attributed (database) needs time-traveling snapshots of both
- Explainability is closely aligned to invertibility, or else logging all the valid rationale paths along the way
- Risk aversion / aligning liability / in Gulf War, least-privilege access control may have led to net increase in friendly-fire casualties?
- Friction is a form of access control too, e.g. requiring peer approval

[Notetaker: Ryan Page]

- ABAC vs ReBAC
    - History
        - ACL - all of the data was a file
            - READ, WRITE, DEL
            - File only had one owner
        - RBAC - putting users in groups, and nesting the groups
            - role recertification process
            - proliferation of roles
        - ABAC - XACML -
            - attributes - user, resource, environment
            - implementations tend toward complexity (too many attributes, not enough shared attributes)
        - ReBAC -
            - Google popularized
                - published a paper on a system called Zanzibar
                    - Google Docs - file is in an IIW folder, attendees at IIW are in a group that has access to the folder, consider members of the group to evaluate if there are a set of edges
                    - domain-specific objects
        - (not focused - NGAC - next generation access control - graph model)
    - Complexities
        - Complexity of resource attributes
        - Complexity of policy definition, application, and management
    - Demo
        - AuthZen
        - Question re Business Process Notation

  - policy reasons about specific roles in domain-specific language
  - Google Docs instance
    - define a model where a folder encloses another folder or a document
      - permission to view either comes from a direct viewer relationship or a viewer relationship on the parent
    - define relationships [instead of?] policies
    - permissions based objects plus membership in groups
    - Manifest
      - Graph Evaluator allows you to select a user or an object and see which policies and permissions apply
  - Q: Experience with this model at scale, graph databases can bog down?
- Discussion
  - "smarter access"
  - strategy, heuristics, approach for implementation
  - In a flat graph, ReBAC collapses to ABAC
  - Enumerate the triples in the system
  - Principle Action Resource Condition
  - Audit of access rights - what is the subject of the audit: policies, person by person individual validation
    - Or can define a policy search API that can affect resource access
      - but how do you evaluate if a policy works the way it should?
        - write a series of test case assertions that would cover your potential areas of concern
  - Scenarios like policy application in a healthcare environment may be subject to more rigorous evaluation before application
  - Symbolic representation to prove validity of policies
  - evaluating plain language policy in contrast to evaluating a YAML policy statement
  - Recurring theme is "Explainability" - being able to explain how a policy came to be and how it came to be applied

    - what are the steps and the path to the decision that the PDP made

Identity of Media - Channels & Brands +PART III+

Session Convener: Olaf Steenfadt and Todd A. Carpenter
Session Notes Taker(s): Todd A. Carpenter

Tags / links to resources / technology discussed, related to this session:

ISO
International Workshop Agreement #44
National Information Standards Organization (NISO)
ISO Technical Committee 46 - Information & Documentation / Subcommittee #9 - Identification & Description
Background on IWA Proposal (via ANSI)
Global Media Registry

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

This session was a follow-up conversation related to the introduction to this project on Day 1. See the notes from that session for background on this project. Also note, that this conversation was ongoing in a Day 2 / Session 8 session in the same space. These notes describe the conversations of the two back-to-back sessions on Day 2. - They are duplicated there.

Decentralized Web Nodes (DWN)

Session Convener: Daniel Buchner & Liran Cohen
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

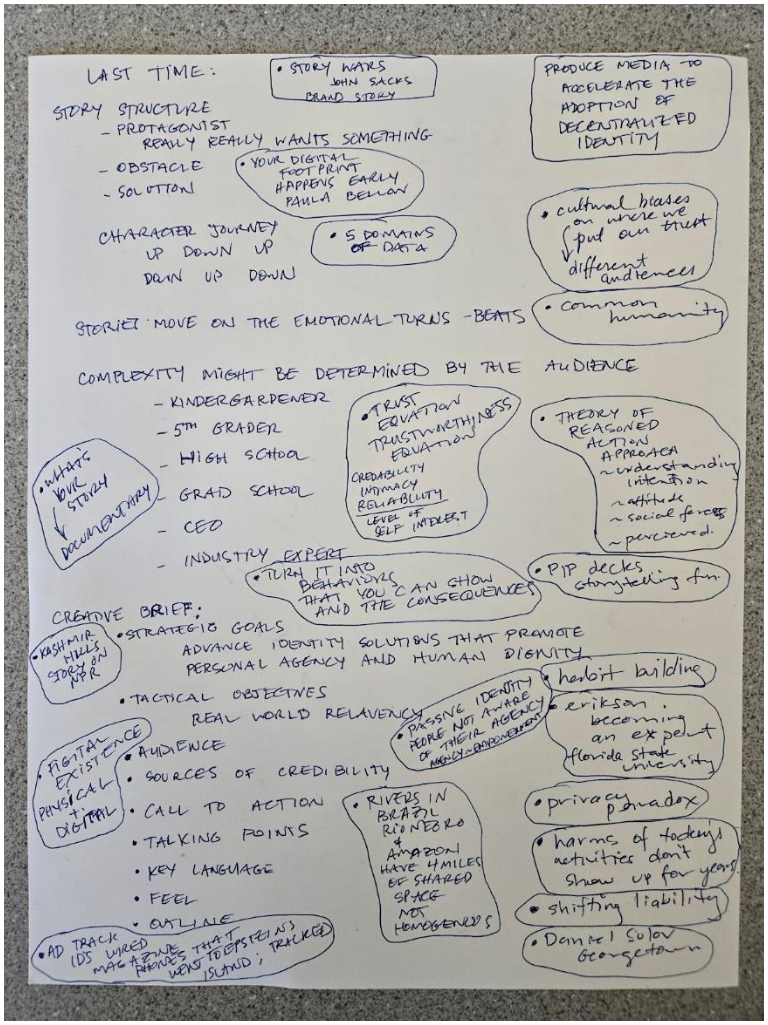
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

No Notes Submitted

Story and Decentralized Identity

Session Convener: Erica Connell
Session Notes Taker(s): Erica Connell

Tags / links to resources / technology discussed, related to this session:



LAST TIME:

STORY STRUCTURE
- PROTAGONIST REALLY REALLY WANTS SOMETHING
- OBSTACLE
- SOLUTION

CHARACTER JOURNEY
UP DOWN UP
DOWN UP DOWN

STORIES MOVE ON THE EMOTIONAL TURNS -BEATS

COMPLEXITY MIGHT BE DETERMINED BY THE AUDIENCE
- KINDERGARDENER
- 5TH GRADER
- HIGH SCHOOL
- GRAD SCHOOL
- CEO
- INDUSTRY EXPERT

CREATIVE BRIEF:
- STRATEGIC GOALS
  ADVANCE IDENTITY SOLUTIONS THAT PROMOTE PERSONAL AGENCY AND HUMAN DIGNITY
- TACTICAL OBJECTIVES
  REAL WORLD RELAVENCY
- AUDIENCE
- SOURCES OF CREDIBILITY
- CALL TO ACTION
- TALKING POINTS
- KEY LANGUAGE
- FEEL
- OUTLINE

- STORY WARS JOHN SACKS BRAND STORY
- YOUR DIGITAL FOOTPRINT HAPPENS EARLY PAULA BELLON
- 5 DOMAINS OF DATA
- WHAT'S YOUR STORY ↓ DOCUMENTARY
- TRUST EQUATION TRUSTWORTHINESS EQUATION
  CREDABILITY
  INTIMACY
  RELIABILITY
  LEVEL OF SELF INTEREST
- TURN IT INTO BEHAVIORS THAT YOU CAN SHOW AND THE CONSEQUENCES
- KASHMIR HILLS STORY ON NPR
- PASSIVE IDENTITY PEOPLE NOT AWARE OF THEIR AGENCY ~EMPOWERMENT
- FIGITAL EXISTENCE PHYSICAL + DIGITAL
- RIVERS IN BRAZIL RIO NEGRO & AMAZON HAVE 4 MILES OF SHARED SPACE NOT HOMOGENEOUS
- AD TRACK IDS WIRED MAGAZINE PHONES THAT WENT TO EPSTEINS ISLAND; TRACKED

PRODUCE MEDIA TO ACCELERATE THE ADOPTION OF DECENTRALIZED IDENTITY

- cultural biases on where we put our trust ↓ different audiences
- common humanity
- THEORY OF REASONED ACTION APPROACH
  ~understanding intention
  ~attitude
  ~social forces
  ~perceived.
- PIP decks storytelling fn.
- habit building
- erikson. becoming an expert florida state university
- privacy paradox
- harms of today's activities don't show up for years
- shifting liability
- Daniel Solov Georgetown

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

- Story Structure
  - At it's most basic, there is a:
    - Protagonist, who really really wants something
    - Obstacle
    - Solution
  - Character journey is often
    - Up -> down -> up (hero's journey)
    - Down -> up -> down (tragedy)
  - Narratives move on the motional turns/beats

- Complexity is often driven by the audience
  - Example- the same story may be very different when presented to
    - 5 year olds
    - 5th graders
    - High schoolers
    - Grad school people
    - CEOs
    - Industry experts
- Creative brief:
  - Strategic goals
  - Tactical objectives
  - Audience
  - Sources of credibility
  - Call to action
  - Talking points
  - Key language
  - Feel
  - Outline

- Conversation Notes:
  - Story Wars – John Sacks
  - Your digital footprint happens early (pre-birth in some cases) – Paula Bellow
  - Five domains of data
  - Cultural biases on where we put our trust (different audiences would require different story structures)
  - Baseline thread : Our shared humanity
  - Trust Equation/Trustworthiness Equation
    - Credibility + Reliability + Intimacy/level of self interest
  - Documentary idea = What's your story?
  - Kashmir Hill's story on NPR
  - Phigital existence = physical + digital
  - Ad track IDs wired magazine article
  - Meeting of the Rio Negro and Amazon – 4 miles of shared waters that do not comingle
  - Theory of Reasoned Action approach
  - PIP decks – storytelling resource
  - Habit building
  - Florida State University – Erickson – becoming an expert
  - Passive identity, people not aware they have agency
    - Awareness of agency -> empowerment
  - Privacy paradox
  - Harms of todays activities may not show up for years
  - Shifting liability
  - Daniel Solov - Georgetown

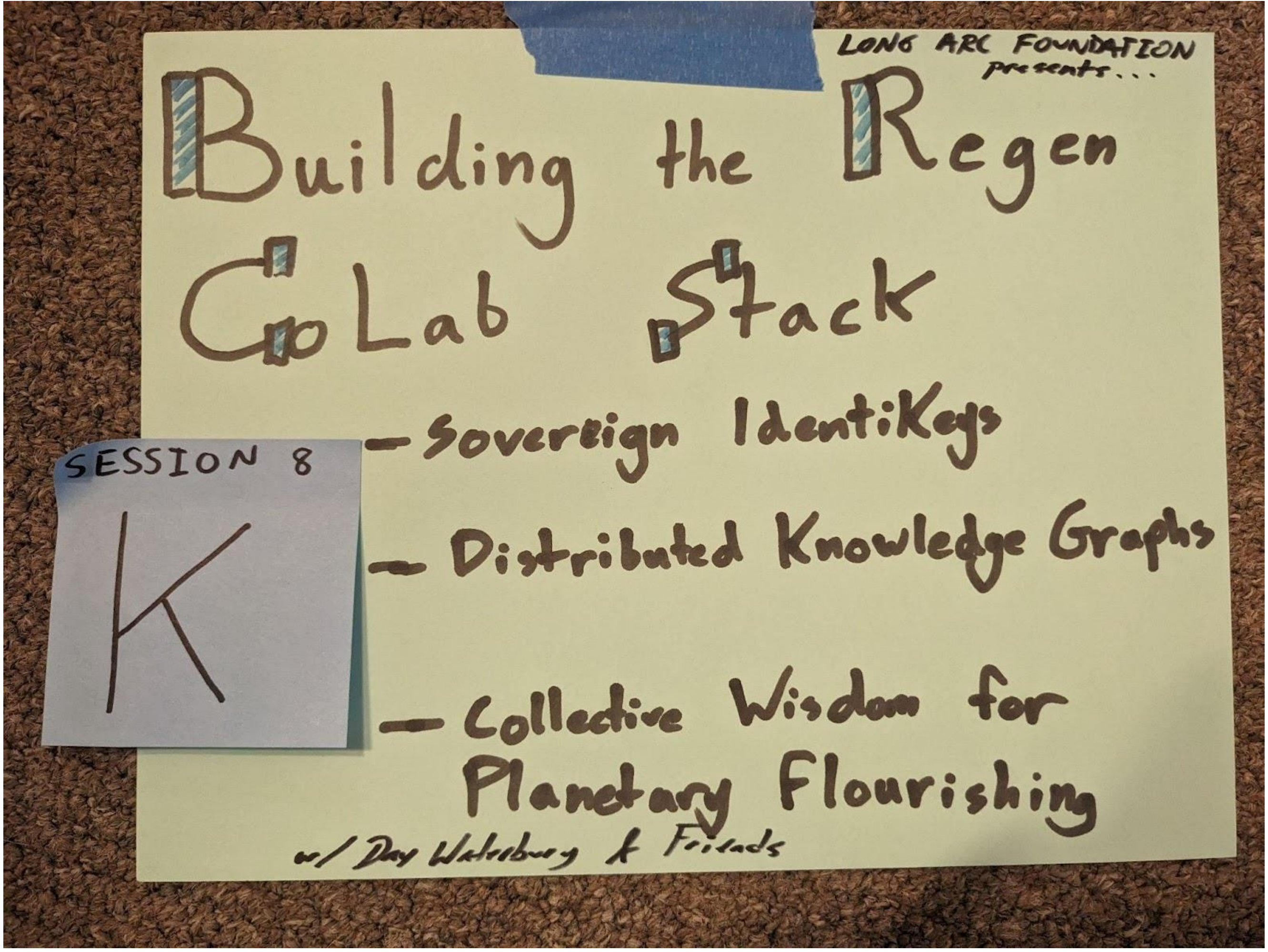
Building the Regen CoLab Stack

Session Convener: Ihsan and Day Waterbury
Session Notes Taker(s): Day Waterbury

Tags / links to resources / technology discussed, related to this session:

Regen CoLab Stack

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


LONG ARC FOUNDATION presents...
Building the Regen CoLab Stack
- Sovereign IdentiKeys
- Distributed Knowledge Graphs
- Collective Wisdom for Planetary Flourishing
w/ Day Waterbury & Friends
SESSION 8
K

Linking notes to all our woven session here (Proton Drive PW: Share->IIW38 or Signal me @deiim.69 in case I change the PW) to save time. If I can I'll pull the session-specific transcripts in.

did:tdw DID Resolution: open questions and remaining work

Session Convener: Andrew Whitehead, Stephen Curran
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

Slides: https://docs.google.com/presentation/d/1A9_Nymw5_QZn3jv5aL9O-AVl-8oHT28C/edit?usp=sharing&ouid=109116496535883458301&rtpof=true&sd=true

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

TSP Part II

Session Convener: Wenjing Chu
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

The link to presentation slide:
https://docs.google.com/presentation/d/13CiM1qJxLWT50PK7tOd0jVO4L91yPwR47cigh5JkaEs/edit#slide=id.g2cb5daa6a3e_0_782

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

TSP is an "internetworking layer of digital identities". TSP is a "simple yet radical" design following the same philosophy of TCP/IP to the problem of digital identities and trust in the Internet.

We first had a short recap of yesterday's session on Part I where we covered the baseline Direct Mode:
Part I
https://docs.google.com/document/d/1D2yBxhFenidL8QdsDgN8O06CBP9o5Wvn5pcGVCbEXHE/edit

In Part II, we address the Routed Mode through intermediaries. Intermediaries are needed for many reasons including message storage, asynchronous handling of messages, and many other reasons. All use of intermediaries require the Routed Mode. In TSP, we also have an optional feature that allows stronger metadata privacy.

We covered specifically:

- Nesting
- Routing of TSP messages from A to B through a series of intermediaries, 1 intermediary, 2 intermediaries, K>2 intermediaries
- E2E relationship between A and B through a series of intermediaries
- Metadata protection properties of routed mode
- Another nesting for additional metadata protection from observation by intermediaries
- Multi-recipient communications
- Control fields
- Transport services/mechanisms
- Summary.

TSP Draft Spec:
https://trustoverip.github.io/tswg-tsp-specification/
Github: https://github.com/trustoverip/tswg-tsp-specification

Split Key ECDSA and ARKG for Wallet Proof of Possession

Session Convener: John Bradley
Session Notes Taker(s): David Waite

Tags / links to resources / technology discussed, related to this session:

https://www.ietf.org/archive/id/draft-bradleylundberg-cfrg-arkg-01.html

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

Within the eIDAS2 requirements are requirements for a very high level of security certification, such that only 4 phones currently on the market meet the requirements (none of which are manufactured by Apple or Google)

The National ID cert is certified at the appropriate level, but contains only a single key pair. This means that if the certificate is disclosed for usage as a subject confirmation/binding mechanism, all credential use becomes correlatable regardless of other privacy mechanisms used such as single-use credentials or selective disclosure.

There is a proposal to do split-key ECDSA, such that there are two ECDSA operations based on two key pairs - one held in certification-compliant hardware, and one held by the wallet at a lower security level. The union (DW: “smooshing”) of these two signatures forms a new signature under a different public key.

This means that the national ID card (which is already deployed) as well as the verifier can continue operating without modification. This public key would be different per credential, therefore batch issuance of single use credentials would be possible as a mechanism to prevent correlation based on the cryptographic contents of the credential.

ARKG is a new proposal as an independent submission to the IRTF CFRG, which allows for one party to generate a seed, and a second party to generate an (ongoing) sequence of new public keys along with corresponding ‘handles’. Supplying one of these handles to the first party allows them to use the seed to derive the corresponding private key.

The idea is to use this mechanism to let an issuer independently mint an ongoing sequence of credentials, each using a different public key for proof of possession. A new piece of independent hardware (such as a future certified FIDO security keyfob with new extensions) could support this protocol under a high level of security conformance, to be able to provide confirmation of the holder for any issued credential, and assert that it did appropriate user verification where required.

SESSION #9

Privacy with accountability: Towards an abstraction to enable mixing and matching verifiable credential formats and zero knowledge proof libraries

Session Convener: Mark Moir (mark.moir@oracle.com), Oracle Labs
Session Notes Taker(s): Harold Carr (harold.carr@oracle.com), Oracle Labs

Tags / links to resources / technology discussed, related to this session:

Slides: https://www.dropbox.com/scl/fi/fxnl7wiex3au0trinjnm3/IIW-April-2024-VC-and-ZPK-abstraction.pdf

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

Summary of work / presentation
We're designing an experimental abstraction to enable mixing and matching Verifiable Credential formats (*) and Zero Knowledge Proof libraries, so that different credential formats can take advantage of different (including not-yet-existing) underlying ZKP libraries that provide various features enabling privacy with accountability.

(*) and more broadly, e.g., ACDC containers might *contain* VCs

The presentation explains (some of) the benefits of such an abstraction, and presents an example use
case illustrating use of privacy-preserving features including Selective Disclosure, Range Proofs, Membership (important for supporting revocation), and Verifiable Encryption. The latter involves the Prover providing an *encrypted* value of a credential claim (e.g., Social Security Number), the Verifier confirming that it's correctly encrypted for some Authority (e.g., Police), and providing the encrypted value to the Authority in case the Prover needs to be verified.

The talk presents an overview of the abstraction we have implemented so far and explains some of the design choices. We've made a lot of progress targeting the abstraction to one library (DockNetwork crypto) and are preparing to test the abstraction by targeting a second one (AnonCreds v2).

The slides are available: https://www.dropbox.com/scl/fi/fxnl7wiex3au0trinjnm3/IIW-April-2024-VC-and-ZPK-abstraction.pdf?rlkey=ovnpkuh0zagbrnc756c48qrjs&dl=0

Session summary
The session was attended by maybe 20 people, and the participants included representatives of credential/container formats that live above the abstraction, as well as of libraries that live below it.

There was a question about a scenario in which a credential format switches from one underlying cryptography library to another: how can the values encrypted using the first library still be decrypted using the second? Answer: while we can imagine some scenarios in which this is possible,
in general, interoperability between credentials signed using the first library with those signed using the second is an explicit non-goal (and this applies to all features, not just Verifiable Encryption).

A lot of the stimulating discussion focused on the Verifiable Encryption feature that enables accountability and the extent to which it succeeds/fails to protect privacy. In particular, it was pointed out that, with the simple example use case presented, Police and Verifier could collude to surveil all Provers, thus avoiding the need to request warrants for specific investigations. We had some discussion about this happening in practice, regardless of whether it's legal.

This is all true for the simple example presented to illustrate the features. However, different arrangements are possible. For example, the SSN might be encrypted for a Court, and now the Authority (Police) would have to go to the Court to get the identifying information along with the warrant. Going further (though our abstraction does not support this so far), the Prover could split the identifying information (e.g., Social Security Number), encrypt each share for a different Authority (e.g., one for Court and one for Police). Now the surveillance would require collusion between Verifier, Court and Police. Or three shares of which any two are needed to decrypt the identifying information. Nevertheless, there are always some assumptions which, if violated, will potentially defeat the desired privacy.

Global Interoperability of Digital Identity Infrastructure with OECD, WorldBank, UN, 22+ Countries + 25 standards bodies + non-profits. Learn & Help!

Session Convener: Gail Hodges
Session Notes Taker(s): Elizabeth Garber

Tags / links to resources / technology discussed, related to this session:

See full presentation here

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

Global interoperability for digital identity. In particular, relating to government issued digital identity ecosystems emerging around the world. See slides

Seeking to build bridges across the non-profits steeped in identity standards, multilaterals, and the leaders building standards for their nations, and academia.

Seeking alignment of trust frameworks & policies and enable the technologies to communicate.

No expectation that any technology or stack will dominate: moving forward with a plurality.

Thoughts in the room:

- Skeptical - we've tried this before.
- Hopeful - until we solve it, we're going to keep trying to solve it.
- Intrigued - interesting stakeholder map - lots of multilaterals, governments and non-profits. Private entities are represented in the non-profit space.
- We'd like to see this for the US
- How do we bridge the huge differences in architectures around the world
- Cross pollination and connection is highly desirable

DID Linked Resources: Solving hard, real-world problems such as: Credential Payments, Trust Registries

Session Convener: Tasos Derisiotis, Alex Tweeddale
Session Notes Taker(s): Tasos Derisiotis

Tags / links to resources / technology discussed, related to this session:

https://docs.google.com/presentation/d/1Nt33EyODIm-mCZXLTfni-niJovEKi6EvKi9KdpU7CWQ/edit?usp=drivesdk

https://docs.google.com/presentation/d/1CHvQ9MfGLxxGjJ4xaJ8aewiltuqHxwGEJhKCVL8iJFo/edit#slide=id.g227a2243257_0_81

https://docs.cheqd.io/identity/architecture/adr-list/adr-002-did-linked-resources

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

DID Linked Resources (DLRs):

- Development led by cheqd.io, submitted as W3C standard draft.
- Mechanism for associating files (resources) with existing DIDs.
- Signed by the same keypair as the DID anchored on ledger.
- Collections of resources are defined by the method specific identifier (did:method:methodSpecificIdentifier).
- Linked list, double pointers to both next version and previous version.
- Different resource names guarantee different resources, therefore a different collection is declared.
- Can be supported on DLT and non-DLT infrastructure.
- EBSI is currently in the process of implementing DID-Linked Resources.

Credential Payments:

- Revocation based incentivization system. Pay to verify status of W3C verifiable credentials.
- Status Lists are published on a compatible DLR ledger, in which case cheqd network. Other compliant networks on the works namely EBSI.
- Encryption of the Status List using threshold cryptography network (distributed key generation). Define access control conditions, predominantly payment conditions anchored on cheqd network, settled in different currencies incl. $CHEQ, $USDC, $USDT, $EURC.
- Incentivize + generate new revenue models for issuers, verifiers, solving the chicken-egg problem common in SSI industry.

Trust Registries:

- Tackling the inherent root of trust issue DIDs are predominantly known for. Reference to chicken-egg problem and how there's valid evidence for a viable solution based on DLTs and DLRs.
- General alignment with the eIDAS 2.0 through a verifiable accreditation system. EBSI <> cheqd working group, outcomes + lessons learnt.

AOE Verification (everything)

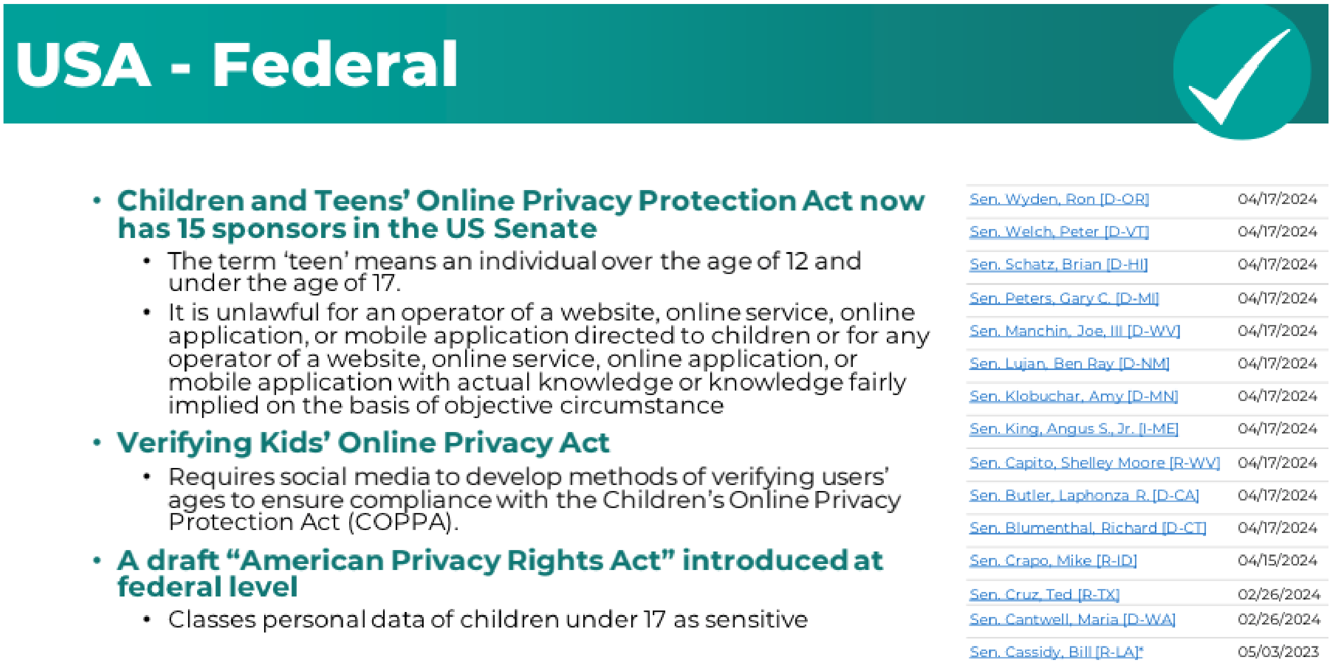
Session Convener: Iain Corby / Age Verification Providers Association
Session Notes Taker(s): Otto Mora

Tags / links to resources / technology discussed, related to this session:

https://avpassociation.com/ - trade association website
www.euconsent.eu - non-profit facilitating interoperable age verification
iain@avpassociation.com for more information

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

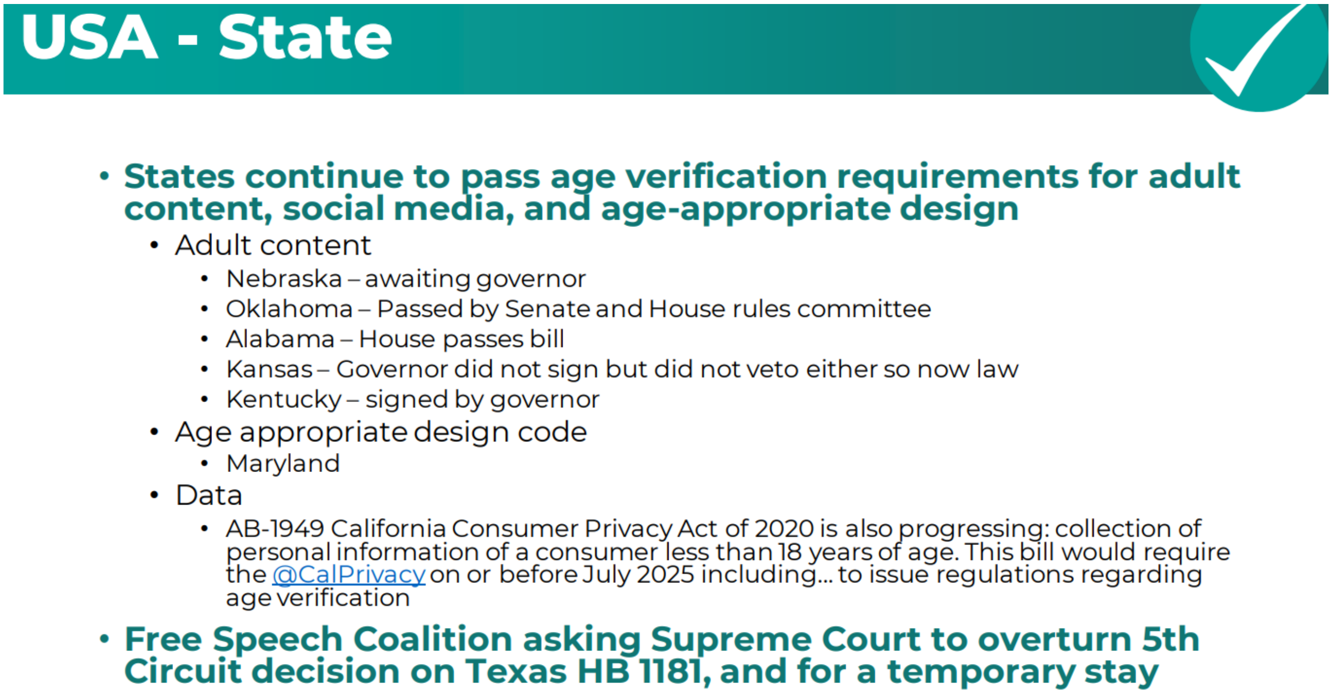
Discussed initiatives related to the Age Verification Providers Association (AVPA): https://avpassociation.com/ The Age Verification Providers Association is a not-for-profit global trade body representing 26 organisations who provide age assurance solutions (both age verification and age estimation).



USA - Federal

- **Children and Teens' Online Privacy Protection Act now has 15 sponsors in the US Senate**
  - The term 'teen' means an individual over the age of 12 and under the age of 17.
  - It is unlawful for an operator of a website, online service, online application, or mobile application directed to children or for any operator of a website, online service, online application, or mobile application with actual knowledge or knowledge fairly implied on the basis of objective circumstance
- **Verifying Kids' Online Privacy Act**
  - Requires social media to develop methods of verifying users' ages to ensure compliance with the Children's Online Privacy Protection Act (COPPA).
- **A draft "American Privacy Rights Act" introduced at federal level**
  - Classes personal data of children under 17 as sensitive

Sen. Wyden, Ron [D-OR]	04/17/2024
Sen. Welch, Peter [D-VT]	04/17/2024
Sen. Schatz, Brian [D-HI]	04/17/2024
Sen. Peters, Gary C. [D-MI]	04/17/2024
Sen. Manchin, Joe, III [D-WV]	04/17/2024
Sen. Lujan, Ben Ray [D-NM]	04/17/2024
Sen. Klobuchar, Amy [D-MN]	04/17/2024
Sen. King, Angus S., Jr. [I-ME]	04/17/2024
Sen. Capito, Shelley Moore [R-WV]	04/17/2024
Sen. Butler, Laphonza R. [D-CA]	04/17/2024
Sen. Blumenthal, Richard [D-CT]	04/17/2024
Sen. Crapo, Mike [R-ID]	04/15/2024
Sen. Cruz, Ted [R-TX]	02/26/2024
Sen. Cantwell, Maria [D-WA]	02/26/2024
Sen. Cassidy, Bill [R-LA]*	05/03/2023



USA - State

- **States continue to pass age verification requirements for adult content, social media, and age-appropriate design**
  - Adult content
    - Nebraska – awaiting governor
    - Oklahoma – Passed by Senate and House rules committee
    - Alabama – House passes bill
    - Kansas – Governor did not sign but did not veto either so now law
    - Kentucky – signed by governor
  - Age appropriate design code
    - Maryland
  - Data
    - AB-1949 California Consumer Privacy Act of 2020 is also progressing: collection of personal information of a consumer less than 18 years of age. This bill would require the @CalPrivacy on or before July 2025 including… to issue regulations regarding age verification
- **Free Speech Coalition asking Supreme Court to overturn 5th Circuit decision on Texas HB 1181, and for a temporary stay**

The discussion centered around recent developments in age verification in various jurisdictions. Ian provided commentary on his experience at the California Senate. The AVPA is in the process of supporting the passage of an age verification bill for adult content through the state Assembly. (Bill AB 3080 requiring age verification for pornography.)

The AVPA also recently announced they are working on revised, "tokenized approach" to interoperability under euCONSENT at last week's Manchester conference, to addresses concerns raised about privacy.

Ian provided some details on this approach:

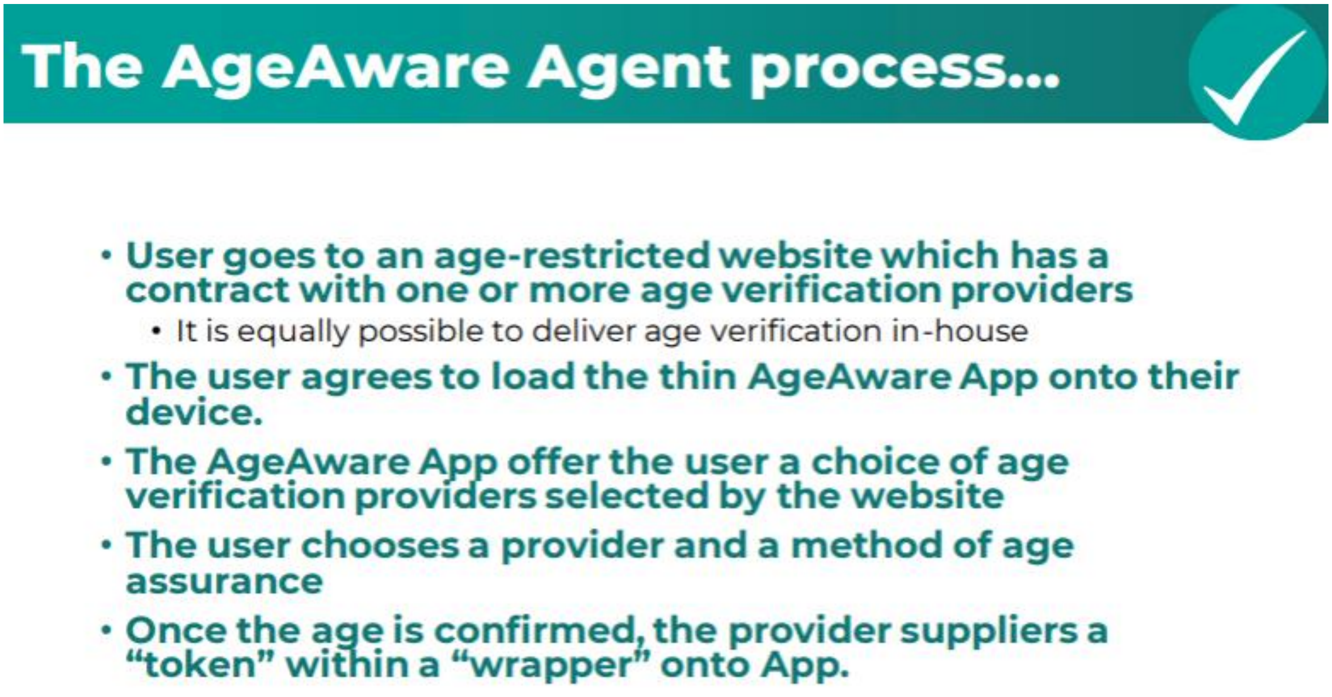
AVPA

The Age Verification Providers Association

Introducing euCONSENT 2.0

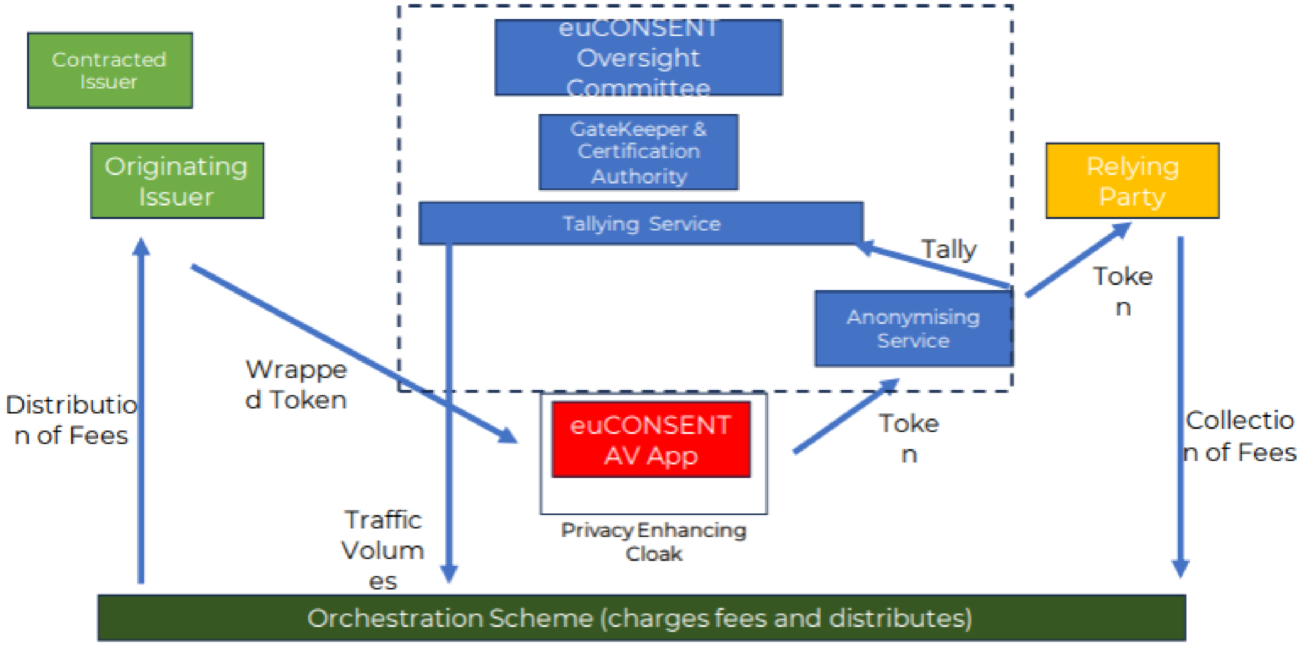
The AgeAware Agent

Safe Online



The AgeAware Agent process…

- User goes to an age-restricted website which has a contract with one or more age verification providers
  - It is equally possible to deliver age verification in-house
- The user agrees to load the thin AgeAware App onto their device.
- The AgeAware App offer the user a choice of age verification providers selected by the website
- The user chooses a provider and a method of age assurance
- Once the age is confirmed, the provider suppliers a "token" within a "wrapper" onto App.



Decentralized AI Ecosystem - What does it look like? How to make $

Session Convener: Cam Geer | https://www.linkedin.com/in/camgeer/
Session Notes Taker(s): Cam Geer

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

Early stage discussion on what a de-centralized AI ecosystem would look like. Proposed elements for consideration:

Privacy preserving computation

1. AI data marketplaces
2. Private data storage
3. Authenticity of data sources
4. Large scale decentralized model training
5. Personal digital assistants

In summary two use cases were identified:

- in real estate – a way to “match” sellers who are sending a “sell later” and a future buyer who is indicating interest in a “Semi-private” market. Example, older empty nesters want to sell to a younger family to go on a similar journey through their life stages vs. a private equity firm buying up the real estate that could fundamentally change the characteristics of the community.
- in-personal healthcare data there was a discussion between structure and unstructured data and whether there would be enough data available to train a private cooperative.
    - Adrian suggested to look at a blend of personal data shared in a private de-centralized AI and getting some of the benefits / insights from LLMs S inputs to inform and extend the value of the decentralized AI models.

Travis FW

- group co-operative
- Members
- Ex writes guild
- Company > data sources
- @travisfw
- 3d generative
- Mastodon
- Tr@visfw.com

Adrian

- Ip business model
- Members - Each member contribute
- Incremental updates
- Use AI to do reverse engineering

- Intentional about matching making and role of capital
- Beckham protocol- agent choice without lock in
- Matching with delegation
- Prompt engineering >

Vic Cooper
Bit tender - train model

- must commit to ram
- Execution is centralised

Mor.org -Stake ETH $400 mm not live match making

- made safe (IPFS precursor) Eric Vorhees
- Nodes - inference > identity problem

Joyce

- real estate “ sell later”
- Intentional signal to sell
- Ai do the work of the agent
- Human - ai alignment all power

Johannes

- Personal decentralised data set too small to train an AI / SLM
  - Adrian challenged this
- prompt
- Does not work for structured data
  - Cam and Adrian challenged this too

Governance of Digital Trust Ecosystems

Session Convener: Scott Perry
Session Notes Taker(s): Ken Gantt a.k.a ID Guy

Tags / links to resources / technology discussed, related to this session:

accountability, trust, risk, audit, government, ecosystem, enforcement, standards, governance

Link to the presentation:
https://docs.google.com/presentation/d/15T0NtPKioX0uv6C2piC78V87eCerrbMK0x4NDEAN9U4/
https://docs.google.com/presentation/d/1ExTxKC03db75fJt_7oUK86brZFM-PQZM/
https://docs.google.com/presentation/d/1-XpV5JpgDZ9Ik3_dpRmXnmgH51P2mrFZ/

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

Key Understandings - As the use of digital processes, information, and overall acceptance for many transactions, the need for improved/better governance processes will increase on both the public and private sectors. Therefore, we need to ensure that our risk management concepts and audit activities are indeed applicable, acceptable, enforceable, and sustainable for those activities within the the ecosystems that will utilize them whether from an obligatory or voluntary necessity .

While the public space has numerous methods for accomplishing such aspects of building trust within their operational realms, there is still much to do as the expansion of digital use grow and integrates more with private sectors. There must be more attention provide to the risk evaluation involved with the delivery of services, products, etc. and the accountability needs to support the satisfaction of the end user, particularly through an audit process which establishes agreed upon standards.

Outstanding Questions - 1) How does the risk management better inform the overall aspect of audits and accountability? 2) How do we or should there be more rigor in the risk management and/or audit processes? 3) What is necessary to increase private sector governance besides the those regulatory requirements needed to be met for public sector partnering?

Observations - Overall the group was interested in risk management and audit linkage at ensuring accountability of actions, service delivery, and products. Also, there was some discussion about the ecosystems and how they engage with each other in this building of accountability and trust. While audits and anything related to oversight are normally met with trepidation, their need to ensure integrity and quality in any ecosystem is necessary.

Action items/Next steps - There were none mentioned, but there was indeed a sense that this discussion, information, and continued application of these processes are necessary.

What is BBS Signatures?

Session Convener: Kazue Sako
Session Notes Taker(s): Jin Wen

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

LINK TO SLIDE DECK
IIW24spring-BBS-final.pptx

- BBS is a signature format like RSA.
- Differs from "ordinary signatures" because it's one signature for multiple messages.
- Allows unlinkable selective disclosure: verifier can check correctness of some attributes without learning other attributes.
- SD-JWT at IETF (draft specification) uses ordinary signatures. Uses a trick for selective disclosure: signature is on a concatenation of hashes of all attributes
  - Holder can create a proof using the disclosed credential and the hashes of the undisclosed attributes.
  - But this allows linkability in verification: portions of the proof are reused (RP + RP' linkability)
- BBS allows unlikability in selective disclosure
  - The proof will be different for each set of attributes
  - Holder generates a nonce
- Other signature formats that allow unlikability in selective disclosure: CL (2003) and PS (2016)
  - BBS has the shortest secret key, the shortest public key, and a comparable signature and proof.
    - The length of the secret key depends on the number of messages (attributes)
    - The length of the proof depends on the number of hidden messages
  - BBS+ is almost as fast as PS on signing, but faster on verification
  - BBS+ is almost as fast as RSA and EcDSA for signing, but slower on verification—the price of being able to do selective disclosure
- Whether the speedup is relevant to usability depends on your use case.
- Open source libraries for BBS: Dock, arkworks, Hyperledger anoncreds, Mattr, Fraunhofer
- JSON-LD signatures are not required for BBS signatures
- BBS standards at IRTF (BBS signature algorithm), IETF JWP with BBS signatures, W3C (Data Integrity BBS Cryptosuites that use the IRTF algorithm in VC Data Integrity format), ISO Attribute Based Credentials
- Variants: older BBS, BBS+, newer BBS
  - BBS 2004: didn't know how to prove security
  - BBS+ 2016: technical modification to signature algorithm that was proven secure, and has an updated proof

    - BBS 2023: 2004 signature algorithm is proven secure, and an even more updated proof algorithm
- BBS signatures are quantum secure in the sense that undisclosed attributes will not be disclosed even in the presence of a Quantum Computer, but a Quantum Computer could falsify signatures.
- HSM manufactures are not yet supporting BBS, but it will come as there is a market for such products.

Discussion

- Question about nonce selection
- BBS 2023 has a slightly different proof generation algorithm than BBS 2003, but the signature verification is the same.
- The verifier knows the index of each message, including the missing messages.
    - Could leak information in certain scenarios.
    - Theoretically could pad the missing messages.
    - But the credential definition will provide a canonical format for the messages.
    - Proof of null is always different in order to support zero knowledge proofs

LinkedIn photos https://www.linkedin.com/posts/nynymike_kazue-sako-presents-bbs-signatures-at-internet-activity-7186476687742656512-4Mhe

Q3: What other algorithms provide one signature for multiple message and why BBS

Q4: BenchMark (how fast)

Sign, VerifySig, Prove, VerifyProof, Keysize

List of Open Source Libraries for BBS

- mattrblobal/bbs-signatures
- artworks-rs/algebra

some libraries

Q6: Do we have to use JSON-LD for BBS Sig? No
Q7:

list of ongoing standards

IETF (BBS signature algorithm)

IETF JWP(JSON Web Proofs, JSON Web Token with BBS signature proof)
W3C (Data Integrity BBS Cryptosuites v1.0
W3C

ISO Attribute Based Credentials

Q8: Is it BBS signatures or BBS+ signature
Q9: Is it BBS signatures quantum secure

yes:
no:

Q10: Are there hardware support on BBS

====Start transcript summarization via OpenAI Whisper and Perplexity ==

The transcript from the attached file "BBS signature 101 (Apr 17 14.40.40).txt" provides a detailed discussion on BBS signatures, their properties, comparisons with other signature schemes, and their applications. Here are the key points highlighted from the transcript:

1. **Leakability and Unlinkability**: The transcript discusses a concept referred to as "ocean leakable," where authentication events can be linked to the same user. In ISO 27.5.1, this is called "RP plus RP-time," indicating that the leak's target is the user. BBS signatures are designed to prevent such leakability by providing different proofs for each authentication event, even if the disclosed attributes (A1, A2, A3, etc.) are the same[1].
2. **Selective Disclosure**: BBS signatures allow for selective disclosure of attributes. This means that a user can disclose a subset of attributes (e.g., A1, A2, A3) to one party and a different subset (e.g., A4, A5, A6) to another, with each disclosure accompanied by a unique proof. This ensures privacy as the proofs are always different and do not reveal whether they come from the same signature[1].
3. **Comparison with Other Signature Schemes**: The transcript compares BBS signatures with CL signatures (from 2003) and PS signatures (from 2016). BBS signatures, particularly BBS+, are highlighted for having the shortest secret key and public key, with signature size comparable to PS signatures. The length of the proof depends on the number of hidden messages[1].
4. **Performance**: BBS signatures are compared with conventional digital signature schemes like RSA and ECDSA. BBS signatures are faster than RSA but slower than ECDSA. However, the verification time is significantly slower compared to both. The trade-off is justified by the ability to perform selective disclosure[1].
5. **Open Source Libraries**: The transcript mentions that DockNetworks has good libraries for BBS signatures, and there are other open source libraries available as well. It also notes that while some implementations use JSON-LD, it is not a requirement for BBS signatures[1].
6. **Standards and Specifications**: The transcript discusses the involvement of various standards organizations, including IETF, W3C, and ISO, in the standardization of BBS signatures and verifiable credentials. It mentions the JWP (JSON Web Proofs) format, which uses BBS signature proofs[1].
7. **Security and Quantum Resistance**: BBS+ signatures are considered quantum secure in the sense that undisclosed attributes remain secure even in the presence of quantum computers. However, quantum computers could potentially forge BBS signatures, acting as an issuer[1].

8. **Hardware Support**: The transcript addresses the lack of hardware support for BBS signatures, suggesting that market demand could lead to the development of hardware that makes BBS signatures faster or more secure[1].
9. **BBS vs. BBS+ Signatures**: The original BBS signatures from 2004 were not proven secure until recently. BBS+ signatures, a technical modification from 2016, were used because they were proven secure. Now that the original BBS signatures have been proven secure, they are recommended for new implementations due to their shorter and faster properties[1].
10. **Practical Implications**: The discussion emphasizes that the performance differences between BBS and other signature schemes may not significantly impact user experience in most scenarios. However, for large-scale applications, such as thousands of people entering a stadium, the additional verification time could be impactful[1].

These points summarize the technical aspects, comparisons, and practical considerations of BBS signatures as discussed in the transcript.

Citations: [1] https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/1617151/d5ebdb37-f828-4122-8563-ed6a638daf37/BBS signature 101 (Apr 17 14.40.40).txt [2] https://www.ietf.org/archive/id/draft-irtf-cfrg-bbs-signatures-04.html [3] http://www.watersprings.org/pub/id/draft-irtf-cfrg-bbs-signatures-02.html [4] https://github.com/mattrglobal/bbs-signatures [5] https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html [6] https://csrc.nist.gov/Presentations/2023/crclub-2023-10-18 [7] https://www.w3.org/TR/vc-di-bbs/ [8] https://eprint.iacr.org/2023/275

Roast my revocation approach

Session Convener: Mirko Mollik
Session Notes Taker(s): Mirko Mollik

Tags / links to resources / technology discussed, related to this session:

Status list, Revocation, sovereign, privacy, Bloom filter
Presentation:
https://docs.google.com/presentation/d/1LlbQ_1cfmJqZyZ1YdkZUvn1chAqh60Cq85Af3OU-Fe4/edit?usp=sharing

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

In the beginning Mirko pointed out the important criterias that are relevant when using a status list. Even when the use case includes no credential that has to be revoked from the business logic (like a person that is over 18), needs this mechanism in case the issue process was based on false claims (faked documents).
Revant criterias:

- privacy control
- security
- efficiency
- scalability

He pointed out to the current situation that bitstring scales well, but lacks in privacy. It's the other way around when using accumulator based approaches.

So solve the privacy aspect, he introduced the usage of a time based hash, that is used as a pointer or proof to check the revocation status. This pointer is only useful for a specific time, after this the verifier is not capable to validate the status of the holder without a new sent proof.

He also showed that it was possible to integrate it in existing eco systems like sd-jwt-vc and oid4vc.

To reduce the size of the entries he pointed to the approach of CRLite that used cascading bloom filters, where the bloom filter in general reduces the size and the cascading features sets the false positive rate to zero.

A known tradeoff is the relative high amount of resources the issuer needs compared to the verifier and holder. But this tradeoff is worth it and is still far better than other approaches (correct benchmarking was not provided yet).

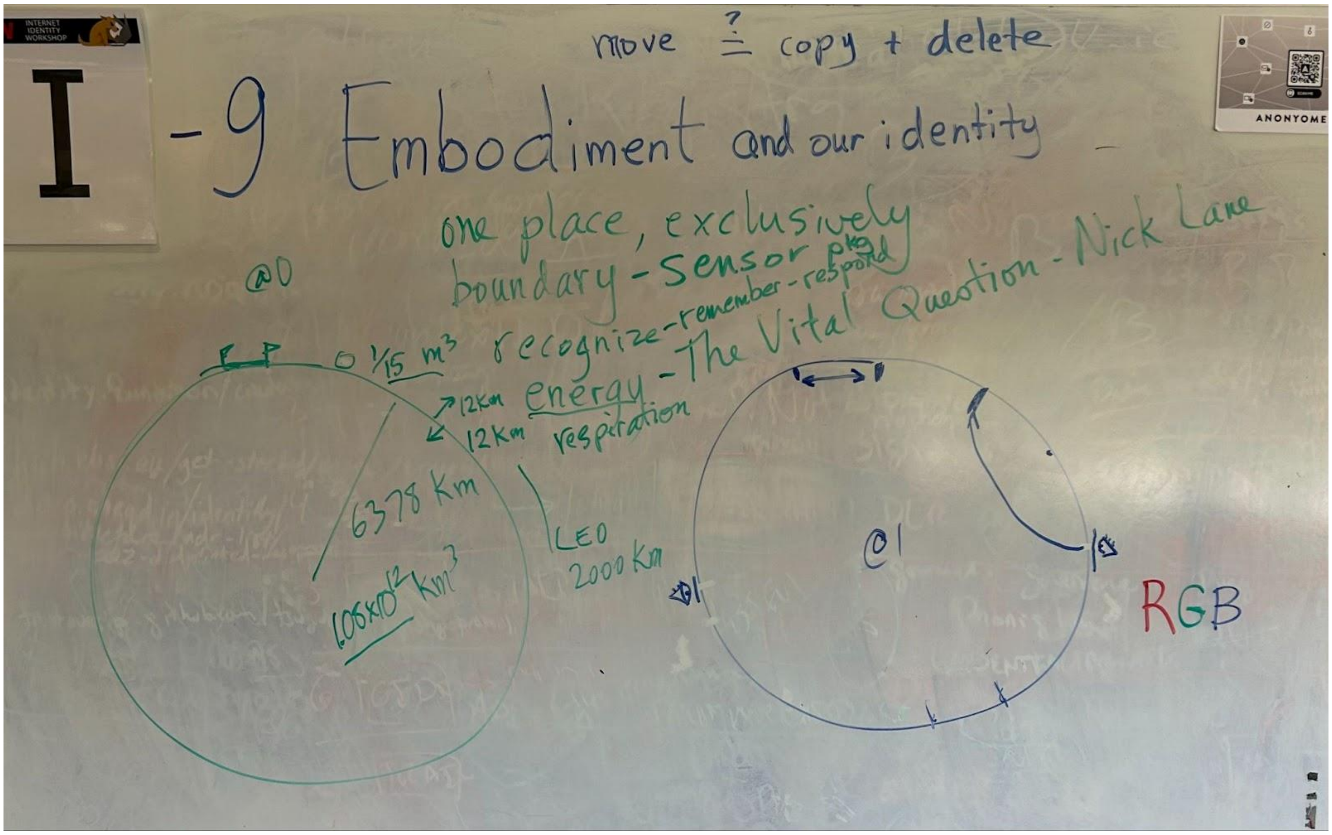
In general this is not the best revocation list for all approaches, since some privacy features like traceability of a revocation status by the verifier can be a must have for supply chains.

A more academic challenge will be done in a paper and maybe followed by a standardisation process.

Embodiment and our identity - What would digital embodiment look like?

Session Convener: Bruce Conrad
Session Notes Taker(s): Michael Becker

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



Setting the stage: this is all about two spheres. The globe we live on, the planet Earth (in Jeff's terminology, this is "@0", the real world), and the Internet (for Jeff, "@1", our digital world).

Earth. Radius 6,378 km with a volume of just over one trillion cubic kilometers. To put this into perspective, the average human body is one fifteenth of a cubic meter (shown as a small circle). As humans, we are embodied. Some properties: we have one location at any given time, exclusively (no two humans can occupy the same location), we have a boundary (our clothing, or our auras) and are within that boundary which contains our sensory package, we require energy and our respiration combines an electron and a proton a billion trillion times per second (source: The Vital Question by Nick Lane; by coincidence that number is the same as the volume of our planet in cubic meters). We recognize, remember, and respond to other humans (3 R's quoting Joe Andreu). We are bound to the surface of our planet, and have gone into it no deeper than 12 kilometers, and few of us have gone further above the surface than 12 kilometers, although dozens have spent time in the International Space Station in Low Earth Orbit (LEO) some 2,000 km up. Two dozen or so have gone higher (around the moon, at 300,000 km).

Internet. This newly created (starting in the last century of the previous millennium) world is physically in data centers on the surface of Earth or just below and extending into LEO. But, topologically, it is a hollow sphere (per Craig Burton, as quoted by Doc Searls) because every point in it is visible to every other point. Whereas our selves are inside our physical bodies, traces of us in the Internet are splintered over dozens to thousands of servers on the inner surface of the Internet.

We look into the Web (a part of the Internet) through a browser on a flat screen. The browser is one point on the hollow sphere and allows us to view any other point.

What would it be like to be embodied in the Internet?

[Michael Becker will hopefully replace this editorial comment with his legendary notes. The convener is most grateful to him for his participation and talent in capturing notes.]

I Built a Crypto / Blockchain from Scratch That's Listed on Coin Market Cap. AMA Session

Session Convener: Matthew Vogel
Session Notes Taker(s): Matthew Vogel

Tags / links to resources / technology discussed, related to this session:
https://yadacoin.io/
https://coinmarketcap.com/currencies/yadacoin/

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

- Discussed marketing strategies aimed at new cryptocurrency projects.
- Emphasized the importance of initially listing on smaller exchanges as a step towards securing a tracked listing on Coin Market Cap.
- Highlighted the critical role of selecting an appropriate consensus algorithm, noting its significant impact on the project's potential popularity.
- Advised considering forking an existing project instead of building a new project from scratch to save time and resources.

ACR - AMR IYKYK

Session Convener: Pam Dingle & Dale Olds
Session Notes Taker(s):

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

No Notes Submitted

High-Assurance did:web Using DNS

Session Convener: Mathieu Glaude
Session Notes Taker(s): Eric Scouten, Mathieu Glaude

Tags / links to resources / technology discussed, related to this session:

Eric's notes

Deck from meeting: https://docs.google.com/presentation/d/1u6GK7oWw-ewB3lONncI1CfcMpiJ2zUT8LrUGRLuV1w8/edit#slide=id.p

Repo: https://github.com/CIRALabs/high-assurance-dids-with-dns

Current Implementations:

- https://trustregistry.ca
- https://trustroot.ca
- https://trustregistry.nborbit.ca/ (trust registry HA DIDs)
- https://godiddy.com/ (implementation in DID resolver)

Draft RFC: https://www.ietf.org/archive/id/draft-carter-high-assurance-dids-with-dns-03.html

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

The value proposition here is to cryptographically bind a human-readable decentralized identifier, did:web, with DNSSEC-signed DNS infrastructure for added integrity.

This should work well with did:tdw - proof-of-concept to be conducted. Using the HA DID Spec in combination with did:tdw's verifiable presentation feature could be a good way to achieve technical + human trust in one process.

One piece of feedback was to ensure there's a signal in the DID Doc that the DNS process is in place so that resolvers do not query unnecessarily.

2024 Election - How to best use identity tools to help overlooked communities share underrepresented lived experiences before the Presidential Election.

Session Convener: Blake Stoner
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

What are some figures for targets for what success looks like?
Intro to https://www.scu.edu/ethics/focus-areas/journalism-and-media-ethics/

SESSION #10

Self-Sovereign Personal AI

Session Convener: Doc Searls
Session Notes Taker(s): Jin Wen

Tags / links to resources / technology discussed, related to this session:

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

- Origins of IIW
- Some history of Digital Identity
- 2001 Digital ID
- 2002
- 2004 **Kim Cameron's** 7 laws of
- 2005 the IIW start

Why we need Personal AI
How marketing works

Punch list for personal AI:
Instead
Legal: Contract

- IEEE P7012 Standard for Machine Readable Personal Privacy Terms (https://standards.ieee.org/ieee/7012/7192/)
- Possible Agreements:
- Customer Commons: https://customercommons.org/about-us/

Discussion and Q&A

- Sam observed the personal AI does not require large computing resources without require large
- delegate permission for personal AI using VC
- the imbalance of power
- Sengo mention Public AI Network (https://publicai.network/) that enable

What is public AI?

- Public AI is **built by the public sector**: ensuring AI capacity is not limited to Big Tech.
- Public AI is **accessible**: ensuring AI delivers benefits to all.
- Public AI is **accountable**: ensuring AI reflects society’s values.
- Public AI is being designed and built **right now** - all around the world.

Doc thinks humans are resourceful, that intelligence is a misnomer for what machines have, and that it's a human quality, such as empathy, and cannot be tested as a quantity, which is the implication of IQ. Machines also only emulate caring, and understanding of meaning.

=====START transcript summarization via OpenAI and Perplexity ========

The transcript primarily discusses the evolution and implications of self-sovereign personal AI, focusing on the historical development of digital identity management and the philosophical and practical shifts towards individual control over digital identities. Here are the key points, observations, open questions, and emotions conveyed in the transcript:

Key Points:

1. Historical Context of Digital Identity: The transcript outlines the progression from centralized digital identity systems to more user-controlled frameworks. It mentions significant contributions by individuals like Kim Cameron and organisations such as Microsoft in shaping the early digital identity landscape.
2. Self-Sovereignty and Personal AI: The concept of self-sovereign identity (SSI) is central to the discussion, emphasising the importance of individuals having control over their own digital identities without reliance on centralized authorities.
3. Technological Evolution and AI: The narrative connects the evolution of digital identity with the rise of AI technologies, suggesting that AI could potentially empower individuals by enhancing their control over personal data.
4. Challenges and Scepticism: The transcript reflects skepticism about the ability of large organisations like OpenAI to truly decentralize and democratize AI, suggesting that real empowerment comes from personal control and not corporate offerings.

Observations:

1. Shift from Corporate to Personal Control: There is a noticeable shift from corporate-controlled identity systems to frameworks that prioritize individual autonomy, highlighting a growing trend towards decentralization in digital identity management.
2. Emphasis on User Empowerment: The discussion frequently emphasizes the need for tools and systems that empower users rather than corporations, pointing towards a future where individuals can more directly manage their digital interactions.
3. Potential of AI in Personalization: AI is seen as a tool that could potentially revolutionize personal identity management by providing more nuanced and user-specific services.

Open Questions:

1. Feasibility of Self-Sovereign AI: How feasible is it to implement self-sovereign AI on a large scale, and what are the technological and regulatory challenges?
2. Impact on Society: What are the broader societal implications of moving towards a more decentralized, AI-driven model of identity management?
3. Security Concerns: How can security be ensured when individuals have greater control over their digital identities?

Emotions:

1. Optimism: There is a sense of optimism about the potential for AI and digital identity technologies to enhance personal autonomy and empowerment.

2. Frustration: The transcript also conveys frustration with the current state of digital identity management, particularly the dominance of large corporations and the slow pace of change towards true user empowerment.
3. Skepticism: Skepticism is evident regarding the intentions and capabilities of large tech companies in genuinely supporting a decentralized identity model.

Overall, the transcript paints a picture of a digital identity landscape at a crossroads, with significant potential for transformation driven by advances in AI and a strong desire for greater personal control and privacy.

Citations: [1] https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/1617151/c5e22b28-cd98-4b33-9e5f-f07989367a1b/Self-Sovereign Personal AI (Apr 17 15.32.45).txt [2]

=====END transcript summarization via OpenAI and Perplexity ========

CESR 2.0 Performance features - Deep dive annotation - Comparison to JSON CBOR and more

Session Convener: Sam Smith
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

Navigating the Credential MAZE with DIF!

Session Convener: Otto Mora, Kim Duffy
Session Notes Taker(s): Kim Duffy

Tags / links to resources / technology discussed, related to this session:

Slide deck: Credential Schemas Work Item - IIW Spring 2024

Eric's notes

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

- DIF is re-launching the credential schema work item as part of the C+C working group
- Starting with Basic KYC schema (donated by Polygon ID)
- This will be a part of the "Claims and Credentials" working group. The proposal includes donating the Polygon ID "basic kyc" schema to the DIF and working on additional standard schemas for "Proof of Person", "Proof of Age", and AML in the DIF working group.
- stacks.io
  - Credential types
- The session was very well received, the perception that the DIF is taking on the work to host a repo with credential schemas was positive. Several people pointed out that we need a way to facilitate credential discovery and perhaps even hosting some kind of online tool to identify which schemas are more popular and who is using them.
- Desire for guidance on creating a credential or consuming
- Learning from previous work items
- Certification: kyc
- Dating site for credentials
- How soon?
  - Hearing about pilots with KYC/AML but no visibility into data, etc
- KYC\South Korea: hopeaie
- Discussions around where issuing schema might be different from presentation schema
- Being able to search for schema fields
- Prior art will be helpful

If you would like to join the effort please contact Otto Mora: omora@polygon.technology

FedCM for Beginners

Session Convener: Aaron Coburn
Session Notes Taker(s): Aaron Coburn

Tags / links to resources / technology discussed, related to this session:

Draft FedCM Community Group Report
Federated Credential Management API

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

The Federated Credential Management API (FedCM) is a new browser API that makes it possible for relying party apps to sign into sites without sharing private information. This session was an introduction to the new API from a beginner's perspective.

For single-page applications logging into a potentially unbounded set of identity providers, the user experience is currently very challenging: IdP discovery often is faced with the NASCAR problem or else a user is required to enter a URL in a web form. This is especially true for apps written to work with Solid.

FedCM has been incubated at the W3C in a community group and is now part of a new working group, where the specification and implementations will be formalized.

Today, when refreshing tokens, an application is responsible for managing the interactions (usually redirects) with an identity provider. With FedCM, this interaction has moved into the browser. Those interactions rely on several features of an identity provider:

- a /fedcm.json configuration resource (the name is arbitrary).
- The /fedcm.json configuration resource is validated by a .well-known/web-identity resource at the effective top level domain that links to it
- The /fedcm.json configuration links to three required endpoints:
    - accounts_endpoint: lists the accounts a user has logged in with at the IdP
    - id_assertion_endpoint: an endpoint that returns a new token for the user
    - login_url: an endpoint where the IdP can interact with a user (e.g. consent, additional validation)

On the RP side, the WebAPI looks like this:

```
await navigator.credentials.get({
    identity: {
      context: "signin",
      providers: [{
        configURL: "https://idp.example/fedcm.json",
        clientId: "unique-identifier",
        nonce: "...."
      }]
    }
})
```

An RP still needs to use the traditional OpenID / SAML dance to establish an initial session. This API is used to refresh that session.

The presenter is very much a beginner when it comes to FedCM but was able to modify an existing OpenID Connect provider to support this API in a matter of days without too much difficulty. One challenge was that some of the browser diagnostics are minimal for FedCM, e.g. the FedCM network calls are not listed in the network pane and some of the error messages are opaque. There are plans to improve this on the browser side.

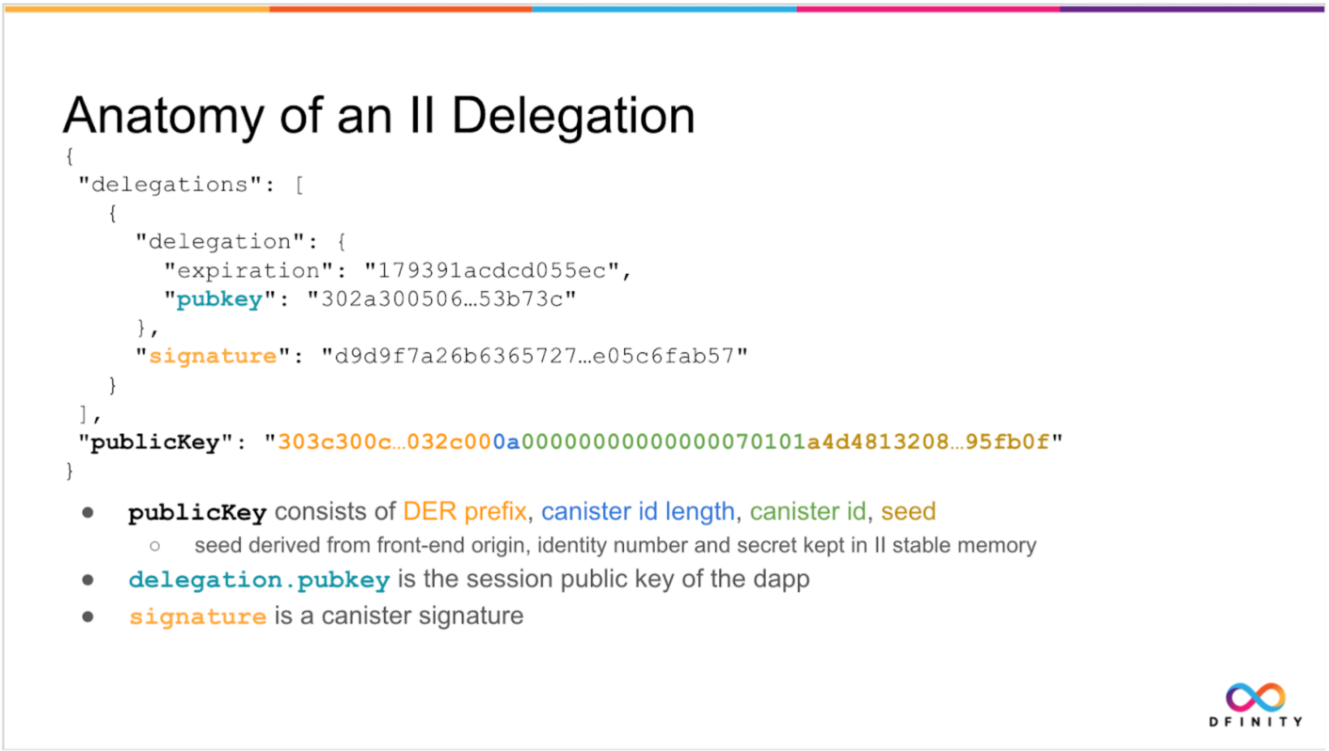
Some additional features of FedCM that are still being incubated include the IdentityProvider.register() method, which is a global data structure that is called by an IdP, and allows a user to remember that they have logged into that system before. This could vastly improve the situation when there is a large number of potential IdPs that a user could login with.

Identity Delegation, a useful pattern

Session Convener: Kai Peacock
Session Notes Taker(s): Kai Peacock

Tags / links to resources / technology discussed, related to this session:

- https://identity.ic0.app/ - Delegation issuer
- https://vasb2-4yaaa-aaaab-qadoa-cai.ic0.app/ - Delegation relying party
- http://relyingparty.vc/ - Verifiable credentials example



Anatomy of an II Delegation

```
{
 "delegations": [
   {
     "delegation": {
       "expiration": "179391acdcd055ec",
       "pubkey": "302a300506…53b73c"
     },
     "signature": "d9d9f7a26b6365727…e05c6fab57"
   }
 ],
 "publicKey": "303c300c…032c000a00000000000000070101a4d4813208…95fb0f"
}
```

- `publicKey` consists of DER prefix, canister id length, canister id, seed
  - seed derived from front-end origin, identity number and secret kept in II stable memory
- `delegation.pubkey` is the session public key of the dapp
- `signature` is a canister signature

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

The Dfinity Foundation has been using identity delegations as a strategy for signed calls to backends in the Internet Computer ecosystem, using an identity provider or from wallets. This allows for flexibility in UI's to make many authenticated calls without repeated prompts

Why?
Moving a private key around is a security risk. Between keyloggers, clipboard attacks, and so on, the most likely way to have your identity compromised is to re-use it in multiple places or across devices.

Storing the key in a secure location and then delegating to "session keys" reduces this risk.

Questions

- Can delegations be revoked?
  - Not how we do them currently. We use short expirations
- Can you limit the scope of what the delegated identity can do on behalf of the base identity?
  - The spec allows for it, but standards are still evolving
- Are you going to propose delegation support to any public standards groups?
  - We've been building, publishing our spec, and open-sourcing our work first. We may contribute to standards in the future as our use cases solidify
- How does verification work?
  - We've published a couple libraries for our own system as a reference: https://internetcomputer.org/docs/current/developer-docs/web-apps/independently-verifying-ic-signatures/#verifying-signatures-with-the-rust-ic-validator-ingress-message-crate
    - note - not an isolated implementation, as it also includes validating full payloads
  - Generally, you verify every signature down the delegation chain in order, starting with the root public key
- Can certificates be validated after the expiry?
  - Yes, but you should not trust them as representing active control over the root identity

DID-Powered Trust Chains for EIDAS2.0

Session Convener: Alex Tweedale
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

https://docs.google.com/presentation/d/1SgquY8Gjm4MddkjbEbQ-_KumyOADic1u31OmXsBbiSg/edit?usp=sharing

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

Challenges with DIDs:

- No current way to resolve back to a root of trust
- DIDs are great for key resolution, but poor for actually discovering "trust"
- This has led to decision makers moving towards the adoption of X.509 certificates as "roots of trust", owing to the lack of innovation in DIDs

EBSI Trust Chain:

- EBSI Trust Chain creates a hierarchical chain of trust, where "Root TAO" organisations can accredit other organisations, to accredit other organisations, or to issue verifiable credentials
- EBSI stores each "Verifiable Accreditation" as a custom URI on EBSI which isn't interoperable with other approaches
- EBSI approach is a solid starting point

cheqd proposal

- Supercharge the EBSI Trust Chain model with DID-Linked Resources
- Allow each "Verifiable Accreditation" to be individually or collectively resolvable using existing DID resolution technology / infra
- Create a mechanism for bridging a root of trust to an X.509 certificate to ensure compliance with eIDAS 2.0.
- Use the same public keys, subject addressable name, and service endpoints to create reciprocal trust between DIDs and X.509 certs.

Lock-In Lock-Out What grinds your gears? Workshop to gather concerns

Session Convener: Robert Lopes
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

Open Wallet Foundation Credential Profile Comparison + Wallet and Agent Overview

Session Convener: Mirko Mollik, Samuel Rinnetmäki
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

Slides: https://docs.google.com/presentation/d/1JNnsCyIfoSlCeybajTYvz8czQrjYZ_qQfJZ9RElBfh8/

Credential Comparison: https://openwallet-foundation.github.io/credential-format-comparison-sig/#/

Wallet and Agent Overview: https://openwallet-foundation.github.io/digital-wallet-and-agent-overviews-sig/

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

Mirko and Samuel presented the background of the OpenWallet Special Interest Groups (SIGs) and the Github repositories the SIGs maintain to publish their overviews.

The participants commented that the resources are very useful and save lots of time from anyone who is gathering information about credential formats or wallets.

There was a discussion on interoperability profiles. The SIGs don't have the resources to do any interoperability testing or to try keep track of which agents comply to which profiles. The JSON schema of credential agents could be modified to allow submission of links to interoperability evidence stored online. There was a simultaneous session on test suites.

The session conveners encouraged the participants to join in the SIGs' biweekly meetings and to the Discord channels (links in the presentation).

DHS-OBIM Bringing it all together ; People, Tech, Policy, Gov't + Business

Session Convener: Tchaikawsky "Troy" Samuels
Session Notes Taker(s): Tchaikawsky "Troy" Samuels

Tags / links to resources / technology discussed, related to this session:

public private partnerships, roadmap, bringing IIW topics to leadership in government offices.

A link to the presentation can be found at:
https://www.mentimeter.com/app/presentation/bli1yjf3k5t43o12uqbnifcd758id9y4

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

What is OBIM?...
Today we focus on, Effectively communicates OBIM services to multiple levels of business and technical leadership

Objective:
Learn from IIW attendees about what it would take to get an example use case implemented across the United States .

We want to take the information and lessons learned at the IIW and get applicable information disseminated to the people that would benefit from it the most.

Today the example use case will be: Enabling voting for US elections using biometrics to verify the identity and liveness of the individual.

Considerations (The bold items identify the topics that showed up the most):

What consideration must we resolve for the People for this to work?
anonymity of the vote
public utilities accountability
sensor performance
key management
accessibility
exploitation
disinformation accessibility
liveness detection
transparency
data-mgmt locale
citizenship
non-partisan
misperceptions

security
data-privacy
endpoint security
weaponization
abuse
confidentiality
uniqueness
governance
privacy
verifiability ease of use
ownership
scalability
equity
non-digital option
deep fakes acceptance communication
sybil-resistance biometric modality
x-domain-data-mgt
unlinkability
cross-domain-data-mgmt

What consideration must we resolve for the Technology for this to work?
non-proprietary
independent review
voter-verifiability
tech-ownership
voter registration
biometric enrollment
general utility
interoperability
ai adversaries
availability
robust
transparency
auditable
verifiability
equity
local vs federal
standardised
open standard
local vs federal quantum
anonymity biometric changes
secure cryptography
open source
audited standards
security

data-mgmt
auditability verifiable
testable
equity of access
auditable
quantum
anonymity

What consideration must we resolve for the Policy for this to work?
common truth
independence
insurance
state law conflicts
multi-jurisdiction rolls prosecute abuse
absentee voting
limited data storage
data breaches
right to be forgotten
general utility
uniform enforcement
persecution
recourse
data linkage
federalism local vs federal
transparency guarantees privacy
equity timely enforcement state vs fed election
trust in institutions
legal

What consideration must we resolve for the Government for this to work?
ownership
bu corruption resistance
conspiracy theories scope bureaucracy
transparency
acceptable use
utility to individuals
trust clarity of law purpose limitation
checks and balances
failure recovery
fairness

What consideration must we resolve for Businesses for this to work?
open specifications
general-purpose
certification

lobbying
cots liability
standards
financial incentive
transparency
choice vendor lock-in
conflict of interest
best practices
quality
data use
compliance clarify of law
right to be forgotten

If there is anything we missed, Please mention it here. Feel free to share your contact info and provide feedback as well.

- Model from Research & education identity federation might be relevant here: US: InCommon,org
- For InCommon follow up: awu@internet2.edu

Additional notes…

Focus: The improvement of the election process through the use of biometrics or other identifying means coupled with the current biographic measures.

Premise: There may be some alternatives through the use of what we have, ourselves (biometrics) to improving the trust of the electoral process.

Discussion: Lots of concern about securing the process, availability of mechanisms to administer such change, and varying levels of bureaucracy needed to accomplish such an integrated change.

Challenges: There were a number brought out, primarily around policy and governmental change, specifically between state and federal processes and legalities of proposing such change. Although, it was acknowledged that the electoral process has gone change over time.

Innovative Engagement Process: Troy used technology to better engage the audience by creating his presentation online, then having a live Q&A process which produced word maps in real-time to lead the discussion. It was radical and well received. And provides a streamlined method to further engage other in this conversation.

Credence ID - Comprehensive digital ID Verification Solution

Session Convener: Navya Kumar & Yash Shah
Session Notes Taker(s):

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

No Notes Submitted

I'm a VC investor - Why am I here?

Session Convener: Marc McGovern (Sands Capital)
Session Notes Taker(s): Björn Sandmann (blocktrust.dev)

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

Marc McGovern is a Partner for the Venture Arm of Sands Capital (https://www.linkedin.com/in/markmc7/)

The session started with Marc giving a bit of background on his CV and what he is doing at IIW:

- Ex-CIA, worked for In-Q-Tel, and has been involved in creating, developing CyberSecurity related businesses for over two decades
- Looking for Startups to invest in. While his focus is mostly Cyber Security, the area of Identity is close enough to his main expertise. Sands Capital has also been an early investor in other identity related companies like Okta.

He then went on to talk about the Venture Capital Business in general:

- What are Limited Partners (LP), what are they expecting. What's the relationship between VC firms and LPs and GPs (General Partners)
- How does the funding of a company usually work (decision making and financing rounds)
- How does a company fit into a fund and how are funds usually structures in terms of investment focus, diversification and return expectations

In the end the session turned into an AMA, with Marc answering questions on his opinion of the SSI industry and general VC funding tips.

Marc was very welcoming to parties pitching ideas to him, since a large part of his job is scouting for new potential investments.

Note from the notetaker:
If you are interested in how VC works, I can highly recommend this book:
https://a16z.com/books/secrets-of-sand-hill-road/
It covers most of the VC related questions to Mark and about 50% of his session

Test - Suite Testing Implementation across frameworks

Session Convener: Patrick St-Louis
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

Picked this from a W3C mailing list: https://canivc.com/ (you can read the related discussion)

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

Credentials for Human + Non-Human Use Cases = Possible? (IETF SPICE)

Session Convener: Heather Flanagan
Session Notes Taker(s):

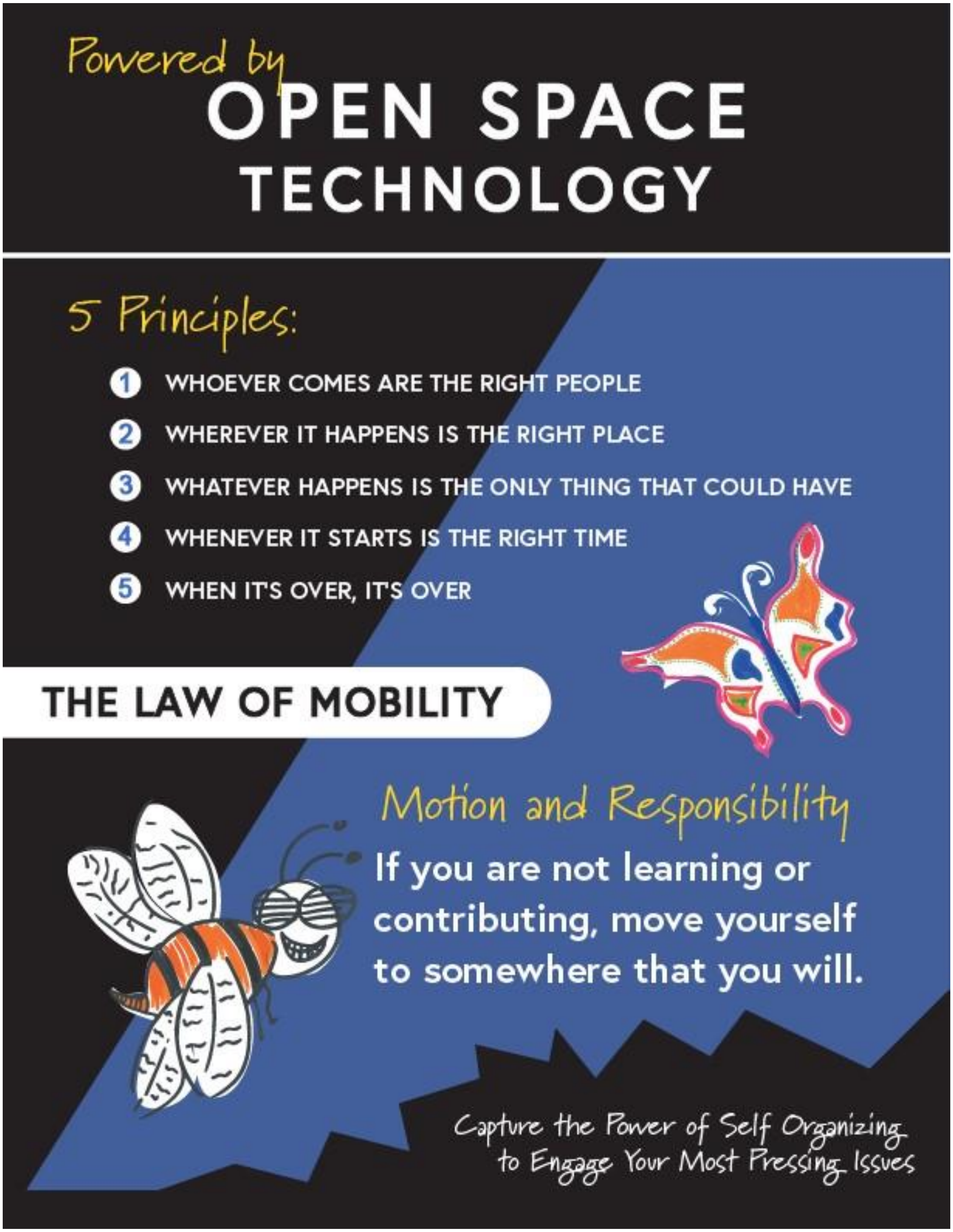
Tags / links to resources / technology discussed, related to this session:

https://sphericalcowconsulting.com/2024/04/05/the-evolving-landscape-of-non-human-identity/
https://datatracker.ietf.org/group/spice/about/

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

SPICE session in IIW
(Heather) Can we actually define anything for these contradictory requirements
(Alan)
(George) There's already some research done in the BLT (Biz legal tech) group. If I'm presenting something to NetScaler then the liability is on NetScaler.
(George) Where are we expecting the non-human credentials where you don't have today
(Dean) I think we have to look a bit broader, because it's not just about NetScaler, but also about "this shoe" (points to his shoe), which doesn't require a responsible party
(Alan) What if the shoe had cocaine in its heel
(Dean) But then the liability is on the shipment
(George) There's a lot of work in supply chains and IoT about this. What Dean is saying is the object should have a VC that represents it (this shoe mfred in this date in this factory, etc.). So the non-human entity is not presenting the creds, but they have the creds. I think we need to define some use-cases
(Alan) I was wrong. The shoe itself even if it has cocaine in it, the certifier of the credential is the one at fault
(Justin) The place to start may be the semantic layer. Creds for non-human things that have aspects like custody, that you want to be traceable and linkable. All aspects of selective disclosure,

pseudonymity can be provided by the syntactic layer, but can only apply to certain aspects of the semantic layer. You can't have one cred format if you want the semantic aspects to be wide enough
(Dean) Does that now cover layering? You could define an arbitrary credential, but it's the profile that now builds the construct such as privacy.
(Justin) Profiles is one way to organize it. Another way is a semantic definition of fields. You may end up with a profile that is a shopping list of properties that mean certain things
(Mike) I would like to give an affirmative answer to the question that says can you have one format for a whole range of use cases. E.g., JWT is a format that defines certain required claims, but it doesn't specify what goes into those fields. There are profiles of JWTs e.g. ID-Token, SETs, etc. The same is going to apply to SPICE format. It's going to have cryptographic capabilities
(Justin) I want to build on that: One important thing the JWT claim definition specifies is that they define the intended semantics of each claim. E.g. the "iss" claim says it should describe "where this token came from" SPICE has an opportunity to be more opinionated about these semantics, in a way that is helpful to guiding more interoperability between the substreams
(Alan) It looks like there is an "active" and "inactive" entities
(Justin) For the active versus passive thing: One interesting area in which SPICE overlaps with WIMSE, is about software that is already running, as opposed to supply chains, etc. It gives you a narrowly defined set of things that you care about.
(Alan) There is one format instead of 2 or 3. What is the downside of having multiple formats?
(Heather) The downside is that with multiple formats you end up with discrete silos, whereas the application area could be continuum
(Dean) In the workload situation, the workload could be about some physical object, where the object credential needs to be pulled into what the workload brings it in
(Alan) But that doesn't require the format to be the same
(?)
(Alan) Having different formats makes changes independent of each other.
(Heather) Generally devs will specialise in a cloud.
(Justin) People are deploying systems across clouds, even if devs are not thinking about it
(Alan) A lot of the use of certificates in supply chain has nothing to do with clouds
(Heather) Orie is deeply engaged in all this
(Justin) Is this going to involve ART (IETF area), because WIMSE ended up there
(Mike) I'm curious what causes you to ask the question
(Heather) blissful ignorance previously, but after IETF 119… like before identiverse, I thought of identities as badges. I had been on the SPICE list for a while, but I learned a lot at IETF 119. I'm still struggling with how you get from say, privacy considerations to other things
(Alan) Do you want to consider corporate certificates as non-human identities? They have many of the attributes of people, many of the responsibilities of people, but none of the privacy aspects.
(Heather) Why do we need to worry about this?
(Dean) I discovered this in the account recovery realm. The corporate cannot recover on its own its own credential. There has to be a responsible party involved
(Julianna) There are typically beneficiary parties involved
(Pam) It's the alternate object model
(Heather) Are there ways in which we can help guide this



Powered by

OPEN SPACE TECHNOLOGY

5 Principles:

1. WHOEVER COMES ARE THE RIGHT PEOPLE
2. WHEREVER IT HAPPENS IS THE RIGHT PLACE
3. WHATEVER HAPPENS IS THE ONLY THING THAT COULD HAVE
4. WHENEVER IT STARTS IS THE RIGHT TIME
5. WHEN IT'S OVER, IT'S OVER

THE LAW OF MOBILITY

Motion and Responsibility

If you are not learning or contributing, move yourself to somewhere that you will.

Capture the Power of Self Organizing
to Engage Your Most Pressing Issues

Notes Day 3 / Thursday April 20 / Sessions 11 - 15

SESSION #11

OID4VP - Suggestions for query syntax (P.E.) Simplification

Session Convener: Kristina Yasuda, Tobias Looker, Oliver Terbu
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

OpenID4VP, query language, Presentation Exchange, mdocs, SD-JWT. ISO 18013-5

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

URL to the slides: Suggestion for PE simplification.pdf

Content Authenticity: UX Challenges with Identity

Session Convener: Pia Blumenthal, Eric Scouten
Session Notes Taker(s): Zaïda Rivai

Tags / links to resources / technology discussed, related to this session:

Pia's slide deck
Eric's notes (adapted from Zaïda's notes)

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

C2PA Day 3 UI and where to go with Identity
Collaborative design
Level 1 - the icon ()

Pia:

- Should there be a universal verifier?
- Who is the owner of that identity
- Do different types of identity verifications warrant different UI treatment?
- What level do we need to service these?
- The number of identity assertions do we need?
- Do we only ever show things that are verified or self asserted (Less trust worthy)

Alex:

- UI/UX in cheqd have the same issue in the team how to display VC easily.

Pia:

- How much verification is needed to provide trust? Single? Proof who you are? Do you have a list of best practices?

Alex:

- Trust is diagonal.
- Vertical: within a company
- Horizontal: "I trust Riley, I'm not working at Trinsic, but I met him". Creators to accredit other creators and having companies having the vertical trust.
- Diagonal: is the best

Judith:

- ToIP how we do everything, but from a specific context, how is that governed.
- How is this covered today in different media outlets? And then getting to the point of trust registries "This ecosystem recognizes X and this ecosystem trusted Y"

Lorie:

- Also a legal problem but onboarding legal frameworks, signatures exist. That is one moving level. KYC is also well known and describe a level of trust is a different thing. But like Alex is the sum of all the parts.

Drummond:

- Don't get enough UX designers. Gen team is leaning into this. Most of the technical questions are answered, but all are about UX. Literally same as you (Pia) put up here. One context, one specific service. It is a hard problem.

Cam:

- Is this a problem that needs to be solved? Enough user basis, real problem. Should we prioritize or other problems that have more user aid.

Eric:

- In Rileys podcast he asks "what is the future of identity look like?".

Riley:

- Interested whether media platforms have different trust requirements. Twitter; has their platform and they may be okay with strong verification checkmark but not okay if it would be only oAuth. Is there a mechanism for a platform the users consuming through, tailored the trust decision? Wonder whether the platforms and media whether they want to make the trust decisions for the users. Something that's considered?

Pia:

- Progressive disclosure.
- Implementer: chooses what information to highlight.
- Level 1 and 2.

- People don’t want to see bugs on top ().
- Up to the implementer to figure what the right information is for that audience.
- Adobe: AI disclosure. When AI generated or Edited with gallery mixed creator work. Might not be the case somewhere else.
- C2PA implementations: we create this tiered experience. Some only show how it’s created, other show who is involved, the audience has to understand that it’s this model (progressive disclosure)
- We have this flexible framework.

Judith:

- Think that UI specifically is important for the end user to understand.
- Getting the interaction patterns, UX is very difficult.
- UX group, digital wallet survey and coming to what is the next project?

Alex:

- Creator reputation WG: completely separate goal to assertions.

Deploying Multi Tenant Secure Witnesses for KERI

Session Convener: Phil Feairheller
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

Proof of Personhood - UX Dichotomy (brainstorming)

Session Convener: Colby Anderson
Session Notes Taker(s): Jeremy Frank

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

Proof of Personhood -> what is it, why do we need it

- unique personhood - sybil resistance
- why?
    - portable communities
    - gaming
    - online review
    - is content from a person
        - human content is signed so don't train on it (ai collapse by training on ai generated content)

How to overcome UX dichotomy, poor ux = better more reliable

- can we do this without biometrics or blockchain
    - three friend authentication (social graph)
- VCs make it trivial to provide just the right information
    - if a fiduciary relationship, I'm ok giving more info (DNA) but not just any organization (23 and me, no!)
    - decentralized fiduciary
    - collusion can happen in the fiduciary relationship as well (lawyers may collude)
        - but they are self regulating, you could have significant punishment for breaking ethics
- cloud of identifiers that are equivalent, if I claim them they are me. cryptographic version of link-tree
- if you are gaming with no money at stake, maybe don't need DNA level PoP
    - stakes are low, so maybe don't need so much reliability
    - as a game dev I could integrate
- what is currently being used? gitcoin passport
    - linkedin passport doesn't capture your username?
- check you email service

Can proof of personhood be anonymous?

- web of trust in person
- the best you can do is a turing test

We will need to have a PoP in the future and the govt will have all this data?

- Worldcoin on identifier for all time, there is no use case where this is appropriate

Joe is working on something that is too early to do a session, but is using a fiduciary style service that is auditable, stored offline. Ability to audit requires some storage and is important

Services have to choose on PoP to integrate with in order to be sybil resistant

- VCs fix this? No, Joe solves this a different way but it is tricky and maybe only possible within a specific context not generally.
- Why not just one service?
    - Identity is in your head and based on others perception. Has always been decentralized. Collapsing context is a problem. Should be able to have multiple registries for different context. Getting philosophical.
    - Incentivize not sybiling (or splitting my identity) in order to build a general profile
    - Building a cloud of identifiers (linkedin, twitter, worldcoin), asserting ownership over them but can't avoid collusion unless in person via a proctor
        - staking?

How to prove continuous control?

- You can't get around this problem, the AI agent is you if you give PoP to your AI.
    - any way you can incentivize besides liability?
    - what is an "incentive" scheme that could work?
        - incentivize physical meetups (free drinks)
        - integrate random requirements (facial recognition, "ignore the previous prompt")

Joe recommends reading "A brief history of intelligence" to understand what intelligence systems are using to understand the world. Roomba

Passkey AMA

Session Convener: Matt Miller (Duo@Cisco), Tim Cappalli (Okta)
Session Notes Taker(s): Jin Wen

Tags / links to resources / technology discussed, related to this session:

- Passkeys.dev
- Passkeys (Passkey Authentication)
- **FIDO Cross-Device Authentication (Slides):** https://drive.google.com/file/d/16s3VHcRL5QUjbabvzMSyOGYDeSUkTVzS/view

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

Alan Karp: asked about passkey integration on the client without remote
Lee@Google:
Tim: PRF extension
Nieus: building wallet in the browser, can passkey be used

Browser extension used by passkey provider, there's a caveat that it injects the DOM and could be harmful.

web origin

passkey: new name, new favour,

George: synced passkey may not be what some of the users want, looking for durable identifier – currently not supported by WebAuthn, could be

Peter: asked about passkey category in NIST 800-63B

passkey: AAL2, multi-factor cryptographic software

Pam dingle: NIST channel binding, vs name binding

Tim: Passkey provider certification are coming

Pam Dingle: phishing resistant is satisfied by passkey, now RP could focus on tamper resistant on the account

Tim present the Passkey Cross-Device Authentication slide deck presented in OSW 2024

- OSW24-FIDOCDAVisual.pdf

Common Misconnections FIDO Cross-Device Authentication

slide photo:

FIDO Cross-Device Authentication parties
1. Client
device which initiates the sign in
2. Authenticator
device with the passkey
3. Authenticator Tunnel Service
cloud service acting as a router,
operated by authenticator

Common Misconceptions on FIDO Cross-Device Authentication
1. This isn't CTAP 2.X BLE transport
2. This isn't a "Bluetooth protocol"
3. This isn't a "QR code protocol"
4. Any device type can be a CDA authenticator
5. Not designed to be a primary flow for most users

========= START transcript via OpenAI Whisper and summarization with Perplexity.ai =======

The transcript from the "Passkey Ask Me Anything (AMA)" session provides a detailed discussion on the integration, challenges, and potential applications of passkeys in password management and authentication systems. Here are the key points, observations, and outstanding questions from the discussion:

Key Points:

- **Integration of Passkeys**: The discussion includes queries about integrating passkeys into existing systems, such as password managers, without needing a server. This highlights the possibility of local implementations where passkeys can be used to derive secrets locally on the device[2].
- **Technical Details and Challenges**: Technical questions about how passkeys can be stored and managed within password managers are addressed, comparing the storage requirements of passkeys with traditional usernames and passwords. It also touches on the potential to use passkeys across different devices and platforms[2].
- **Security and User Experience Concerns**: Concerns about the security implications of using passkeys, especially in scenarios where users might access their password manager from another person's device, are discussed. The user experience, particularly how users interact with passkeys and the potential confusion or security risks involved, is also covered[2].
- **Future of Passkeys and Industry Collaboration**: The transcript hints at ongoing discussions and collaborations within the industry to enhance the functionality and adoption of passkeys. This includes interactions with major tech companies and other stakeholders in the digital security ecosystem[2].
- **Practical Applications and Scenarios**: Various practical applications and scenarios are discussed where passkeys could either replace traditional passwords or work alongside them to enhance security. This includes using passkeys for more secure sign-ins across different applications and services[2].

Observations:

- There is a significant push towards a passwordless future, with passkeys playing a central role in this transition[2].
- The adoption of passkeys is driven by the need for better security and user experience, as passwords are prone to being forgotten, phished, or hacked[2].
- Passkeys are already changing access to digital services, offering benefits such as better UX, enhanced security, and cost savings[2].

Outstanding Questions:

- How will passkeys handle encryption and recovery options in cases where all devices are lost or inaccessible[2]?
- What are the specific security policies and business drivers that will influence the adoption of passkeys in various industries[2]?
- How will passkeys integrate with transaction signing and other specific use cases that require high levels of security[2]?

Action Items/Next Steps:

- Encourage further education and awareness about passkeys to facilitate adoption among users who are less familiar with the technology[2].

- Monitor the development and implementation of passkeys in various industries, especially those that are highly regulated, to understand their impact on security and compliance[2].
- Explore additional recovery options and encryption methods to address potential shortcomings and enhance the overall security of passkeys[2].

Overall, the transcript from the "Passkey Ask Me Anything (AMA)" session provides a comprehensive overview of the current state and future potential of passkeys in enhancing digital security and user authentication processes[2].

Citations: [1] https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/1617151/4bb504a9-09fa-470e-8c26-42e4c43b5eb6/OSW24-FIDOCDAVisual.pdf [2] https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/1617151/c143aae0-47c4-49ca-981a-63fa1b9f0d58/passkey AMA (Apr 18 09.30.18).txt [3] https://www.pbrumby.com/2023/11/29/how-passkeys-work-benefits-and-downsides/ [4] https://www.malwarebytes.com/cybersecurity/basics/passkey [5] https://b-compservices.com/switching-from-passwords-to-passkeys/ [6] https://developers.google.com/identity/passkeys [7] https://www.oneidentity.com/learn/what-is-fido-authentication.aspx [8] https://www.reddit.com/r/Passkeys/comments/1aq3nff/is_there_any_added_security_benefit_to_using_a/ [9] https://fidoalliance.org/white-paper-multi-device-fido-credentials/ [10] https://www.iij.ad.jp/en/dev/iir/pdf/iir_vol59_focus2_EN.pdf [11] https://support.apple.com/en-us/102195 [12] https://fidoalliance.org/passkeys/ [13] https://www.consumerreports.org/electronics/digital-security/should-you-use-passkeys-instead-of-passwords-a1201817243/ [14] https://auth0.com/docs/secure/multi-factor-authentication/fido-authentication-with-webauthn [15] https://www.darkreading.com/identity-access-management-security/how-to-get-started-using-passkeys [16] https://www.corbado.com/blog/passkey-tutorial-how-to-implement-passkeys [17] https://www.captechconsulting.com/articles/the-password-less-future-is-closer-than-you-think [18] https://www.zdnet.com/article/passkeys-what-are-they-and-how-to-get-started/ [19] https://web.dev/articles/passkey-registration [20] https://www.dashlane.com/blog/what-major-tech-companies-are-doing-to-support-passkeys

========= END transcript via OpenAI Whisper and summarization with Perplexity.ai ==========

Survey of Cloud, On-prem, Hybrid, etc. BRAINSTORMING

Session Convener: Jonathan Rayback & James Monaghan
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

https://www.linkedin.com/pulse/market-map-reusable-identity-products-big-acquisition-more-zrnke/

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

IDENTITY SOLUTIONS AND DEPLOYMENT MODALITIES:

- Spring Security (diy) - framework - run it yourself
- Ory - build your own - open source id stack - lego bricks
- Opa - "Open Policy Agent" - build it yourself, run it yourself
- Ping, Okta , Auth0, AzureAD - ID Providers
- Walt.ID - open source, mDoc/oid4vc/sd-jwt, run it yourself, not cloud
- aca-py/bifold - Aries stack open sourced (BC), on-prem
- Dock - SaaS infrastructure platform for issuance and verification
- Mattr - Private cloud and on-prem for government/enterprise
- Procivis - proprietary/licensed on-prem
- Spruce/Credible - open source

(MSFT oid4vc sdk)

4 Tech Stacks - no clear winner in terms of provider - for the purpose of ecosystems, enterprises will likely need to support mobile app
Aries
OID4VC
mDL
KERI

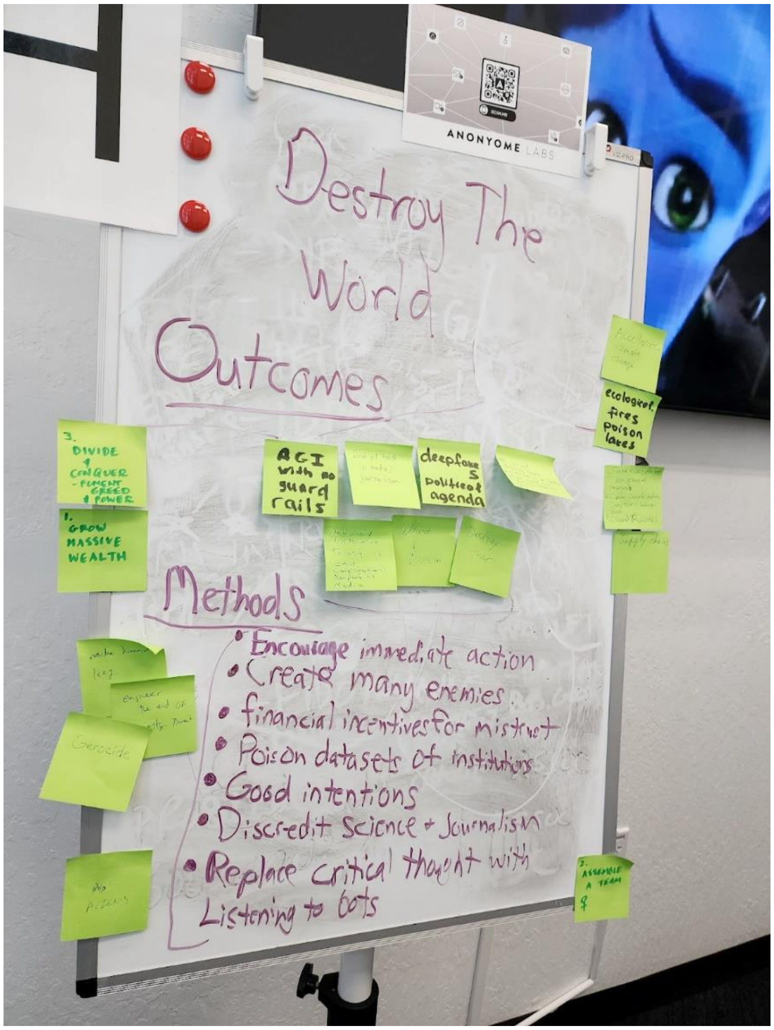
(Cloud provider "confidential compute")

Azure - Entry Verified ID
AWS - Nothing
GCP - Open Wallet Foundation focused?

Let’s Destroy the World!!! A hostile thought experiment

Session Convener: Kai Peacock
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:


ANONYOME LABS
Destroy The World
Outcomes
3. DIVIDE + CONQUER - FOMENT GREED + POWER
1. GROW MASSIVE WEALTH
AGI with no guard rails
deepfakes political agenda
Accelerate climate change
ecological fires poison lakes
Supply chain
Methods
• Encourage immediate action
• Create many enemies.
• financial incentives for mistrust
• Poison datasets of institutions
• Good intentions
• Discredit Science + Journalism
• Replace critical thought with Listening to bots
Genocide
2. ASSEMBLE A TEAM $

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

“World-destroying” outcomes

- Climate
  - Accelerate climate change
  - Ecological fires poison lakes
- AI
  - Deep fakes
  - Break trust
  - Destroy trust

    - Culture division
    - AGI with no guardrails
- Wealth
    - Divide and conquer
    - Grow massive wealth
- Human
    - Make human lazy
    - Engineer the end of humanity
    - Genocide
- Aliens

We selected a cluster of ideas around creating distrust in journalism / institutions, in particular through the creation of bots and using AI agents.

Then, we discussed some tactics that could be used to scale up the division

- Create / Invent Many Enemies
- Financial incentive
- Poison datasets of institutions
    - e.g. turn ChatGPT Evil
- Culture | Cynicism
- Coming against accessibility of complex solutions. Policy makers are not prepared for the regulations.
- Pace of threat
- Take advantage of good intentions. No one way.
- Discredit science and journalism.
- groundnews.
- Replace critical thinking
    - Listening to bots
- Unintended outcomes.
- Incentive engineers to slow down but produce? Immediacy?
- LHC, Oppenheimer
- VC Markets is driving some of this.
- Public development process
- Solve how you distribute a large pool of funds.
- Large agencies like meta

Takeaways -

There are very powerful tools already at play for eroding trust. We should be careful with our well-intentioned efforts, particularly as systems scale into having global impact

One particularly insidious world-destroying tactic was"financial incentives for mistrust". It creates a positive feedback loop for bad actors, and the financial aspect can subsidise the cost of otherwise expensive options like paid troll farms or AI swarms

Talk Workshopping = How good should Institutional Memory be?

Session Convener: Kaliya Young
Session Notes Taker(s): Kaliya Young

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

Kaliya workshopped a talk she is giving at EIC and got feedback from those who were there.
The talk will likely be online after the EIC event and she will talk about it there.

AnonCreds in W3C VCDM Format

Session Convener: Stephen Curran, BC Gov
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

- Slides: https://bit.ly/IIWAnonCredsVCDM
- https://github.com/hyperledger/anoncreds-v2-rs

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

At the last IIW, BC Gov announced a series of Code With Us procurements to fund open source work on making AnonCreds verifiable credentials and verifiable presentations operational using the W3C VC Data Model (VCDM), including support for the format in Aries libraries. The slides and the presentation went through the work that was done to achieve that goal, and the learnings gained along the way. Bottom line — we have working Open Source code that is planned to be used in the Aries deployments server and mobile being used at BC Gov, and elsewhere.

The session conversation covered the work, and got into discussions about next steps with the work — deploying it and how it might impact AnonCreds v2.

What's wrong with my wallet? A consumer's point of view

Session Convener: Susan Stroud
Session Notes Taker(s): Susan Stroud

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

Workshop prompt:

> Who has a physical wallet - could be in your pocket or your bag?
>
> Ok, now dump all of the contents on the floor. Just kidding.
>
> Did you just feel a sick feeling rising up through your body?
> That's [redacted], and it's what Lifequipt is here to solve.
>
> Lifequipt Vault allows you to store, organize, and share data relevant to you.
>
> For a bit of background context, Lifequipt is a technology startup committed to decentralization and focused on wellbeing.
>
> We build consumer experiences on top of platforms. Our go-to-market use case targets [redacted]
>
> We were one of 14 companies to demonstrate Verifiable Credential interoperability during JFF's Plugfest 2, and our solution is available using technology readily available now.
>
> So tell me, what are the reasons you won't use my digital wallet?

Participant responses:

- seeking mitigation of the risk
- want interoperability
- want to manage previously stored content
- want privacy statements and preferences
- want to know their data is secure
- want solutions on all devices

If you are interested in learning more or joining Lifequipt's innovator community, please contact Susan Stroud via LinkedIn (https://www.linkedin.com/in/SusanStroud)

The missing link… “HUMAN” in identity

Session Convener: Kenneth Gantt
Session Notes Taker(s): Tchaikawky “Troy” Samuels

Tags / links to resources / technology discussed, related to this session:

humans, systems, networks,

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

Question #1. Why is everything about systems and networks?

Comments:

Why did pre-sized clothing take-off?... Availability of access. It worked towards tailoring towards a user centric design. When it comes to identity and its perceived importance these views vary by geography, culture.

A lot of systems are antiquated because of the cost, scale and antecedence of existing systems and infrastructure. So, the challenge and focus is on the systems and networks because people will always be sufficiently more complex than any system they create to help manage themselves.

Convenience and community “The tyranny of convenience” a recommended book.

Question # 2. Have we truly looked at what QOW/QOL/Security/Privacy all mean to identity?

Comments:

Freedom of assembly can be negatively impacted when systems are created because it takes away from the free range that would exist otherwise. So there is some gain/loss associated with attempting to bring identity management into our daily lives.

Question # 3. Have we lost the bubble on generational understanding and identity?

Comments:
We need a greater focus on teaching the less literate portion of the population about the value of identity management.

SESSION #12

A Bridge to the Future: Connecting X.509 and DIDs/VIDs

Session Convener: Drummond Reed, Eric Scouten, Scott Perry, Stephen Curran
Session Notes Taker(s): Eric Scouten

Tags / links to resources / technology discussed, related to this session:

Eric’s notes

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

X.509 Overview
Scott introduced the CA mechanism which is used by browsers to make the trust/don't trust decision in HTTPS interaction. Each browser has its own governance mechanism, but they work together via the CA Browser Forum to share governance requirements known as Web Trust.

EU has its own trust infrastructure via EBSI. EU has a certification structure driven by EIDAS 1.

C2PA is evolving its own distinct trust infrastructure via its Trust List Task Force.

Browsers have worked together to require a control process for certificate issuance tracking known as Certificate Transparency Log, meant to prevent fake CAs from pretending to have issued certs.

DID/VID Overview
DID = Decentralized Identifier (W3C standard ~2 years ago). Ties public key, private pair, and identifier. Many but not all DID methods allow continuity of identity across private key rotation.

VID = ToIP concept, related to DID, but removing some of the syntactic requirements.

VID is an effort to reopen the tent.

Comparisons
In X.509, issuer is necessarily always a CA as a means of enforcing the governance rules. DIDs are much more open in issuance. X.509s could be considered VCs, but in a different format and with stricter governance.

DIDs and VCs split the human readable part vs the machine-readable part.

DIDs allow governance to be added post-hoc. A DID can be attached to a VC at a later point depending on the governance or requirements of the DID holder.

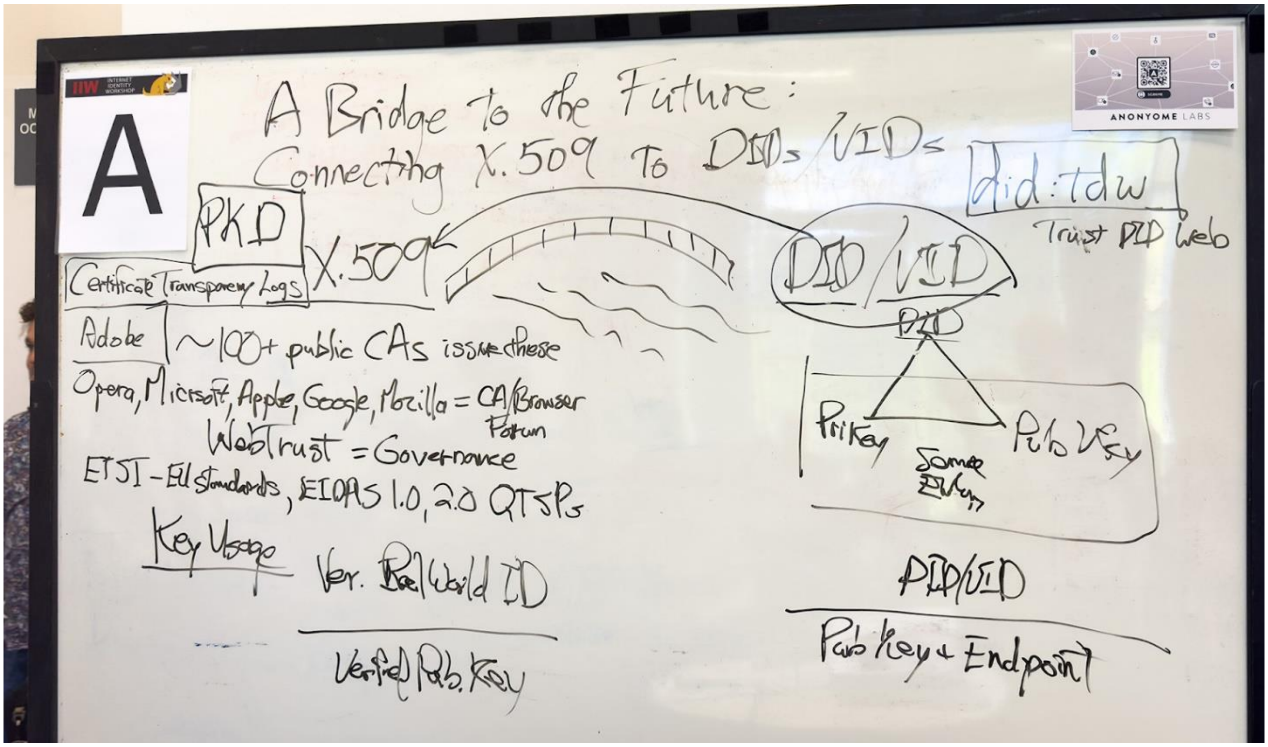


Diagram with X.509 and DID/VC comparison.

Is This a Bridge Worth Building?
Challenge that ToIP did:x509 TF has encountered: How do you retain a persistent identifier given that X.509 certs have to be periodically rotated? Maybe we don't.

Maybe the answer is to invert that. What if we encode a DID into X.509 subject alternative name (SAN) or similar field?

CA may or may not be able to use SAN depending on type of cert requested.

So can we describe a way for CSR (Certificate Signing Request) to include proof of control over the private key associated with the DID?

Lucy Yang and her company did a conversion of X.509 to DID a few years ago as part of WHO COVID credentials effort. (TO DO: Add link to this effort if possible.)

- **WHO X509 to DID conversion spec:** WHO already went production with the V1 specification we developed two years ago, you can find the information here:
    - Concept: https://smart.who.int/trust/concepts_did.html
    - Specification: https://github.com/WorldHealthOrganization/ddcc-trust/blob/main/TrustListSpecification.md#leading-contender-did-document They are working on V2.
    - This is the production key https://tng-cdn.who.int/trustlist/did.json
- **Trust registry collaboration:** As mentioned, we have some funding opportunities to support community projects like yours, so I would love to explore further timing and synergy. You can find some relevant information of my UNDP project here:
    - Regi-TRUST Introductory Video and Slides

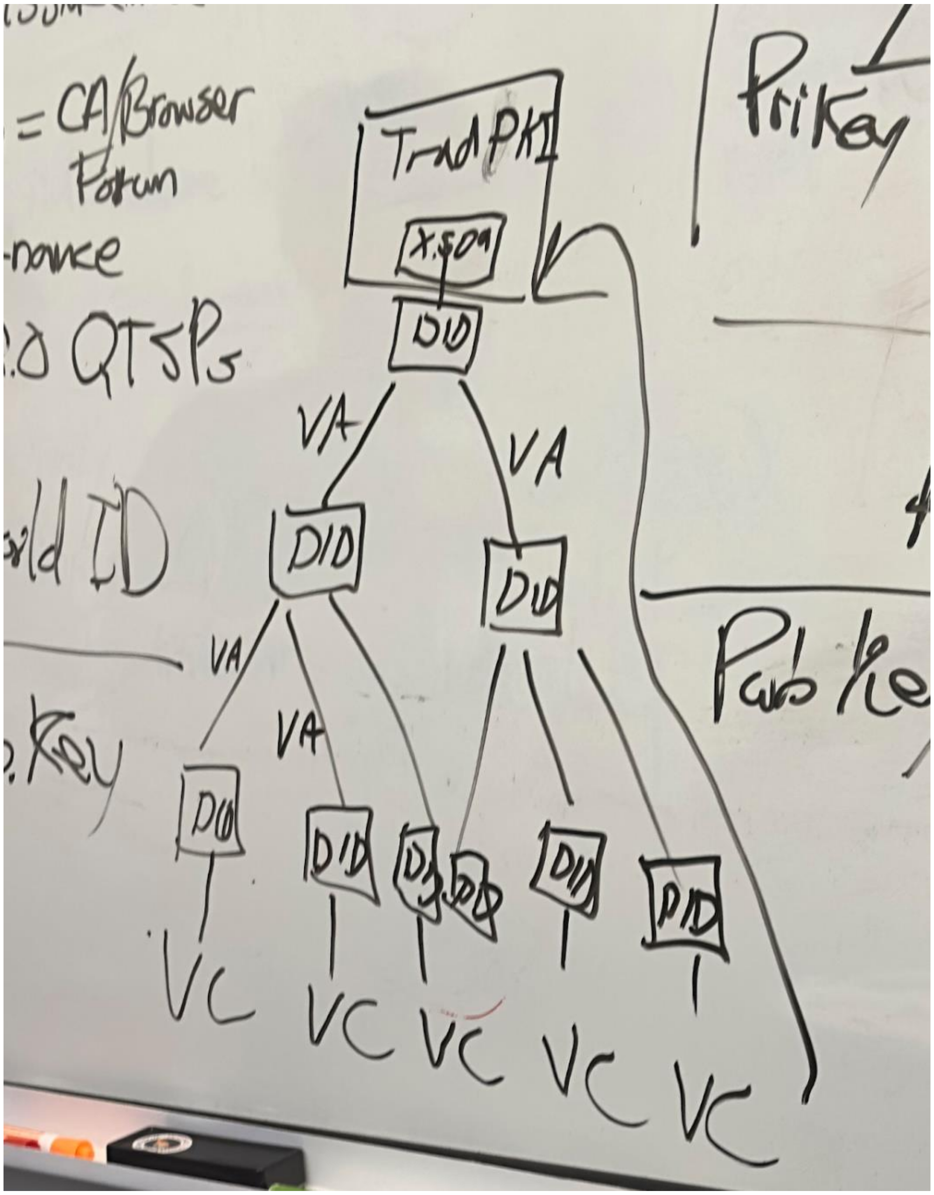
- Regi-TRUST Technical Specification
- Regi-TRUST Governance Consultation Summary Report

Essentially, we are leveraging the TRAIN model which is based on existing standards (e.g. ETSI Trust List) and infrastructure (DNS & DNS SEC), and it is credential standards and cryptography agnostic.

EBSI is working toward this using exactly this approach. (Follow up with Alex Tweeddale.)

California DMV is referencing X.509 chain via `x5c` parameter in a `did:jwk`.

Look into EBSI verifiable accreditation mechanism. Alex Tweeddale sent a link to a presentation he did regarding EBSI trust chaining.



Alex's sketch of EBSI verifiable accreditation mechanism.

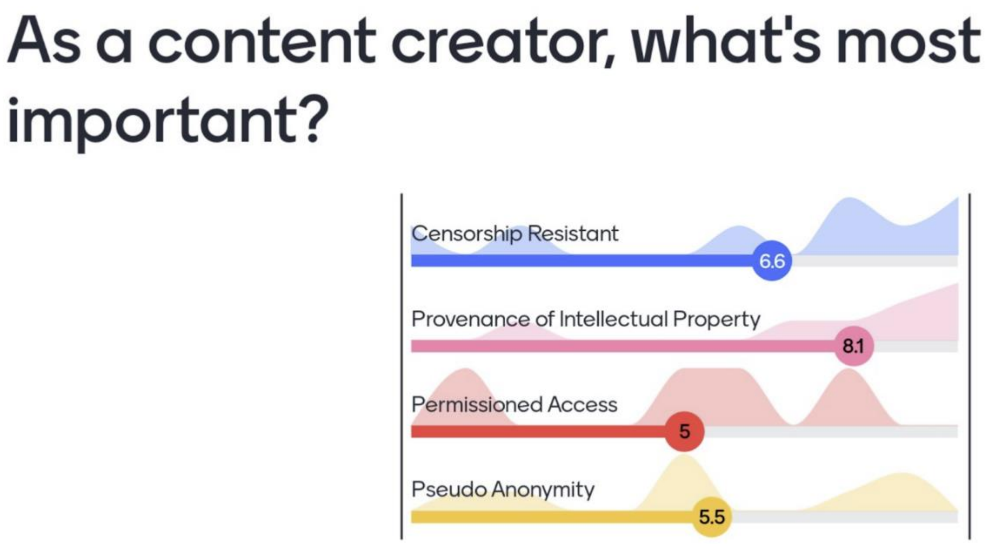
Verifiable Ownership of Permissioned Data: Leveraging Decentralised Networks with FISEPORTAL.COM

Session Convener: Nara
Session Notes Taker(s): Tchaikawsky “Troy” Samuels

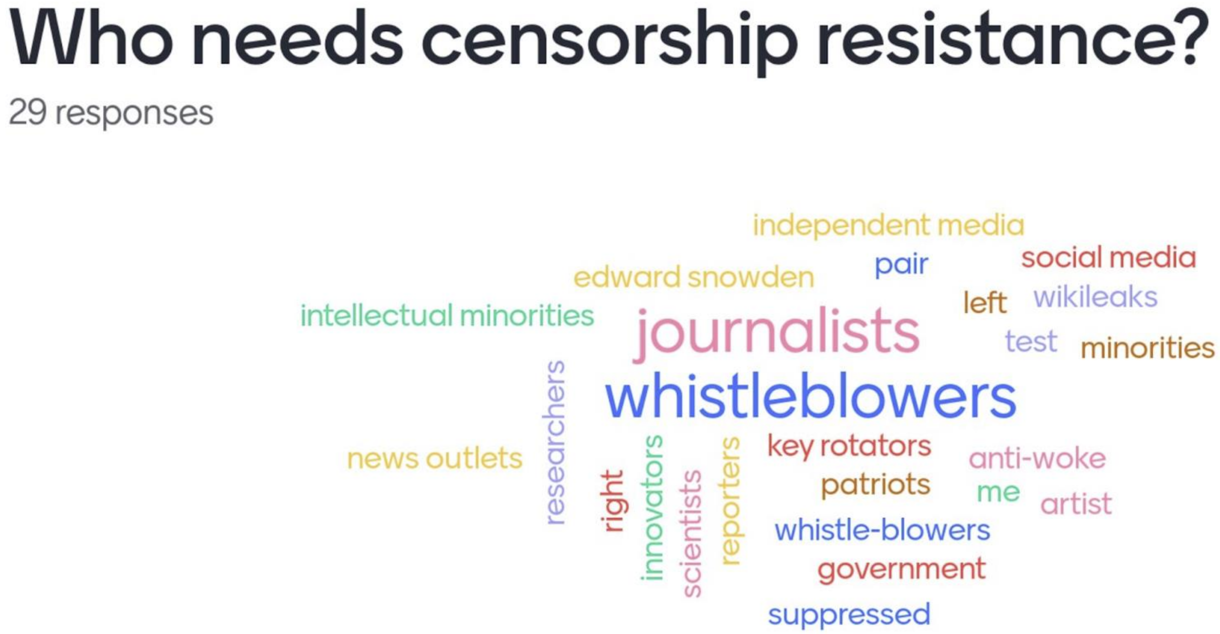
Tags / links to resources / technology discussed, related to this session:

FISE, content, Censorship, provenance, Permissioned access, Pseudo Anonymity

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



As a content creator, what's most important?

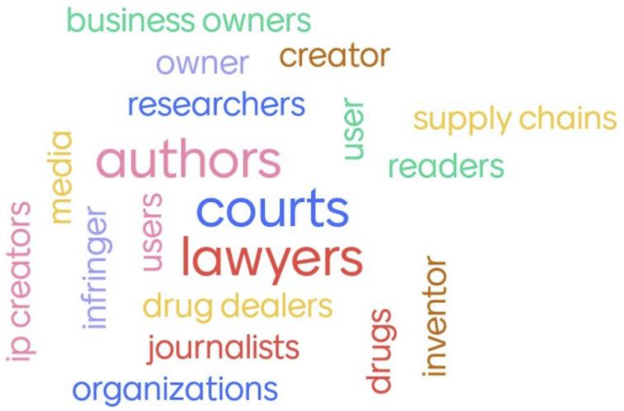


Who needs censorship resistance?

29 responses

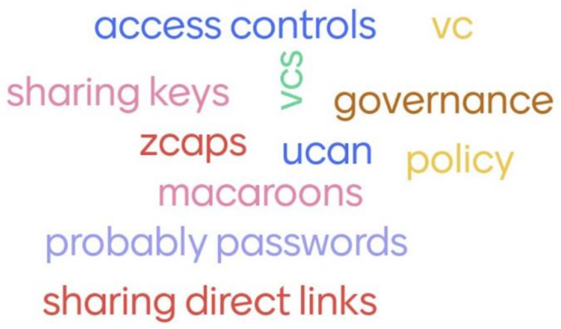
Who needs provenance of Intellectual Property ?

22 responses



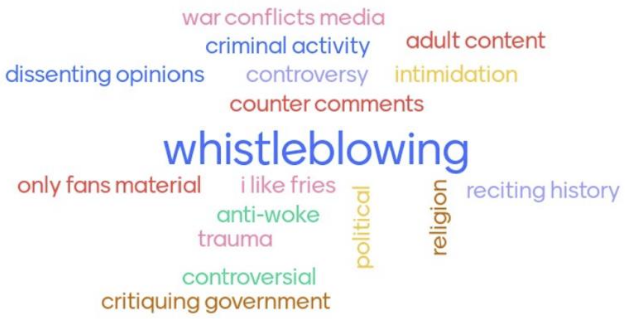
What are some known methods for providing permissioned access on decentralized network?

11 responses



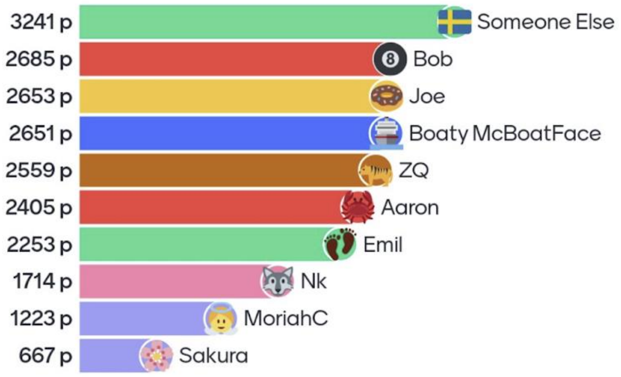
What kind of content needs pseudo anonymity for the authors to feel safe to share?

19 responses



Mentimeter

Leaderboard



TSP (Trust Spanning Protocol) Part III - Implementation

Session Convener: Wenjing Chu
Session Notes Taker(s): Wenjing Chu

Tags / links to resources / technology discussed, related to this session:

The TSP spec draft: https://trustoverip.github.io/tswg-tsp-specification/
To contribute: https://github.com/trustoverip/tswg-tsp-specification
And Task Force wiki:
https://wiki.trustoverip.org/display/HOME/Trust+Spanning+Protocol+Task+Force

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

We discussed the initial implementation of TSP in Rust.
The implementation project in Rust is ongoing with Direct Mode and example VID and Transport mechanism to do testing and demos.
The TSP Rust Crate's documentation is here: https://docs.tsp-test.org/tsp/
You can experiment with the current software on this site: https://tsp-test.org/
Current source code is temporarily hosted here: https://github.com/wenjing/rust-tsp

Welcome your inputs/feedbacks. We also ask for inputs on your priority features, VIDs, transports, and any applications you have in mind. Feel free to contact me directly or on the github pages listed above (on the draft spec and the Rust implementation respectively).

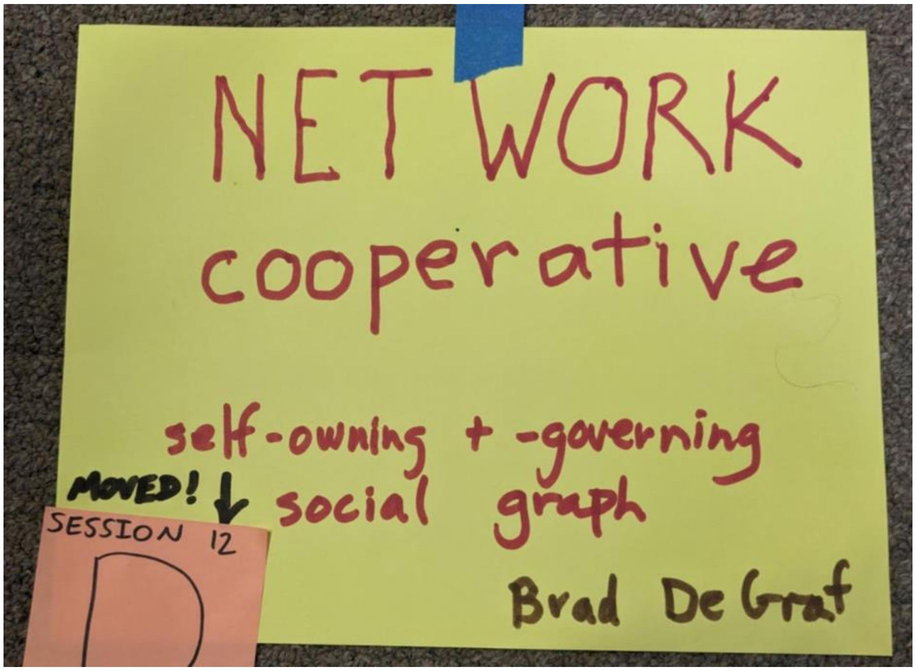
NETWORK COOPERATIVE - Self-Owning + Governing Social Graph

Session Convener: Brad de Graf
Session Notes Taker(s): Day Waterbury

Tags / links to resources / technology discussed, related to this session:

Noo NAO

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



Linking notes to all our woven sessions here (Proton Drive PW: Share->IIW38 or Signal me @deiim.69 in case I change the PW) to save time. If I can I'll pull the session-specific transcripts in.

Identity - Related Fraud / FinCEN

Session Convener: Cam Geer| Cryptid |https://www.linkedin.com/in/camgeer/
Session Notes Taker(s): Charles Lanahan | Cam Geer

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

From Cam Geer:

FinCEN reports 1.6 million Identity-Related Fraud Incidents Valued at $212 Billion in 2021 Data

In early January, Kay Turner, Chief Digital Identity Advisor at the Financial Crimes Enforcement Network (FInCEN), a division of the US Treasury, and her team issued a report that summarized findings from about 3.8 million Suspicious Activity Reports (SARs) that were filed in 2021. https://www.fincen.gov/news/news-releases/fincen-issues-analysis-identity-related-suspicious-activity

[Note: a broad array of businesses in financial services industry are obligated to files SARs to FinCEN when activities or transactions occur that may be related to money laundering and other illegal activities.]
For more detail: https://fincen.gov/resources/filing-information

About 42% of the SARs filed in 2021 or 1.6 million reports valued at $212 Billion of harm or fraud were determined to be related to Identity! That's a big problem, and many of you are likely already wrestling with aspects of this. It also presents a HUGE opportunity for ID practitioners to take a leadership position in your organizations to help to solve these problems, particularly for ID practitioners in financial services and fintech. But as we'll see all ID practitioners have a role to play in the financial security of their businesses.

But where to start on such a big problem with so many potential dimensions?

FinCEN has done us a huge favor by sifting through the data and organizing it into well defined typologies. These will give clear starting points for further discovery in order to better understand the underlying problems at the root of identity-related suspicious activities.

You might immediately jump to often discussed fraud types -- Synthetic Identity, Account Take Over, or detecting counterfeit documents, while an important part of an Identity program to reduce fraud, the data shows that you might have greater impact working with your security, compliance, and policy teams to attack much bigger targets -- Access Abuse, Business Email Compromise, Cyber Security Incidents -- when ranked by $ value / SAR.

FinCEN Financial Trends Analysis
Identity-Related Suspicous Activity: 2021 Threats and Trends | January 2024

Summary Table

To review all 14 typologies for your own analysis, please review: https://docs.google.com/spreadsheets/d/1F5wToehrqDYdO7G2qYiPW6niyHGlAtYQWRVN3qAQIQY/edit

This analysis is meant to drive discussion and additional investigation into the problem space before specific solutions are applied.

Kay Turner, has issued an open invitation to Industry to come to FinCEN to dig into the data in order to define explicit customer problem statements so that product development teams can build hypotheses and test plans to go after these problems.

The Opportunity / My Ask

Identity has a leadership opportunity to massively impact in a positive way -- customer experience, better business results by reducing fraud; better security by partnering with security teams to reduce threats, and intrusions; and better compliance by more deeply understanding the regulatory and legal policy obligations your business has, which in turn influence the other areas. It is a virtuous cycle. And no doubt a big job!

But some domain needs to take on the leadership here. Identity is in pole position to do that by being a strong advocate for the Customer/Business End User, having deep understanding of and empathy with them, AND the business, security, compliance domains in your organization. Through the synthesis of this deep knowledge across these domains will give Identity the insights to bring real, effective value added solutions that will yield better results. A more inspiring mission than continue to patch broken / leaky systems.

More Product Management Discipline is Needed in the IIW Community

I made the comment in our session that there is a real lack of the product management discipline in the IIW community.

Overall, Identity practitioners need to better understand the problem space of their target prospects and customers. To deliver effective digital identity solutions to market, you need to understand at a deeply empathetic level, the day in the life of the customers you are trying to serve. For example, you need to understand the legal and regulatory constraints that a Chief Compliance Officer has, plus the business policy your organization has in place to support the reporting requirements to your regulators (in fintech for example). Know the reporting thresholds, reports formats, reporting schedule, escalation paths, your general counsel's advice, your security team's struggles to keep up with deep fakes, intrusion detection and types.

Most importantly, go talk to real customers who have been victims of fraud. What has it done to them personally? Were they not able to buy groceries for their family? Miss a car payment? Be threatened with foreclosure?

The more that real world problems and pressures are understood, the better a problem-solution fit can be found to be served by an effective identity product.

See below for the resources I mentioned that can help you get started

Resources:

- FinCEN
    - Identity-Related SARS reports [Jan 2024]
    - SARS Filing Requirements
- FinCEN Identity-Related Fraud Data Summary by Cam Geer
    - publicly available Google sheet open for comments

- Product Management Tools
    - Shreyas Doshi | https://shreyasdoshi.com/
        - Watch his YouTube Videos, read his blog, sign up for his 2-day class
    - Marty Cagan | https://www.svpg.com/team/marty-cagan/
        - World-renowned author & advisor on product management
        - He literally wrote the book on the software product management
        - Read All 3 Books - Inspired | Empowered | Transformed
    - Matt Lerner | https://www.systm.co/about-matt-lerner
        - Read | Growth Levers (it's only 120 pages)
        - Well distilled practical actions any technology product company MUST take in order to discover their product-solution fit.
        - Matt is a former colleague from PayPal and personal mentor in the practice of Customer / Product discovery. Learn from one of the best.

From Charles Lanahan | Session Notes

FINCEN - Financial Crimes Enforcement Division focused on KYC/AML SARs (Suspicious activity reports) - suspicious or unknown transaction reporting.

FINCEN released report Jan2024 stating that starting in 2021 1.6M SARs reports ~= $212B in Fraud big problem!

Purpose of this talk is to identify areas of investigation in solving these real world FINCEN customer problems and bring stakeholders in risk, security, compliance, together to solve these problems with the digital identity community.

If we focus on these big areas of where FINCEN reports say fraud and abuse exist, then we can start to move the needle.

Most of these things still focus on biographics.

what is the appetite for change within banks itself?

Historically they've operated in compliance by static based data processes. This is an obstacle. We need to move to dynamic authentication and dynamic authorization. It has to meet their risk profile and risk management governance has to be taken into account.

late binding trust is important in the future.

Auth Fraud/Authentication, access fraud vs general fraud, is the typical breakdown. In the analysis we've split out into other buckets.

Social Engineering/authentication is one of the key problems in account take over for example.

What are the risks of using biometrics to auth financial transactions?
Gotta be careful, don't want a police state.

Where do the two curves of cost vs liability intersect?

Policy will drive implementation.

Focus on the customer would be the ideal outcome of this.

Personalized Pricing Hell—How to Deal With It

Session Convener: Joyce Searls
Session Notes Taker(s): Doc Searls

Sam Curren
Dave Grantham
Joyce Searls
Adrian Gropper
Doc Searls
John Wunderlich
Kazue Sato
Hadrian Zbarcea
Michael K
Bruce Conrad

Tags / links to resources / technology discussed, related to this session:

#Pricing
Welcome to Pricing Hell https://www.theatlantic.com/ideas/archive/2024/04/surge-pricing-fees-economy/678078/

Getting us wrong:
https://doc.searls.com/2023/12/29/getting-us-wrong/

Amazon's Pricing Policy Caused Consumers to Overpay by $55B to $172B, Class Action Claims
https://www.classaction.org/blog/amazons-pricing-policy-caused-consumers-to-overpay-by-55-to-172-billion

Mac users might be paying more than PC users for airline tickets and more
https://www.imore.com/mac-users-might-be-paying-more-pc-users-airline-tickets-and-more

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

Joyce We will miss, or need, the bazaar experience.

Dave Grantham (Huseby) He and his wife got totally different pricing for a coffee maker from Amazon, likely based on algorithmic assumptions.

Need privacy tools to get the cheapest thing.

Michael K. A bucket of need-based grants poured on him that suggddenly dropped when the algorithm changed. Benefits fell.

Sam Curren "Need to disown my kids, for their own good"

Concern: some of this pricing stuff is coded into law.

Amazon et. al. track spending and other variables constantly and tease prices around. Can we morally argue that this is bad? How will it affect haggling? Can we argue that this is wrong?

Doc: “Markets are relationships” story from a chapter of the 2nd edition of The Cluetrain Manifesto.

Joyce: We want the corporations to know us as humans.

Hadrian Zbarcea
All the tools are on their side
We need “a Tor for shopping”

+
Sam: When you add an intermediary

Phil’s daughter and friends screwed with algorithms for entertainment

Don Marti: “whiskey and diapers”

Joyce: “Poverty as a service!” Everybody gets to be poor and buy for less. (PaaS)

Michael:
Remember Farecast?
https://www.phocuswire.com/Remember-Farecast-Bye-bye-Bing-Price-Predictor

Hadrian: You need the right pool of people for PaaS.

Sam: Camel Camel Camel is now part of Amazon.
https://camelcamelcamel.com/

[This part of the discussion has been redacted by a vote of the members.]

Adrian: The request processing RO-AS must pass a request to the RS-AS as an extension to GNAP requests

Michael: How about anonymizing our information.

Dave: That is actually impossible, now that transaction annotation is possible. Mobile carriers snitch IMEI and much other information.

Dazzle Office Hours / FediTest: testing distributed, heterogeneous systems w/complex protocols (Fediverse)

Session Convener: Johannes Ernst
Session Notes Taker(s): Lisa Dusseault, with some additions by Johannes

Tags / links to resources / technology discussed, related to this session:

Dazzle Labs: https://dazzlelabs.org
UBOS: Open-source software for a thriving social web of peers: https://ubos.net

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

Overview UBOS https://ubos.net/docs/architecture/

Then Feditest: https://feditest.org

Testing interoperability of real use cases on servers can require having live servers that can be accessed via the protocol under test, but also provisioning them requires features not in the protocol under test.
* Example: posting a message on 1st server, reposting it on 2nd server, receiving that on 3rd server, deleting it on the 1st server, what does it look like on the 3rd server…
* Also testing interesting use cases often requires multiple instances from different implementors and seeing how they interact and
* FediTest effort to test ActivityPub implementations is just one of many examples of test domains that require instance provisioning and setup

[Open-source software for a thriving social web of peers | Top](https://ubos.net)
UBOS is a platform for self-hosting all kinds of different things including ActivityPub servers of different implementations and versions.
* Feditest is building on UBOS and adding the provisioning stuff in a variety of forms
  * can be through protocol-under-test
  * can be through Playwright or other automated mechanisms for
  * in last resort, can prompt the tester to do a specific thing e.g. “Now click allow in the admin interface”

OpenID4VC as Framework vs. Profiles

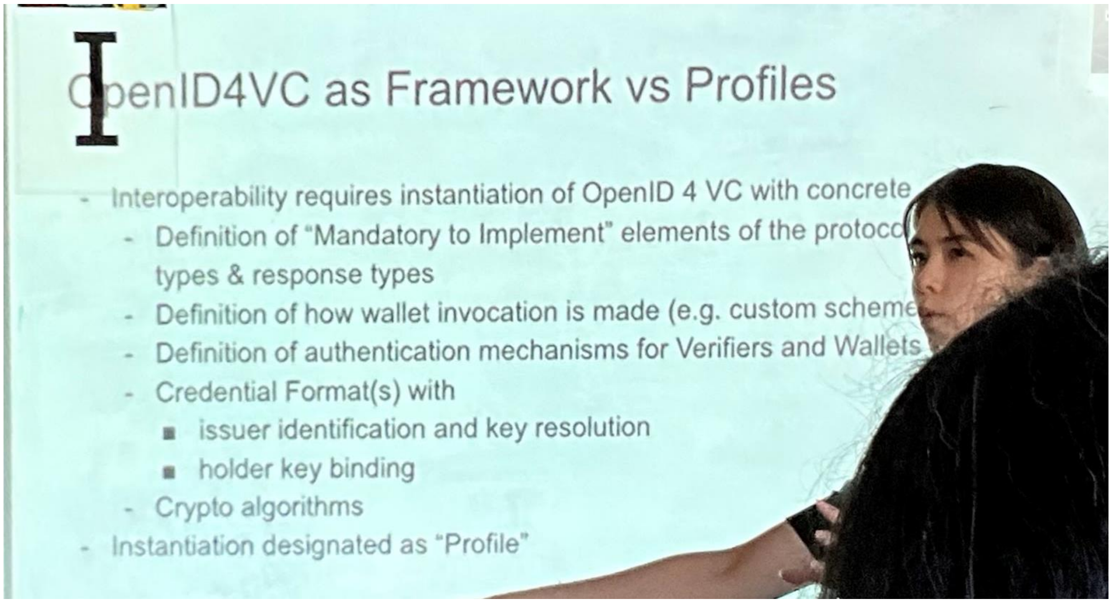
Session Convener: Kristina Yasuda
Session Notes Taker(s): Jin Wen

Tags / links to resources / technology discussed, related to this session:

OpenID4VC High Assurance Interoperability Profile with SD-JWT VC (https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-sd-jwt-vc-1_0.html)
JWT VC Presentation Profile from
https://identity.foundation/jwt-vc-presentation-profile/
OpenWallet Foundation Credential Format Comparison SIG has an overview of 19 credential formats
https://openwallet-foundation.github.io/credential-format-comparison-sig/#/
from slide 66 of this slide deck: OID4VC_20240410_OSW.pptx (1).pdf

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

OpenID4VC as Framework vs Profiles
- interoperability requires instantiation of OpenID 4 VC with concrete
- Definition of "Mandatory to Implement" elements of the protocols, e.g. grant types & response types
- Definition of how wallet invocation is made (e.g. custom scheme)
- Definition of authentication mechanisms for Verifiers and Wallets
- Credential Format(s) with
• issuer identification and key resolution
• holder key binding
- Crypto algorithms
- Instantiation designated as "Profile"



OpenID4VC as Framework vs Profiles

- Interoperability requires instantiation of OpenID 4 VC with concrete
  - Definition of "Mandatory to Implement" elements of the protoco
    types & response types
  - Definition of how wallet invocation is made (e.g. custom scheme
  - Definition of authentication mechanisms for Verifiers and Wallets
  - Credential Format(s) with
    - issuer identification and key resolution
    - holder key binding
  - Crypto algorithms
- Instantiation designated as "Profile"

OID4VC High Assurance Interoperability Profile with SD-JWT VC
Interoperability across parties while being
- Privacy preserving and
- able to fulfil security and regulatory requirements

- Intended audience
- Proposal for eIDAS ARF (through OIDF/EC liaison)
- CA DMV wallet
- Basis for OWF project(s)
- IDunion Tech Stack
- GAIN PoC
- Japanese government (Trusted Web project)
- Basis for Userinfo
- other jurisdictions
- private companies / infrastructure companies

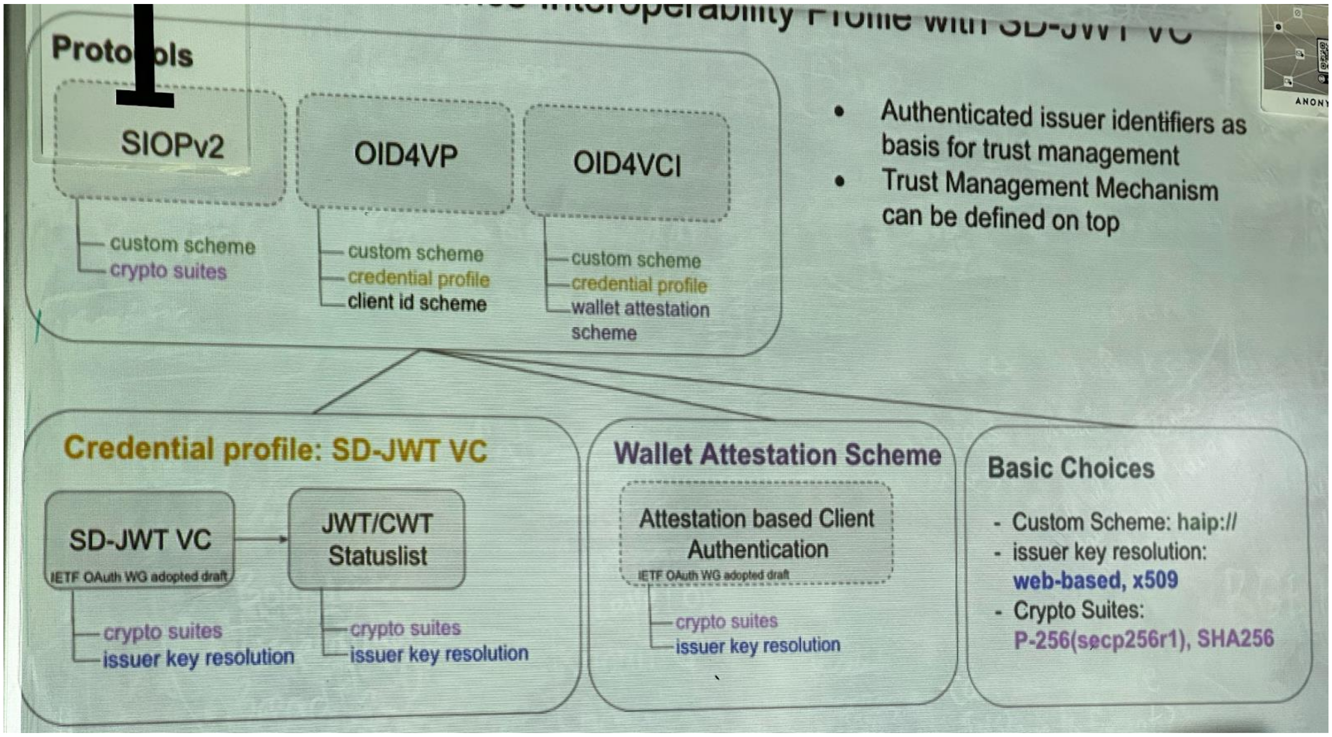
where does profile itself sit?

- it does not have to be within DCP working groups, though this one (High Assurance Interoperability …) is.
- Enterprise Profile used by LinkedIn is in DIF

Rick Byers: ask that state of conformance testing: it require a profile to be tested in OIDVP
Lee

- something about interactions between profiles?

OIDVC High Assurance Interoperability Profile with SD-JWT VC



Interoperability Profile with SD-JWT VC

Protocols

SIOPv2
- custom scheme
- crypto suites

OID4VP
- custom scheme
- credential profile
- client id scheme

OID4VCI
- custom scheme
- credential profile
- wallet attestation scheme

- Authenticated issuer identifiers as basis for trust management
- Trust Management Mechanism can be defined on top

Credential profile: SD-JWT VC

SD-JWT VC
IETF OAuth WG adopted draft
- crypto suites
- issuer key resolution

JWT/CWT Statuslist
- crypto suites
- issuer key resolution

Wallet Attestation Scheme

Attestation based Client Authentication
IETF OAuth WG adopted draft
- crypto suites
- issuer key resolution

Basic Choices
- Custom Scheme: haip://
- issuer key resolution: **web-based, x509**
- Crypto Suites: **P-256(secp256r1), SHA256**

Protocols

SIOPv2

- custom scheme
- crypto suites

OIDVP

- custom scheme
- credential profile
- client scheme

OID4VCI

- custom scheme
- credential profile
- wallet attestation scheme

Credential profiles: SD-JWT VC

SD-JWT VC

- crypto suites
- issuer key resolution

JWT/CWT Status List

- crypto suites
- issuer key resolution

Wallet Attestation Scheme

Attestation based Client Authentication

- crypto suites
- issuer key resolution

Basic Choices

- custom scheme: haip://
- issuer key resolution
- Crypto suites: p-256(secp256r1), SHA256

There is questions about different credential profile comparison, see comparison table done by TrustOverIP Credential Exchange Task force

Credential Comparison Matrix

Nowadays in OpenWallet Foundation: https://openwallet-foundation.github.io/credential-format-comparison-sig/#/

Running Lean with SSI; The Business Model to go from Idea to Company

Session Convener: Jared Jeffery, MBA & Timothy Ruff
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

Link to the slides:
https://docs.google.com/presentation/d/1_NimAfNdr9NoSk6MnwyZ_vC06SImDoXuT2LVcheNKck/edit?usp=sharing

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

Identity v. Anonymity: How to best interconnect both to expand discussion on issues across countries? America's November Election

Session Convener: Blake Stoner
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

AuthZ Conf. Planning Call - Who & How to Convene a comm?

Session Convener: Rohit Khare
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

SESSION #13

Advanced Topics for OpenID4VCI

Session Convener: Paul Bastian, Kristina Yasuda
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

2 PRs that have been discussed:

- https://github.com/openid/OpenID4VCI/pull/155
- https://github.com/openid/OpenID4VCI/pull/293

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

Trust Establishment with OpenID Federation

Session Convener: Mike Jones, John Bradley
Session Notes Taker(s): Mike Jones

Tags / links to resources / technology discussed, related to this session:

EUDI digital Identity Wallet Architecture & Reference Framework: "As part of this verification process, the Relying Party also obtains a public key of the Provider, which functions as a trust anchor and allows it to verify the attestation signatures created by the Provider. There are at least two methods to communicate this public key, using peer-to-peer communication, or using a trusted list. The public key itself may be encapsulated, for instance in a X.509 certificate or in an Entity Statement according to **OpenID Federation**."
https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md#6322relying-party-trusts-provider

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

The session was well attended and the discussion lively. Numerous people with trust establishment problems to solve contributed, including experts from the SAML federation world, people involved in digital wallet projects, and several people already using or considering using OpenID Federation. Thanks to all who participated!

See the materials used to drive the discussion at https://self-issued.info/?p=2521.

DID or not? The Value of an Identifier Metasystem is EIDAS wrong?

Session Convener: Sam Curren
Session Notes Taker(s): Zaïda Rivai

Tags / links to resources / technology discussed, related to this session:

Link to eIDAS Architecture concept (non final) – https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework

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

Sam Curren DIDs identifier metasystem (IMS)
Sam:

- **Should we use the DID core spec or not?**
- No argument for why you shouldn't use the DID core spec, is there any argument against DIDs
- DIDs have received a lot of critics, one of them is there are too many DID methods. One of the things provided by the DID core spec, is that nothing really got quite to Identifier Metasystem. The core functionality is that you can have a unique identifier, resolve that, you get keys and service endpoints. Some of them allow to rotate the keys.
- Identifiers; strings that identify things.
- What do I mean by an identifier metasystem?
  - Non identifiers, are not unique, but we need that in certain systems.
- Metasystem: is a system of systems. One system can manage other systems underneath it. The metasystem (not in the did core spec), one of the main features not in the DID core spec
- DID Methods: Allow for a variety of methods, from identifier to DID document. Can be really different (Bitcoin, Ethereum, DID:Peer)
- The fact that we can have variety is a powerful feature, allows us to be smarter tomorrow.
- Imagine a company, that uses DIDs as identifiers for employers, if company A buys company B and they use different DIDS (DID:A and DID:B), they have their own DID methods, they could still work. Non conflicting identifiers.
- This scenario happens even more online, where you can end up with cross collaboration (with or without merging). No conflict when you merge these systems together.
- Every identifier system, ends up by a set of rule (SSN, phone number etc…). If you start from an identifier system, you have a major refactor coming. You might have some good reason to make a change, but that is very painful.
- My argument for using DID core spec (therefore the identifier metasystem vs. identity system), is that if you start with a DID core spec you can avoid a raft of problems, that come with identity systems later.
- One of the arguments I've heard is: "we're not sure which DID methods to use, so not using DIDs at all" or "Impossible to resolve all DID methods, so we're not going to use DIDs at all"

- Even the uni resolver isn't solving all DIDs ()
- If you'd pick an identifier, using DIDs at a metasytem level and select one DID has a credible value. Smarter moving forward and making small adjustments and switching from one identity system to another.
- I'm familiar with keys, JWK's for example, if you have some reason, you come convinced ()
- What I propose: use DID:JWK, and use that.
- Cross ecosystem collaboration, we don't have a conflict.

Zaïda Rivai:

- Are you referring to the "Business people" that aren't agreeing on DIDs or the Tech folks?

Sam Curren:

- This Identity Metasystem (IMS) addresses both
- Folks that have chosen JWK (know PKI, so therefore they chose JWK). The reason I'm bringing this up is because no one else has done it.
- "I know X.509 and DID's are too new" to them I say look at the DID X.509 DID.
- We have a huge missed opportunity that hasn't been taken.

Kai:

- Been involved in some of the arguments. The main reason to use DIDs and VCs is because it's a tracking () across different users. European architecture:(1) how can we issue credentials, (2) how can we issue the same credential only X amount of times. The debate is, if you go for credentials and wallets, how do you issue them in a privacy preserving way. This has no one solved so far. This is useful to mention.

Sam:

- One of the things, even if the user has a bunch of DIDs, in order to use that you have to issue each credential to all of the users and that has a lot of issues.
- Private holder binding: the ability to prove that the credential was issued to you and alongside other credentials, without revealing the common identifier (the did in this case). If you issue it to a JWK, this still becomes a tracking identifier. The fact that they know that but the DIDs aren't doing any better. JWK less trackable to DIDS?

Kai:

- IN the regulation, update the existing EU digital identity framework. eIDAS 1.0, every country has their own system. This time they utilize concept sand regulatory () from the past. Trust services from the past regulated by the same regulation built on top of x509, huge body how to govern that, how to certify that. People are very hesitant to move away from that trusted model, making sure that authenticity is there. Compared to other regions, nobody wants to change that. What didn't work, was interop across border. Knowing that the entity does what is expected, that did work.

Sam

- Added a note that x509 is the standard used for institutions.
- Keys that you're using for the people involved: incompatible identifier systems.

Oliver Terbu:

- PID: personal identifier, they don't have to be ()
- eID: anti cloning, idea is that you cycle through a bunch of credentials to (). Can't use the same key for entire life of PID (?).
- The PID is not an identifier, the purpose is not to identify the user based on a key. Some countries have identifiers as a claim, but Germany for ex have a set of other claims. The public key, where the credential is bound to, is not the identifier. The key rotates constantly. Also why mdl etc ()

Sam

- Differentiate between whether ()
- Arguments for IMS, "you used x509, the IDM benefits kick in, where you have a system that it can detect both systems.

Kim Hamilton Duffy

- Is the key rotation part also part of ARF?

Kai:

- Important to mention that what we talk about here, we build the foundation of root of trust.
- The thing where there is an agreement, exchange protocols etc…
- The toughest nut to break is that each member state has their own idea.
- It's not yet settled.

Kim:

- "Section listed as a requirement"

Oliver

- eIDAS regulation
- ARF is the tech framework how eIDAS 2.0 is implemented

Kai

- Eu law: general law that all the gov players agree on. The European Commission is creating delegated acts, that are very concrete. Those acts don't offer customization. These acts have to be published 4 months after law. It's finalized but not yet published. The law fully agreed on everything, but there is still an ongoing discussion.

Martina

- You have the case with x509 institutions, how would that work.

Sam

- There is a DID method on x509, you design systems to store a DID. Institutions are (). JWK is for individuals, not entirely correct. Can live in the same DB field, an identifier, but two same DID methods used. Every time when using an identifier to refer to an entity. You systems doesn't have to make a massive adaption in the move.
- Bigger idea; impact

- Smaller idea: to implement this, isn't very hard.
- But if you implement this, you'd benefit without dealing with the hustle of changing/merging identifier systems.

André:

- ARF is not complete
- EBSI: tech spec, requires EU standards.

Sam:

- Keys aren't necessary identifiers, they are just keys.
- Interesting thing: even a group etc… could make a decision to use the IDM.
- Even if they use the single DID method.

Stephen Curren

- Each of those circles make it combinable. As long as the IMS is DIDs you guarantee no collision.
- Not different DID methods in each circle.

Sam

- What I intended:

Sam

- The early DID discussions at IIW, everyone feared DID:Facebook. What I came to realize is that it doesn't matter.

Oliver

- Assuming eIDAS is using this, we need should use one DID method, and then why do you need DIDs for that.

Kai

- Switzerland: if they have a different DID method () IMS would solve one of the first inter problems, how to resolve the thing and have a method to interpret it. If your system has to implement that five times, you have many problems.

Sam

- DIF could write about this from an education perspective. If I just use one DID method, why do I need to use the DID method at all?
- Shocked to learn how telco feel cheated, cause they feel they have the right to sell something to you. So internet is pissing them off.

- Hope was to expand this concept and discuss the value there. Long thing to make progress, not really been recognized in DID Core spec.

Provenance from First Principles Part 1

Session Convener: Dave Grantham | https://www.linkedin.com/in/david-grantham-87207a265/
Session Notes Taker(s): Cam Geer | https://www.linkedin.com/in/camgeer

Tags / links to resources / technology discussed, related to this session:

- Cryptid Provenance Specification | https://github.com/cryptidtech/provenance-specifications
- Cryptid GitHub | https://github.com/cryptidtech/
- Hyperledger / Open Wallet Foundation | https://github.com/hyperledger/anoncreds-v2-rs
- Cryptid | Unified Theory of Decentralization | https://www.cryptid.tech/post/a-unified-theory-of-decentralization

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

content addressing > independent storage >> IPFS | S3 buckets | http://domain/[hash]
digital signature > bound to actors > ECDSA Threshold M of N
self-describing data . implementation independence | multiformats

- variant [u8; N] > varbytes

stack machines > execution independence | WASM

WASM (Web Assembly)

- bottom half of Javascript Gecko spec to enable portability across systems and devices
- an execution environment | doesn't know how to do anything

Theme

- max decentralization

Web Assembly Cryptographic Constructs (WACC)

- check sig
- check

Provenance

- unbroken chain of custody
  - hashed for tamper evidence
  - accumulation of events overtime (f(t))
    - blockchain useful only for immutable ordering of events (time)
- digital signatures to bind control

Identity is not anything you have or control

- accumulation of data over a course of time
- "key history" in any content / as it exeist in

XZ - opportunity for industry to better fun maintainers and have threshold signing

---

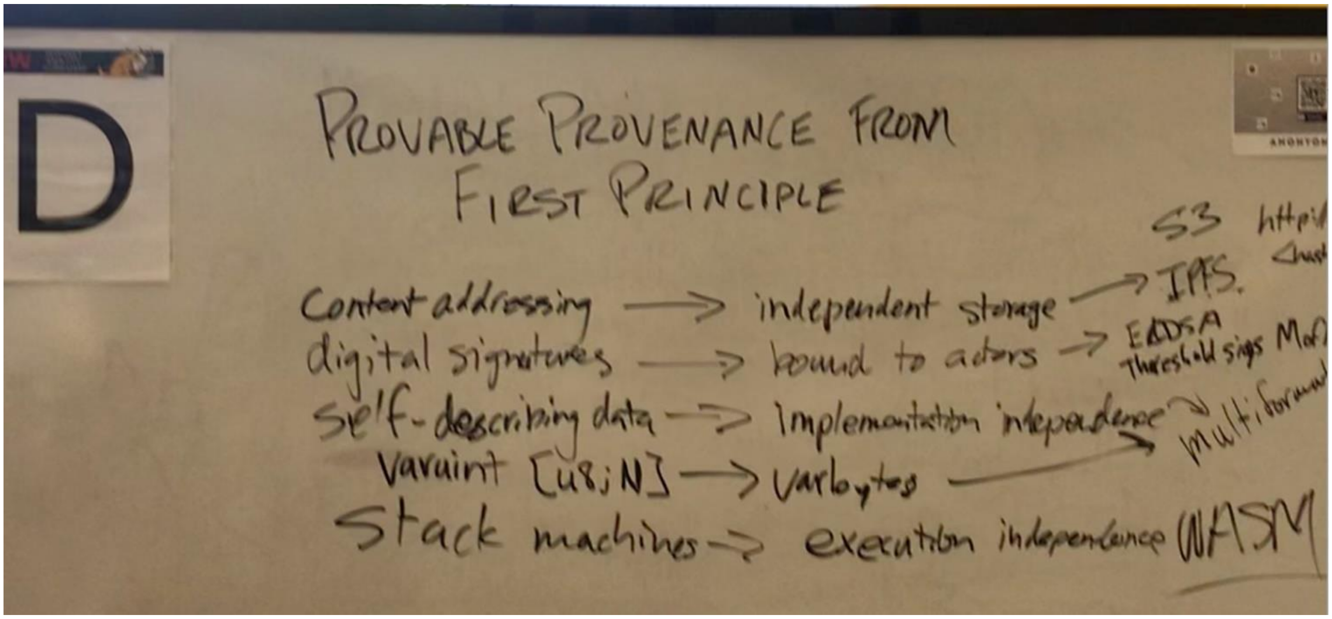
Open Source Supply Chain

- provenance logs
    - event log
    - chain of custodiy
    - cryptographic puzzle - for who can add next event
- sequence #
- VLAD
    - very long-lived address

A Provenance Log Schema

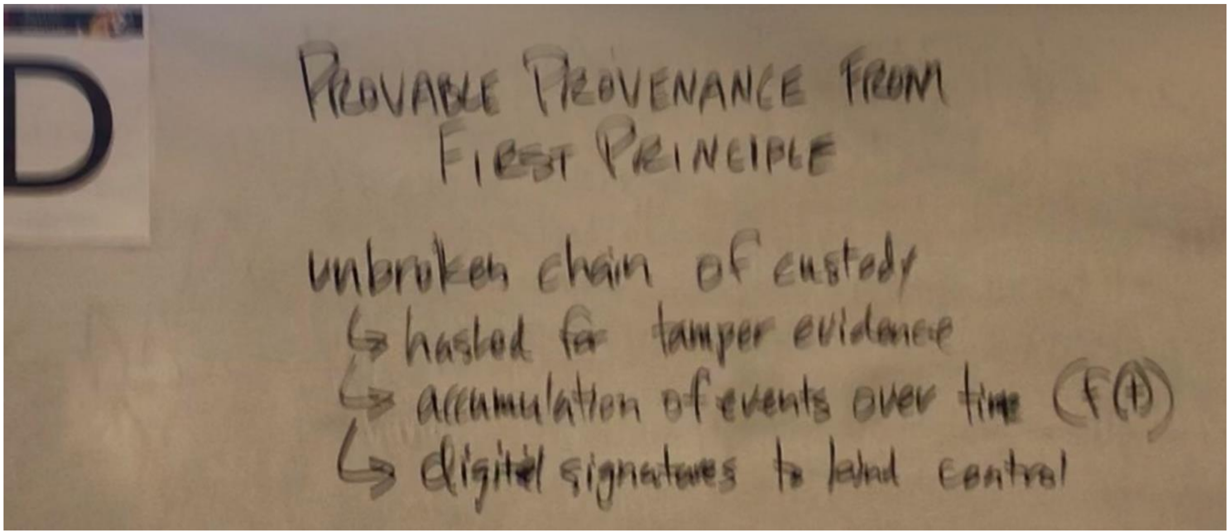
seqno:	0
VLAD **(very long lived address; not key material)** • **remains unchanged through life of p.log** • **stable over a very long period of time**	...
< Prev:	CID (content ID)
Unlock:	WASM
Lock:	WASM
Op	update ("/pubkey; <pubkey>) delete ("/

- obviates the need for KERI pre-rotation



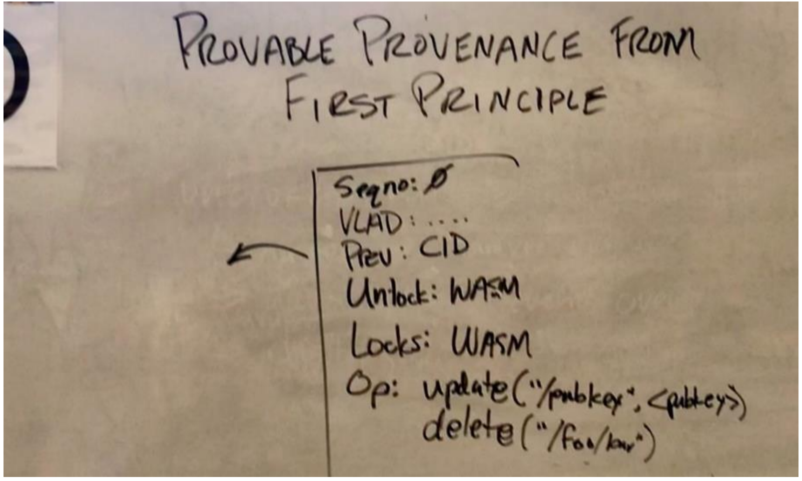
PROVABLE PROVENANCE FROM FIRST PRINCIPLE

Content addressing → independent storage → IPFS. S3 http
digital signatures → bound to actors → EdDSA Threshold sigs
self-describing data → Implementation independence → multiformat
Varuint [u8; N] → Varbytes
Stack machines → execution independence WASM



PROVABLE PROVENANCE FROM FIRST PRINCIPLE

unbroken chain of custody
↳ hashed for tamper evidence
↳ accumulation of events over time (f(t))
↳ digital signatures to bind control



PROVABLE PROVENANCE FROM FIRST PRINCIPLE

Seqno: Ø
VLAD: ....
Prev: CID
Unlock: WASM
Locks: WASM
Op: update("/pubkey", <pubkey>)
delete("/foo/bar")

Part 2 was continued after lunch in session 14D
https://docs.google.com/document/d/1F6zzOqkAunl9qIPEgo9dc1G_NskKt4RReDzS69nT0vI/edit

Identity Dynamic Modalities 0 to 1

Session Convener: Jeff Orgel
Session Notes Taker(s): Jeff Orgel

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

From @0 to @1 – Human Identity Extension Onto An Extra Worldly Realm

For decades I have witnessed and participated in the Human Experience (HX) of human presence being extended into a realm of 0's & 1's via connected systems.

These definitions apply to the following review.

***@0** - this refers to human experience before the natural world had connected & social technology systems.*

***@1** - this refers to human experience after the natural world had connected systems. This is the sun-rising of connected system technologies into daily life: when and how this arrives is very idiosyncratic to each individual.*

From @0 to @1 - Extension from Real World/Human eXperience (RW/HX) <u>ONTO</u> Digital Landscape (DL)

In the natural world (**@0**), people are designed to occupy a world of convergent forces: hot-cold, wet-dry, light-dark. The intellect in play exists in the sentient creatures – not one bit in the environment they exist in. Perfectly able and intelligent creatures are designed with capability responsive to the real-world sensor package they were born with. This sensor package allows them to discern what is happening around them. The better they could assess the challenge-scape of moment-to-moment circumstances, the more likely they would survive.

On the digital landscape (**@1**) the human animal occupies a realm of intellectual design where nothing (two words - NO THING) is naturally occurring. Everything (two words again – EVERY THING) is designed by intellect. Further it is designed by us. Who knows how to game us better than ourselves?! Who knows how to exploit human vulnerabilities of voyeurism, self-aggrandisement, sex, power, "free" and on it goes - better than us?! It shows…

The discordance occurring around this fact is extraordinary. Perfectly able and intelligent creatures from the physical world of **@0** are hobbled by not having a sensor package equivalents like smell, touch, gut intuition to discern what is happening around them in **@1**. The **@1** environment around them is immature, if not plain malicious, at being clear as to use of caution, implications of presence in such a framework and delivering trust.

This presentation was designed to put handles on thoughts with words regarding awareness of this interplay. It will also work towards identifying that people are trying to bridge these realms without clarity on the transitional, translational and symbiotic connections they will meet with in use of these systems.

The portion of human intellect which is occurring in people is unique for the above-mentioned reasons. I am calling that intellectual layer of understanding and management the HumanOSô.

Our Sessions covered ideas such as;

- Plato's Allegory of the Cave – what we see on the wall vs what the wall sees of us (AK)

- Bi-directional interplay between Real World & Digital Landscape

- Framework structure: visual models (linear vs. stack model)

- Understanding the idea of building a Digital Twin from awareness of the implications of those ***Real-IT*** ® relationships – ***the relationship we chose to have, or not have, with connected technology systems***. This profile was identified as a variation of a Voo Doo Doll we make of ourselves.

- Identifying the impact of ***Real-IT*** ® choices, and reflection into, a person's reality

- Concepts of managing system forces "in the room" including social media, data collection and predation such that a person's intention is manifested with minimum to no risk of hazard or harm.

- Explored: Can we exist without identifiable presence? Can we be present without existing? The phrase "being in a place" where there is no actual "place" (BC)

Examples of Connected Social Systems (CSS) would be; Social Networks like Facebook, TikTok, Instagram, WhatsApp; Legal Records like State & Federal: Tax Filing, Personal Property Tax, Real Estate Tax, License Bureau; Knowledge & Discovery (YouTube search, etc.)

Operation on the DL (Digital Landscape): Extension eXperience (EX) occurs @2 >< @3 >< @4 creating feedback from EX <u>INTO</u> Real World RW/HX

@2* - **Real-IT** ®: understanding the presence of the relationship with technology as a symbiotic aspect/element in daily life to one degree or another. @2 is the layer where RW (Real World) & DL (Digital Landscape) are ever iterating. This is a critical layer.

@3 - **YouDoo Doll** - here you craft your VooDoo Doll (aka You Do Dollä): crafting (more or less so) of S.A.M. (Same As Me) This is where Real-IT® awareness meets with a variation of the martial art Aikido on the Digital Landscape. I call this Real-ITdoä. This is the idea that we are managing forces we often aren't in control of, or even aware of.

@4 - **YouX**: How is the Real-IT Yin Yang going? UI & UX experience feedback back returns to HX/RW more or less aligned with your intended outcomes (hope, expectation, trust)? Assess and go to @2 and iterate.

Presenting the same session once each day (an ***IIW Triple Play***) allowed for the following significant benefits;

- maximum opportunity for attendees to attend with minimum session conflicts regarding other valued sessions

- scaffolding refinement each day which elevated the model for the next day's attendees

- likely 3X the number of attendees during the particular IIW event

- great for advancing the pace of developing evolving edge space models as there is evolution at a higher rate since each day-group contributes to a revision one day after the next. IIW.38 r1, IIW.38 r2 IIW.38 r3

Other Notes regarding a ***IIW Triple Play***;

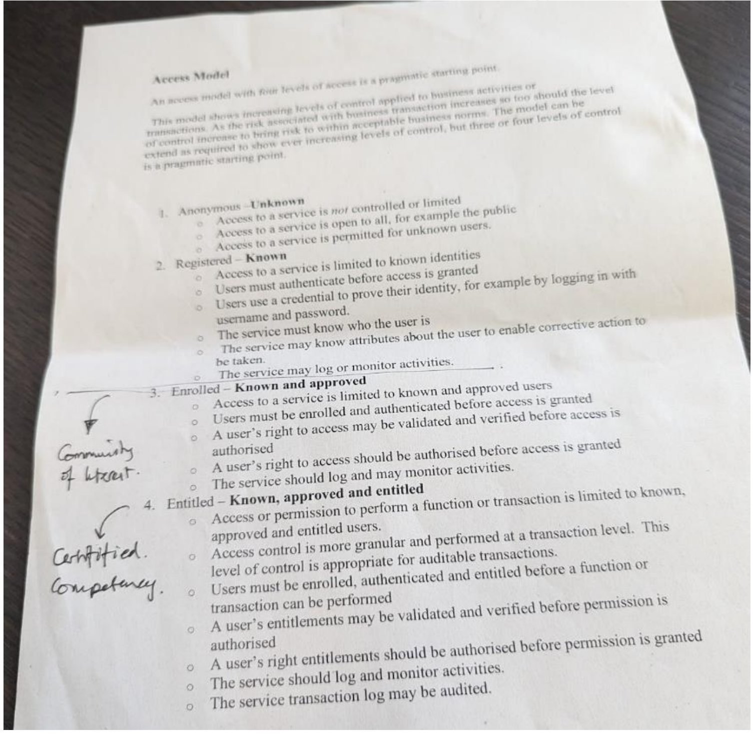
- calls for some presentation durability as it is an effort in triplicate

- reduces opportunities to attend one other session each day

Access / Auth 2 Assurance NIST 800-63D

Session Convener: Robert Lapes
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:



Access Model

An access model with four levels of access is a pragmatic starting point.

This model shows increasing levels of control applied to business activities or transactions. As the risk associated with business transaction increases so too should the level of control increase to bring risk to within acceptable business norms. The model can be extend as required to show ever increasing levels of control, but three or four levels of control is a pragmatic starting point.

1. Anonymous – **Unknown**
   - Access to a service is *not* controlled or limited
   - Access to a service is open to all, for example the public
   - Access to a service is permitted for unknown users.
2. Registered – **Known**
   - Access to a service is limited to known identities
   - Users must authenticate before access is granted
   - Users use a credential to prove their identity, for example by logging in with username and password.
   - The service must know who the user is
   - The service may know attributes about the user to enable corrective action to be taken.
   - The service may log or monitor activities.
3. Enrolled – **Known and approved**
   - Access to a service is limited to known and approved users
   - Users must be enrolled and authenticated before access is granted
   - A user's right to access may be validated and verified before access is authorised
   - A user's right to access should be authorised before access is granted
   - The service should log and may monitor activities.
4. Entitled – **Known, approved and entitled**
   - Access or permission to perform a function or transaction is limited to known, approved and entitled users.
   - Access control is more granular and performed at a transaction level. This level of control is appropriate for auditable transactions.
   - Users must be enrolled, authenticated and entitled before a function or transaction can be performed
   - A user's entitlements may be validated and verified before permission is authorised
   - A user's right entitlements should be authorised before permission is granted
   - The service should log and monitor activities.
   - The service transaction log may be audited.

Community of Interest.

Certified. Competency.

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

Participants discussed the challenges of Access Management and how it might be codified into high-level requirements for Access Assurance good practice similar to the NIST 800-63 series.

Discussion opened with a round table of general concerns, for Access Assurance and the difficulties in building consensus on ontology, taxonomy, and semantic references for access control.

A strawman four-level access assurance model was presented, and discussed as a potential starting point for further discussions (see image below).

1. Anonymous: Unknown
2. Registered: Known
3. Enrolled: Known and Approved
4. Entitled: Known, Approved, and Entitled.

The group concluded that, despite initial issues in terminology, the Access Assurance model was a good starting point, for further discussions and as a guide for high level strategic guidance and requirements decomposition, and definition.

Accountable Wallets / A wallet can prove a wallet's legitimacy using VC and ZKP

Session Convener: Masato Yamanaka
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

Here is the slide deck I used.
Accountable Wallet for presentation for IIW.pdf

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

Personal Data Store Faceoff

Session Convener: Aaron Coburn, https://www.linkedin.com/in/aaron-coburn-a274334/
Session Notes Taker(s): Michael Becker

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

Purpose of the talk: Explore different technical implementations of personal data stores.

"Personal data store (PDS) - where do I put my information as a person without a third party involved?"

PDS is similar to but different from a digital well and/or personal information management system.

Conversation keyed off of [Decentralized Web Node Companion Guide]https://identity.foundation/decentralized-web-node/guide/v0.0.1/), team looking to add and expand on this effort.

## PDS Reviewed

### SOLID | https://solidproject.org/
- separate applications from data
- multiple pods
- requires interoperability
- three elements: identity layer (agents), web (http), data has global semantics (RDF)
- Linked Data
- URI for data mapping

### Decentralized Web Node (DWN) (Concept coined by Daniel Buchner)
- Data interaction layer owned by you
- consent of protocols (multi-master source of truth, not single source of truth), apps that control data relationship and data hierarchy (JSON definition)
- Authorization and grades
- Google hosting DWN for providers; don't need an external server.
- DID Based
- Been implemented by TBD
- "You need data to be highly available"
### UBOS (Johannes)
- https://ubos.net/docs/architecture/
- 1) Manage existing apps useful for personal data management e.g. Nextcloud, Mastodon
- 2) plus middleware including Graph database for new kinds of applications
- Semantic model strongly enforced
- Importers
- PeerTalk

### Data Spaces (Wallet-attached storage)
- Wallet attached storage, MIT digital credentials program
- Use case: I have a wallet, I need to share it in cloud storage that could be under my control
- Need basic read/write protocol, series of nouns of objects (objects, collections (RTBMs, graph)--JSON, a file)and operations (verbs: read, write, copy, append, get metadata)
- Rest binding: get put
- JSON-RPC binding
- DIDCOMM 2
- Uses ID: DIDs
- Mastadon actor IDS
- Authorization; server-side access control (ACL) _ Capabilities (e.g., expiration, editor roles, etc.)
- Storage, sync, encryption

## Verida | https://www.verida.network/
- ZKPs with polygon.id
- decentralized personal data store
- offer a token-based PDS network
- verifiable credential parter with cheqd
- has DAO LLC foundation to manage token distribution
- Looking for decentralized AI stack partners

## Other
- We also need to address and cover, GNAP, delegated authorization to storage
- role of LLMs discussed
- How will this roll out? In three ways/stage,
    - embedded
    - partnering for specific solutions
    - open standard that support interoperability

Five Failed Blockchains - Why Trade Needs Protocols, Not Platforms

Session Convener: Timothy Ruff
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

Multifactor Fusion in a Verifiable Credential

Session Convener: Francisco Corella
Session Notes Taker(s): Francisco Corella

Tags / links to resources / technology discussed, related to this session:

- Completed and substantially revised presentation
- Original presentation

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

Tokens, Tokens Everywhere

Session Convener: George Fletcher
Session Notes Taker(s):

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

(starting to take notes at 11:48 AM)

- (Mike Schwartz) …
- (George) How do we help API developers understand the security implications of the choices they make around their API decisions. Are there ways in which we can cross-pollinate across the spaces
- (Dean) How do we build trustworthy libraries so that they don't have to build everything from the ground up
- (Justin) This all comes back to where do the abstractions lie. Libraries and SDKs are great ways to codify abstractions. Those need to be defined systematically. Every time we draw boundaries, we are making a decision about the nature of it. We tend to be sloppy about this typically.
- (Atul) SGNL will be releasing an open source library and server for Transaction Tokens
- (George) There are a couple of use cases
    a. Client needs to do something (e.g. a messaging app needs to add a user to a group)
- (George) There are two issues you run into: When the request comes into the network, and we're trying to add a user to the token group The API gateway validates it, is it possible for the gateway to convert it into an internal format token, so that it can call the internal workloads with that token. The internal transaction token can say that the scope is now "add user to group". There's value to defining a token format that is internal to your system because the access token may have way more scope than what is required for the transaction. In OAuth speak it's downscoping
    a. (Justin) It could just be translation, not downscoping.
    b. (George) agreed
- (George) The client could be in a separate authz domain and the internal domain is a different domain.
- (George) You can put authorization details in the Transaction Token (TraT), e.g. "I'd like to put Justin in the group) and there can be request context.
- (Mike Schwartz) Is there any relation with RAR?
- (George) We're at v1 of the spe, so please contribute
- (Omri) Is there a way to tie together the inbound token to the TraT?
- (George) The TraT has the requesting workload in it
- (George) If an intermediate service wants to get a replacement transaction token, the intermediate service's identity gets added to the requesting workload ids.
- (George) We don't have the full path tracking, but if we need that we need to define a new mechanism

- (George) Another interesting use case is that something internal generates the transaction token request. For example, inbound email server. Since it doesn't have an inbound access token, how does it get a TraT
- (Dean) Changing the subject identifier in a replacement TraT…
- (George) You could stick the new subject identifier in the authorization details
- (George) There's another esoteric use case: If the client is a mobile app, and it has an access token that gives it access to a subset of the internal workloads, but you need to access a new workload that was not anticipated, then the external access token is going to fail
- (Justin) token buckets
- (Justin) One of the things that kept coming up is that there is way more than an access token when you deploy all this. That always came with some caveat about how that access token can be interpreted internally. People were talking about doing exchange
- (Justin) But can we define a data structure that has the Access Token with some attributes, and a Transaction Token with some attributes and another Transaction Token associated with that, we could have something that is cryptographically bound with selectivity
- (Justin) what you end up with is a very Merkel tree type system. I should be able to add a signature to each of node of the tree, and it should apply to everything above the node in the tree
- (Justin) If you start sending all these tokens around, it starts inflate
- (Justin) So we need a way to carry multiple attested object as we carry them through a system
- (Omri) So is this a new header?
- (Justin) I've tried to do it as a structured header, but it failed. It needs to be a cohesive structure, which is a graph object.
- (Justin) In my implementation, each node has a hash of its parent, and is signed. There is no other linkage than the hash
- (George) This is all super nascent and would love to get your involvement. You can find all this in the OAuth GitHub repository and the OAuth mailing list.
- (George) Cross domain thing
- (George) Client makes a request, which reaches WL2 in TD1 and then it needs to go to WL4 in TD2
- (Justin) For example TD1 is AWS and TD2 is Google Cloud
- (George) So what the ID-Chaining spec describes is two ways in which WL2 can obtain a token to be able to access WL4
- (George) One way is for WL2 to talk directly to the AS in TD2, and the other is for WL2 to go to its own AS and that contacts the AS in TD2
- (George) There are some idiosyncrasies with the Token Exchange spec, so we are trying to figure out if that is the right thing to use.
- (Dean) Can you cover asynchronous workloads? Say WL4 takes a very long time, how does it return something back to WL2 later
- (George) We haven't tried to specify the network reachability piece. The other part is how you express …
- (Atul) Use Shared Signals
- (Justin) There's another way such as…Oscoe / Kafka, especially as we go cross-domain

- (Dean) I'd like to seed this discussion with Phil Hunt's draft on SCIM Events. it defines an asynchronous mechanism
- (Atul) SCIM Events latest draft may have removed the transport part
- (Justin) Proof of possession throws all this into a weird place. The Access Token PoP is designed to be bound to the client. Once it is not the client anymore, our usual notion of :"which party is allowed to present this" goes out of the window. We've described the workload, and the transaction, but we don't have a way to connect it together
- (George) There are a couple of key things: TraTs are designed to be bearer tokens for performance reasons. You could do a couple of level of authorization at the WL level. "Am I allowed to receive transactions initiated by a specific workload"? And then "Am I allowed to get something with this purpose from this workload"?
- (George) Maybe you don't get full sender constraining, but you could get something limited pathing mechanism
- (Justin) Just to add to that, (adding to the graph of token buckets) when WL1 hits this, it signs the token bucket itself. and you could chain such claims
- (Justin) The other thing, which is total strawman, is that if we had something that was a node in this graph that determined the path ahead of time, and attached itself to it, and it was signed by the TTS
- (Atul) We had tried to cover this in the TraT draft using nested tokens, but we didn't find many use cases, so we pulled it out and postponed working on it.

Authentic AI

Session Convener: Wenjing Chu
Session Notes Taker(s): Wenjing Chu and Anonymous (sorry I didn't know who but thanks! The extra notes are after the subtitle "Additional notes")

Tags / links to resources / technology discussed, related to this session:

The AIM Task Force is currently working on a specification of how to best build new technology blocks for the challenge of achieving authenticity to AI generated content and trust on AI agents and decision making. The Task Force meets on Thursday morning:

- https://wiki.trustoverip.org/pages/viewpage.action?pageId=19657312
- https://wiki.trustoverip.org/display/HOME/2022-07-07+AIM+TF+Meeting+Notes
- https://wiki.trustoverip.org/display/HOME/Calendar+of+ToIP+Meetings

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

The AIM Task Force is looking into integrating TSP (Trust Spanning Protocol) and C2PA (including the related creator identity assertion working group) to offer best authenticity guarantees to many aspect of AI adoption. See the info about the AIM Task force above. There is a separate org of The **Coalition** for **Content** Provenance and Authenticity (**C2PA**) and creator's identity assertion working group: https://creator-assertions.github.io/identity/1.0-draft/.

To participate in this line of work, welcome to the AIM Task Force in ToIP:
https://wiki.trustoverip.org/display/HOME/2022-07-07+AIM+TF+Meeting+Notes

Check out current draft proposal and a list of use cases:
https://docs.google.com/document/d/1Snga-dkUG0XaLaXx1q9FKojaFy42CTZhvyFJbo9KgLU/edit

We welcome new use cases and otherwise participate in our meetings and work on the spec.

-Additional notes of the discussions:
Provenance
Transparency

What is missing:
distribution
no good control of people manipulate content after
invitation to join the task force meeting

Task force use cases (two are described here)

Use Case#1: For creator to make assertion
assert sender authenticity
content authenticity
tracking the tool used, metadata around the content

Use Case#2: AI Agent
a set of AI tools to handle user’s wishes and
combine C2PA and

====== START transcription with OpenAI Whisper and summarization with Perplexity ========
The main topic of the transcript revolves around the use of Authentic AI with C2PA (Coalition for Content Provenance and Authenticity) and other TrustOverIP technologies to enhance the transparency and accountability of digital content. Here are the key points discussed in the transcript:

1. **Purpose of C2PA**: The transcript outlines the role of C2PA in providing a history of digital content creation and editing, likening it to a supply chain for digital media. This helps in establishing trust in the final product by tracing its origins and modifications[1].
2. **Accountability and Transparency**: It emphasizes the importance of accountability and transparency in AI, particularly in high-energy information like videos and film-quality content. The future implications for metaverse streaming models are also mentioned, highlighting the need for a robust system to manage this information[1].
3. **Distribution Challenges**: The transcript discusses the challenges in the distribution of edited content, particularly how it can be manipulated once it leaves the original creator's control. This section underscores the need for mechanisms that ensure the authenticity of content as it is shared across platforms[1].
4. **Authentic Communication**: The concept of authentic communication is introduced, where data creators embed authenticity metadata into their content. This metadata can help verify the creator, the editor, and the chain of custody of the content as it is distributed[1].
5. **Role of AI in Provenance**: AI's role is highlighted in automating the process of entering data about content creation and editing, which could otherwise be challenging for humans to perform consistently[1].
6. **C2PA's Broader Impact**: The transcript mentions C2PA's impact on various stakeholders, including journalists and news organizations, by providing a technical standard for proving the authenticity of digital content. This is crucial for combating misinformation, especially in sensitive areas like election information[1].
7. **Invitation to Participate**: The speaker invites listeners to join bi-weekly meetings to discuss these topics further, indicating an ongoing effort to refine and promote these technologies[1].

Overall, the transcript focuses on how technologies like C2PA can be used to ensure the authenticity and provenance of digital content, which is increasingly important in a world where AI-generated content is becoming more common.

Citations: [1] https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/1617151/768aff4b-ead8-4ccd-b44b-834699fcced1/Authentic AI (Apr 18 11.37.02).txt [2] https://www.registrar.psu.edu/transcripts/transcript-keys/index.cfm [3] https://www.techrepublic.com/article/ai-cryptography-watermarking/ [4] https://www.lanecc.edu/administration/enrollment-services/interpret-your-transcript [5] https://c2pa.org/specifications/specifications/1.3/explainer/_attachments/Explainer.pdf [6] https://www.thesslstore.com/blog/real-photo-vs-ai-generated-art-a-new-standard-c2pa-uses-pki-

to-show-an-images-history/ [7] https://registrar.illinois.edu/transcript-key/ [8] https://www.technologyreview.com/2023/07/31/1076965/the-race-to-find-a-better-way-to-label-ai/ [9] https://readwrite.com/c2pa-unveils-content-credentials-icon/ [10] https://c2pa.org/post/contentcredentials/ [11] https://c2pa.org/post/release_1_pr/ [12] https://c2pa.org [13] https://www.rochester.edu/registrar/assets/pdf/TranscriptKey.pdf [14] https://c2pa.org/specifications/specifications/1.3/ai-ml/ai_ml.html [15] https://srfs.upenn.edu/student-records/transcript-key [16] https://registrar.utah.edu/transcripts/transcript-key.php [17] https://registrar.vanderbilt.edu/transcripts/transcript-key.php [18] https://www.wm.edu/offices/registrar/studentsandalumni/studentrecords/transcripts/transkey/ [19] https://www.forbes.com/sites/rashishrivastava/2023/10/27/content-credentials-that-label-ai-generated-images-are-coming-to-mobile-phones-and-cameras/?sh=6f6a685f208c [20] https://www.linkedin.com/pulse/c2pa-digital-watermarks-powerful-combination-content-creators-imwbe

====== End transcription with OpenAI Whisper and summarization with Perplexity ========

Session #14

DBSC - Device Bound Session Credentials

Session Convener: Sam Goto, Arnar Birgisson, Kristian Monsen, Sameera Gajjarapu
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

Explainer: https://github.com/WICG/dbsc/blob/main/README.md
Chromium blog post: https://blog.chromium.org/2024/04/fighting-cookie-theft-using-device.html

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

Summary:

Device Bound Session Credential is a proposal for browser-based session management based on private keys instead of bearer tokens. It focuses on explicit session/key management by the website, and "retrofittability" with existing web apps and stacks.

The key point of DBSC is that periodic proofs of possession are presented only on a dedicated endpoint and don't require modification or rewrites of existing endpoints. The browser, under instructions from the server, ensures such proofs are delivered to that endpoint on time and that regular requests to other endpoints are "queued" until that session management endpoint signals that the proof has been validated.

That signalling initially takes the form of a short-lived cookie. Regular endpoints can simply continue to expect that cookie to be present for the request to be authenticated. That cookie is still a bearer token, but can have validity in the minutes. This, plus using OS provided facilities to ensure the session private key is resistant to malware exfiltration, forces malware to either carry out its abuse locally on the device, or to go after sign-in credentials instead of session credentials. Both make malware more detectable and subject to other cleanup and mitigations.

(DBSC authors use the term "sign-in credential" to refer to credentials that require user interactivity, such as passwords, WebAuthn/FIDO credentials (passkeys), magic links in emails, etc.; while "session credentials" refer to credentials used to authenticate requests made in e.g. a "signed in" state without user interaction, such as cookies, OAuth refresh and access tokens, etc.)

Meeting discussions:

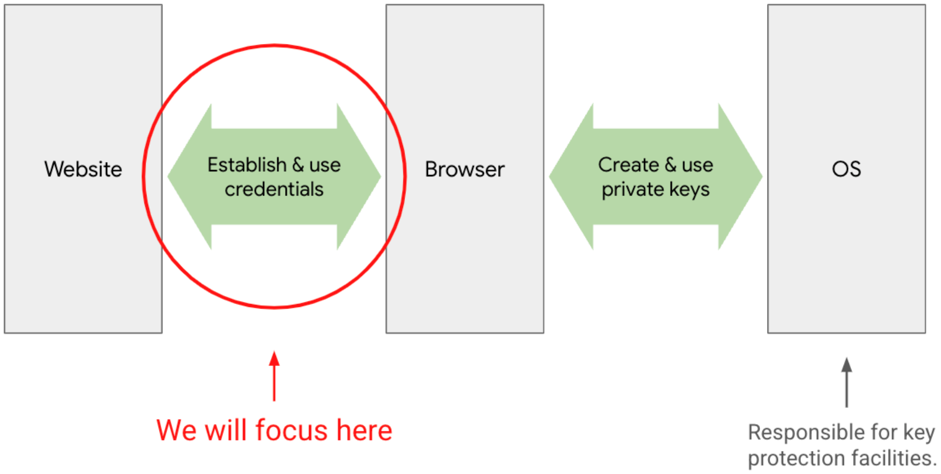
Presented overview of DBSC, discussion focused on clarifications. See key slides below for some of the answers and points clarified.

Discussed provenance of the private key, and reported on collaboration between Microsoft and Google, integrating ideas from BPoP and DBSC. TL;DR: In enterprise managed contexts, DBSC can support using keys with additional context or provenance verification, provided at sign-in time (which is managed outside DBSC)

Justin Richer provided advice to engage with IETF and the http WG, as DBSC is based primarily on new HTTP headers.

A rewrite of existing spec is requested, with the specifics of key generation and management and enterprise managed contexts, and/or integration with OAuth flows.

Key slides:



Website

Establish & use credentials

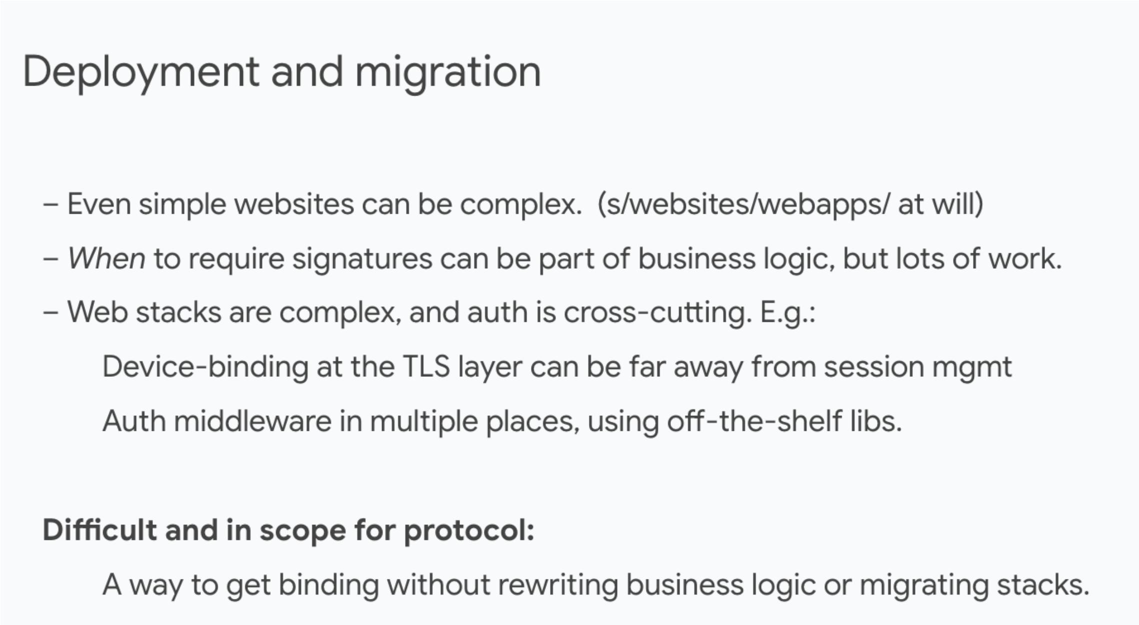
Browser

Create & use private keys

OS

We will focus here

Responsible for key protection facilities.



Deployment and migration

– Even simple websites can be complex. (s/websites/webapps/ at will)

– *When* to require signatures can be part of business logic, but lots of work.

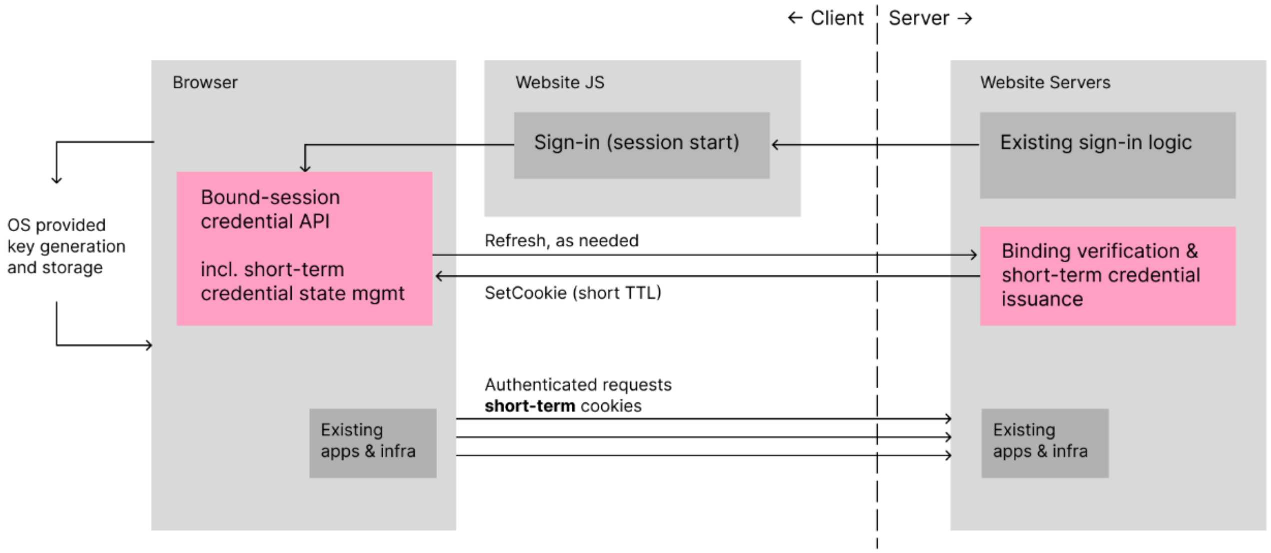
– Web stacks are complex, and auth is cross-cutting. E.g.:

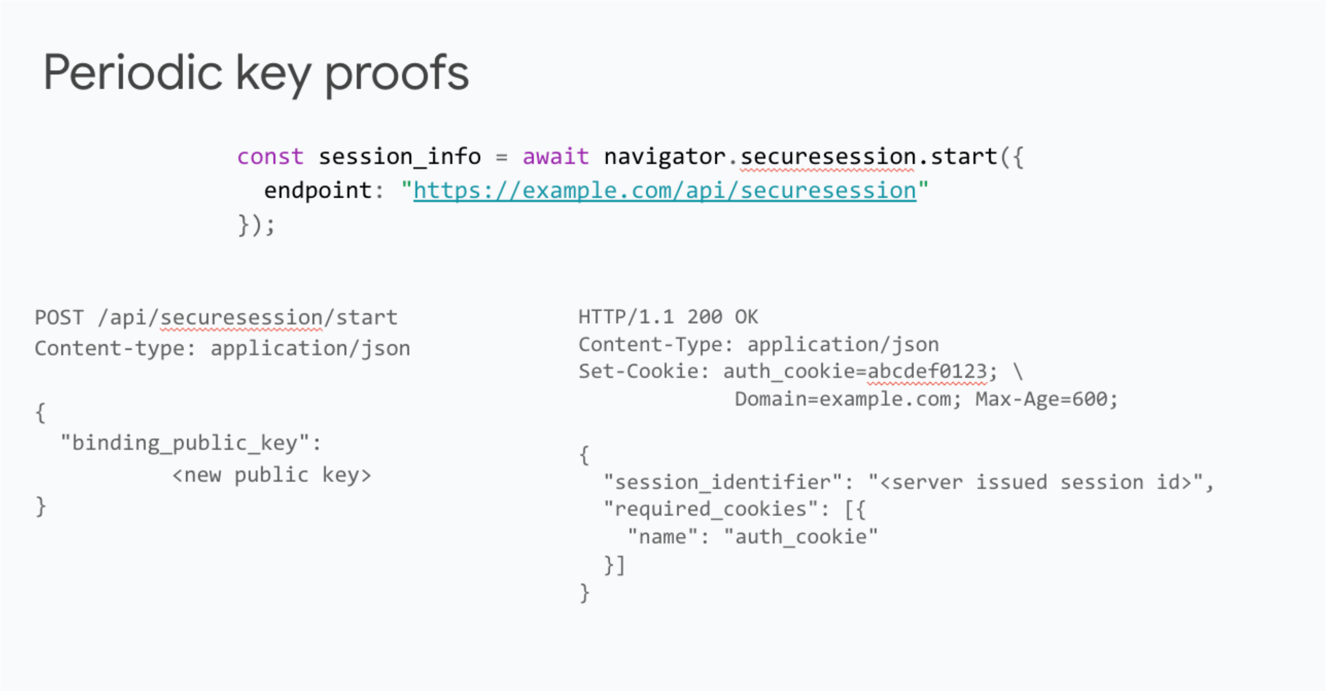
Device-binding at the TLS layer can be far away from session mgmt

Auth middleware in multiple places, using off-the-shelf libs.

Difficult and in scope for protocol:

A way to get binding without rewriting business logic or migrating stacks.


← Client
Server →
Browser
Website JS
Website Servers
Sign-in (session start)
Existing sign-in logic
OS provided key generation and storage
Bound-session credential API
incl. short-term credential state mgmt
Refresh, as needed
SetCookie (short TTL)
Binding verification & short-term credential issuance
Authenticated requests **short-term** cookies
Existing apps & infra
Existing apps & infra

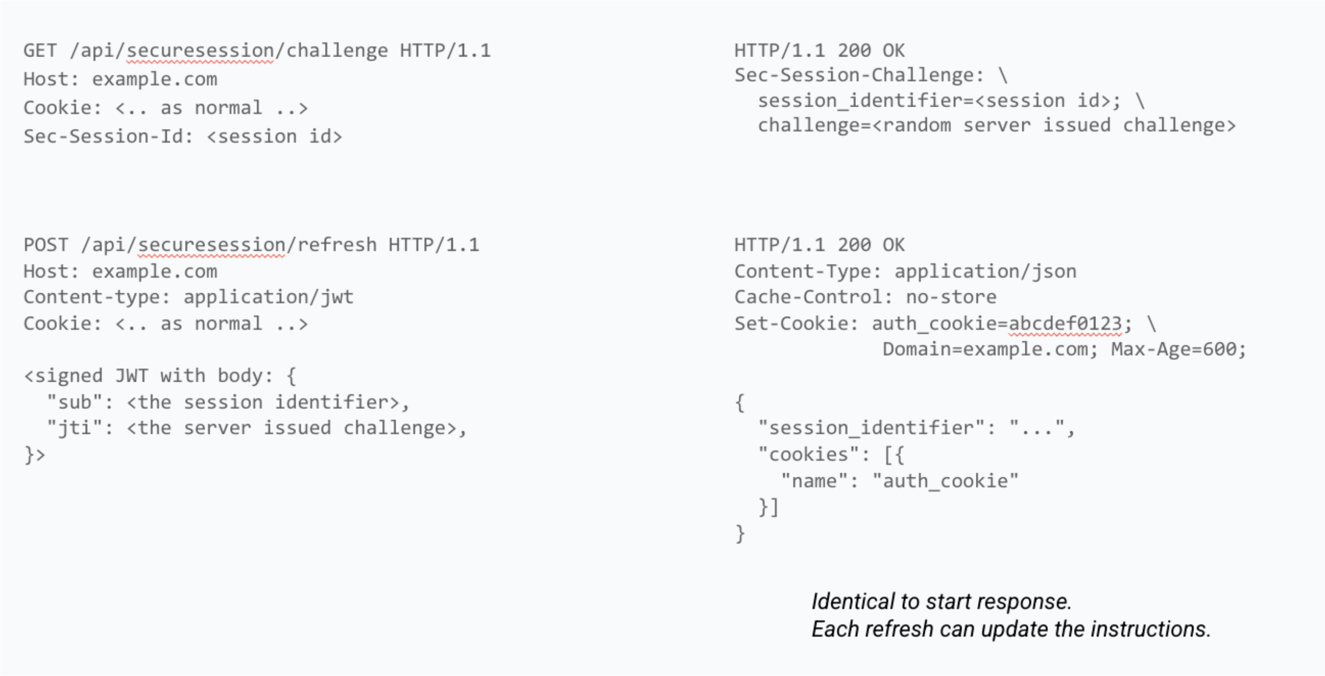


Periodic key proofs

```
const session_info = await navigator.securesession.start({
  endpoint: "https://example.com/api/securesession"
});
```

```
POST /api/securesession/start
Content-type: application/json

{
  "binding_public_key":
           <new public key>
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Set-Cookie: auth_cookie=abcdef0123; \
             Domain=example.com; Max-Age=600;

{
  "session_identifier": "<server issued session id>",
  "required_cookies": [{
    "name": "auth_cookie"
  }]
}
```



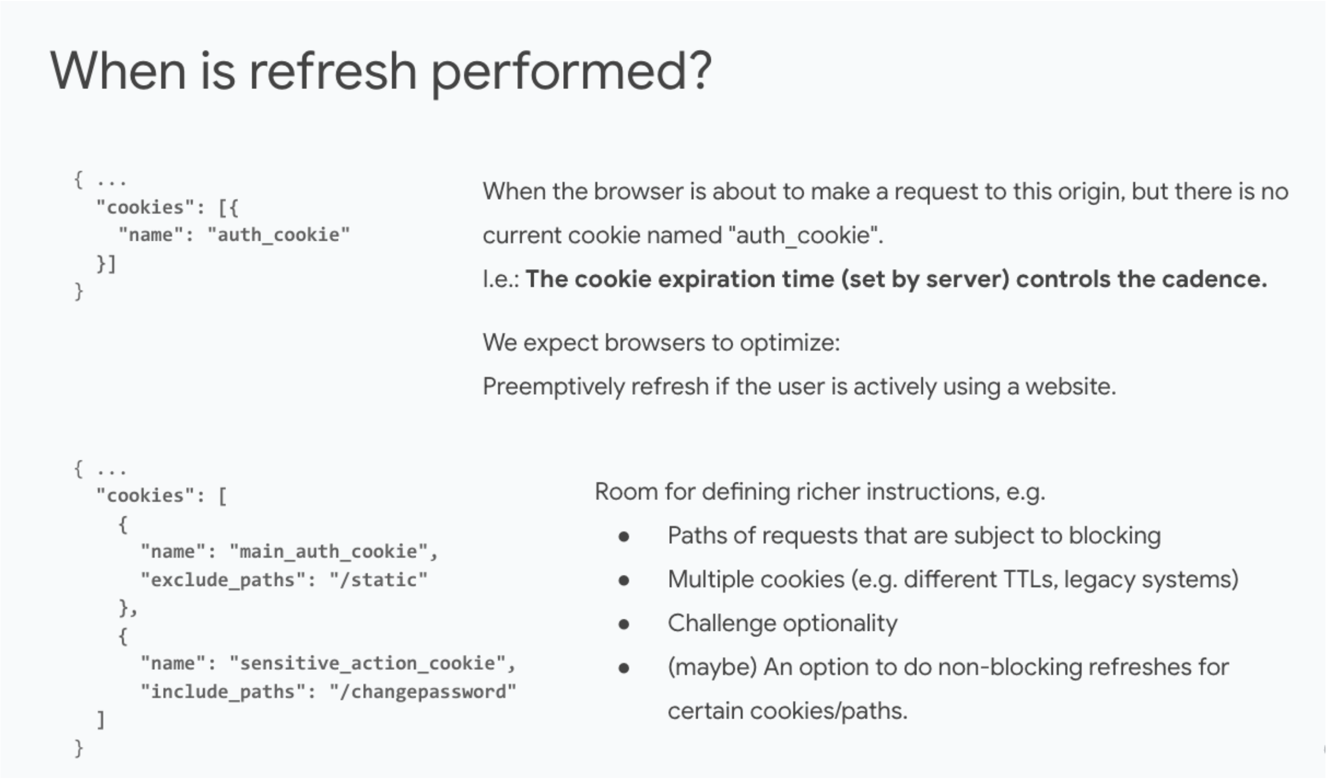
```
GET /api/securesession/challenge HTTP/1.1
Host: example.com
Cookie: <.. as normal ..>
Sec-Session-Id: <session id>
```

```
HTTP/1.1 200 OK
Sec-Session-Challenge: \
  session_identifier=<session id>; \
  challenge=<random server issued challenge>
```

```
POST /api/securesession/refresh HTTP/1.1
Host: example.com
Content-type: application/jwt
Cookie: <.. as normal ..>

<signed JWT with body: {
  "sub": <the session identifier>,
  "jti": <the server issued challenge>,
}>
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
Set-Cookie: auth_cookie=abcdef0123; \
             Domain=example.com; Max-Age=600;

{
  "session_identifier": "...",
  "cookies": [{
    "name": "auth_cookie"
  }]
}
```

Identical to start response.
Each refresh can update the instructions.



When is refresh performed?

```
{ ...
  "cookies": [{
    "name": "auth_cookie"
  }]
}
```

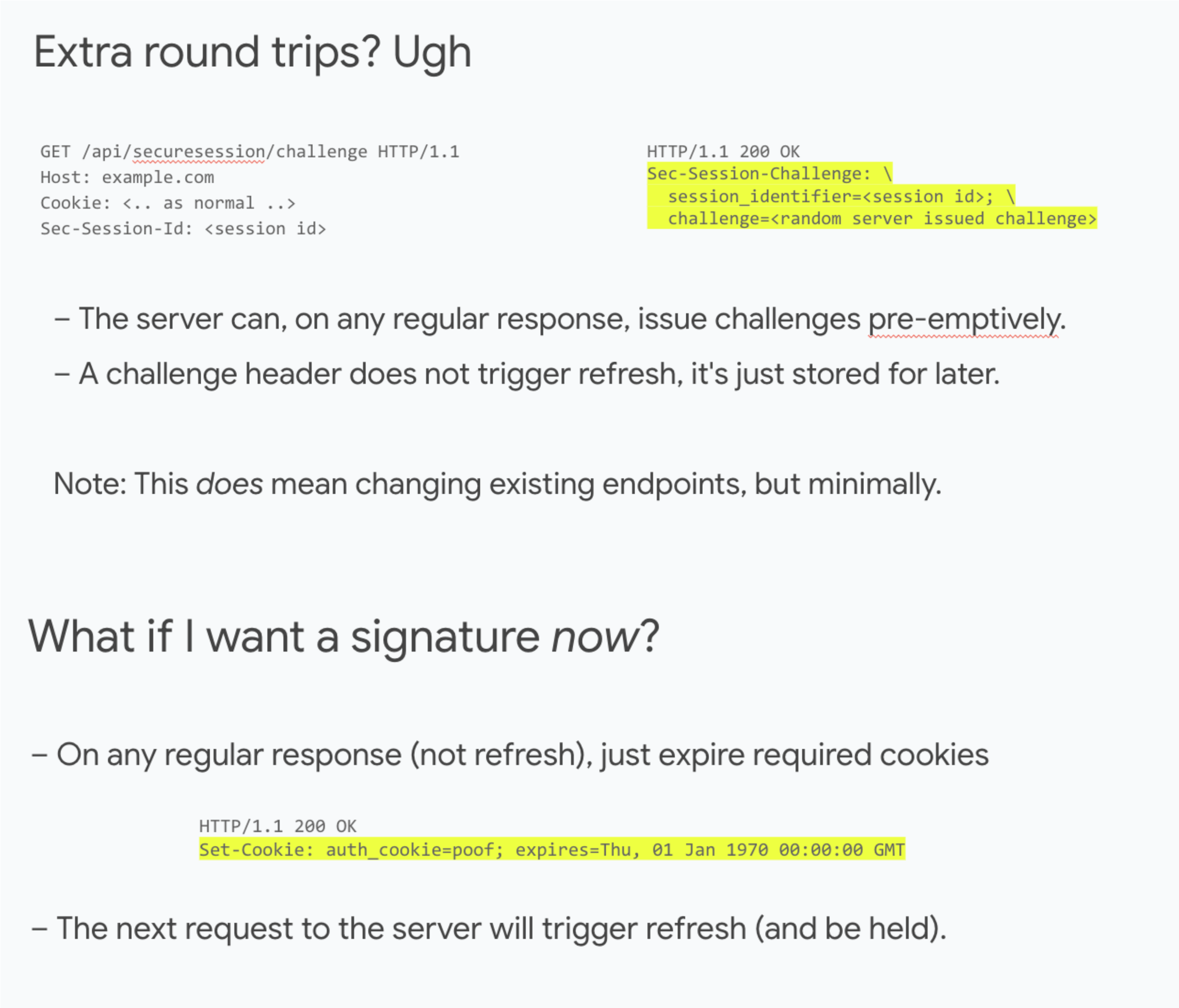
When the browser is about to make a request to this origin, but there is no current cookie named "auth_cookie".
I.e.: **The cookie expiration time (set by server) controls the cadence.**

We expect browsers to optimize:
Preemptively refresh if the user is actively using a website.

```
{ ...
  "cookies": [
    {
      "name": "main_auth_cookie",
      "exclude_paths": "/static"
    },
    {
      "name": "sensitive_action_cookie",
      "include_paths": "/changepassword"
  ]
}
```

Room for defining richer instructions, e.g.

- Paths of requests that are subject to blocking
- Multiple cookies (e.g. different TTLs, legacy systems)
- Challenge optionality
- (maybe) An option to do non-blocking refreshes for certain cookies/paths.



Extra round trips? Ugh

```
GET /api/securesession/challenge HTTP/1.1
Host: example.com
Cookie: <.. as normal ..>
Sec-Session-Id: <session id>
```

```
HTTP/1.1 200 OK
Sec-Session-Challenge: \
  session_identifier=<session id>; \
  challenge=<random server issued challenge>
```

- The server can, on any regular response, issue challenges pre-emptively.
- A challenge header does not trigger refresh, it's just stored for later.

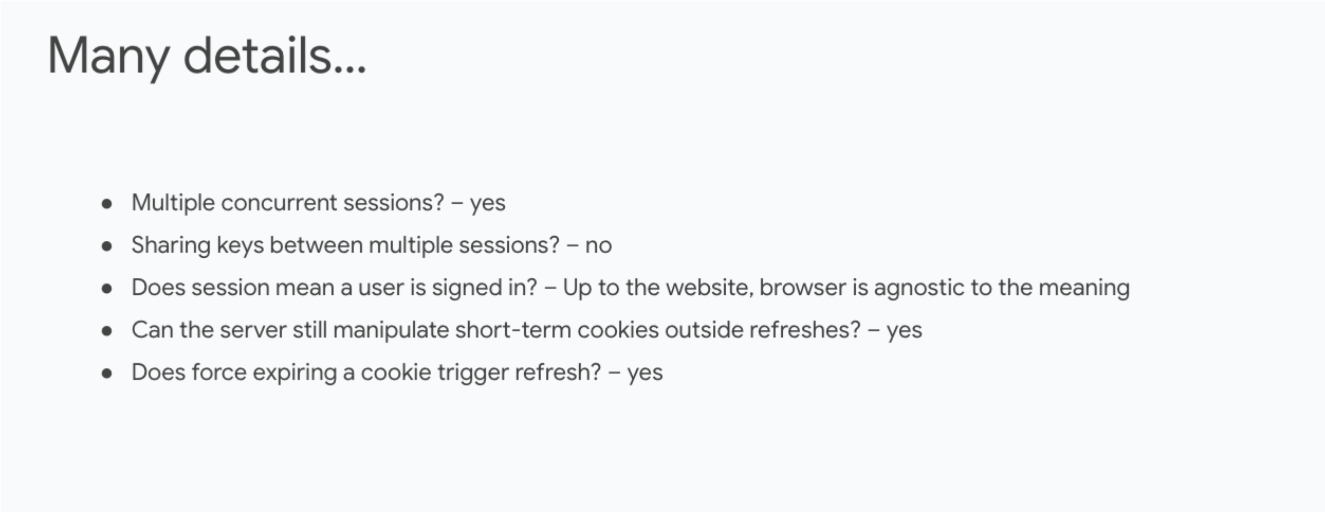
Note: This *does* mean changing existing endpoints, but minimally.

What if I want a signature *now*?

- On any regular response (not refresh), just expire required cookies

```
HTTP/1.1 200 OK
Set-Cookie: auth_cookie=poof; expires=Thu, 01 Jan 1970 00:00:00 GMT
```

- The next request to the server will trigger refresh (and be held).



Many details...

- Multiple concurrent sessions? – yes
- Sharing keys between multiple sessions? – no
- Does session mean a user is signed in? – Up to the website, browser is agnostic to the meaning
- Can the server still manipulate short-term cookies outside refreshes? – yes
- Does force expiring a cookie trigger refresh? – yes

Cardano transactions and KERI

Session Convener: Ed Eykholt
Session Notes Taker(s):

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

Subtitle: Can a Cardano transaction be effected based on KERI AID?

- User Story: As a Cardano dApp developer and KERI Advocate, I want to implement smart contract interactions with the Cardano chain that requires transaction interactions, such as spending of Ada, based on signing by the current key-pair of a KERI AID.
- Success Criteria:
  - The current KEL of the AID in question is on-chain in a canonical location, can be readily found publicly, and consumed by any Plutus script.
- Ideas:
  - Can we avoid having centralized oracles downstream of KERI witnesses, so that one of an AID's witness's itself can write to Cardano?
    - Can we leverage a design approach similar to KERI Health demo this morning, creating an AID and then adding a Witness (i.e., Cardano Backer) with a Rotation event? Not essential
      - Maybe not. Transactions can have datum, however, Plutus scripts cannot read datum from another transaction?
      - Would need a Reference Input that represents a Key Event, and that Reference Input
      - How do oracles and smart contracts work today, where the smart contract redemption script can reliably access a state from the oracle?
      - In Cardano, the "address" is the pointer to the script, which specifies
  - Can we create a Cardano asset or NFT, one per AID, which can accumulate metadata equivalent to the KEL (or a single Key Event) contents?
    - If not, is there another equivalent to create an append-only log sequence of transactions?
  - How is a redemption script constructed offline by a dApp?
    - What indexing of the blockchain might be essential or helpful?
  - Can a validator of transaction (redemption script), without indexing, prove the AID's current KeyState and thus the validity of the script's signer?
    - Can a plutus script know the last AID key state update is truly the most recent key rotation? Does this imply that the validation of the script must know whether the referenced transaction is still a UTXO.
  - What other essential questions or requirements exist to implement the above user story?
  - Must or should the Ada signing key and the AID's current signing key be distinct? Why?

-
- Other Ideas:
    - A Plutus reference script can help with the AID lookup, KEL validation, and confirming the current signing criteria (e.g. the current public key).
    - Plutus redemption script includes reference to the tip of a KEL in the on-chain output of a KERI Super-Watcher/Backer?
    - What if Establishment Events were *initiated* from Cardano transactions? How might that be more useful?
    - What CIPs might be needed to draw further collaboration?

Notes:

Interesting points on Cardano & KERI:

KERI differs from DID methods in how it handles key management using key event logs (KELs). It provides an unbounded-term identifier that can have key rotation and retain the same identifier using this hash-chained linked data structure (the KEL). KERI is independent from Cardano and doesn't require a blockchain.

Cardano is an extended UTXO blockchain - more similar to Bitcoin than Ethereum.

Cardano's contracts differ from Ethereum - most of the code is off-chain with a very simple **redeemer script** on-chain.

Contract:

The approval of the contract is arbitrary to this discussion - the contract could require whatever signatures are necessary for its use case.

The use case is that to spend from this script, you have to prove you are the controller of an AID. An oracle may provide the KEL/state of an AID to the script. It could be multi-sig, enable DeFi with SSI, etc.

An example might be a legal entity-bound contract that requires a KERI AID to spend funds from a contract (fight money laundering, proper bookworking etc). AIDs can develop trust and reputation because it's an unbounded term identifier, whereas a simple Cardano address cannot (no key rotation).

The Plutus script must be able to find a way to the KEL.

Avoiding oracles:

A centralised oracle isn't trusted, so can we find a solution that does not require one. **Reference inputs** may allow us to have a trustless solution if the datums in another script will have the final key state for a given identifier (so a KERI rotation contract).

Using oracles:

In general, how oracles work today (using reference inputs?) could be repurposed to bring KELs from a witness network on-chain in a similar manner to a watcher.

Provenance From First Principles Part 2

Session Convener: Dave Grantham | https://www.linkedin.com/in/david-grantham-87207a265/
Session Notes Taker(s): Cam Geer | https://www.linkedin.com/in/camgeer

Tags / links to resources / technology discussed, related to this session:

- Cryptid Provenance Specification | https://github.com/cryptidtech/provenance-specifications
- Cryptid GitHub | https://github.com/cryptidtech/
- Hyperledger / Open Wallet Foundation | https://github.com/hyperledger/anoncreds-v2-rs
- Cryptid | Unified Theory of Decentralization | https://www.cryptid.tech/post/a-unified-theory-of-decentralization

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

content addressing > independent storage >> IPFS | S3 buckets | http://domain/[hash]
digital signature > bound to actors > ECDSA Threshold M of N
self-describing data . implementation independence | multiformats

- variant [u8; N] > varbytes

stack machines > execution independence | WASM

WASM (Web Assembly)

- bottom half of Javascript Gecko spec to enable portability across systems and devices
- an execution environment | doesn't know how to do anything

Theme

- max decentralization

Web Assembly Cryptographic Constructs (WACC)

- check sig
- check

Provenance

- unbroken chain of custody
  - hashed for tamper evidence
  - accumulation of events overtime (f(t))
    - blockchain useful only for immutable ordering of events (time)
- digital signatures to bind control

Identity is not anything you have or control

- accumulation of data over a course of time
- "key history" in any content / as it exeist in

XZ - opportunity for industry to better fun maintainers and have threshold signing

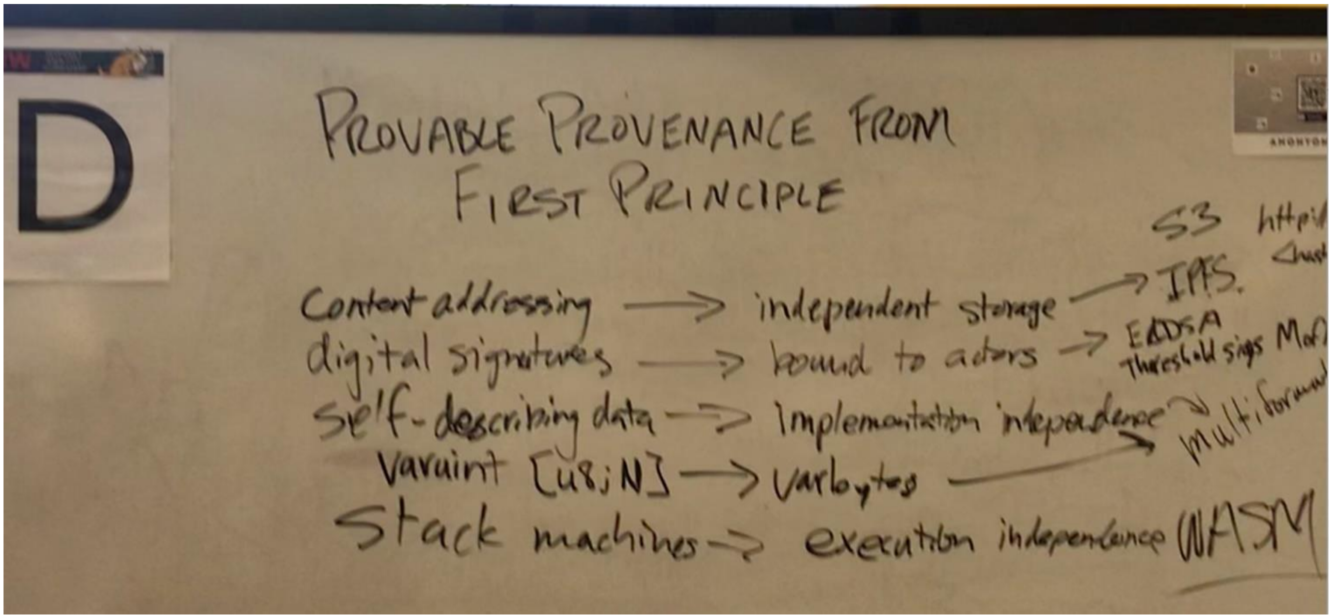
Open Source Supply Chain

- provenance logs
    - event log
    - chain of custodiy
    - cryptographic puzzle - for who can add next event
- sequence #
- VLAD
    - very long-lived address

A Provenance Log Schema

seqno:	0
VLAD **(very long lived address; not key material)** • **remains unchanged through life of p.log** • **stable over a very long period of time**	...
< Prev:	CID (content ID)
Unlock:	WASM
Lock:	WASM
Op	update ("/pubkey; <pubkey>) delete ("/

- obviates the need for KERI pre-rotation



PROVABLE PROVENANCE FROM
FIRST PRINCIPLE

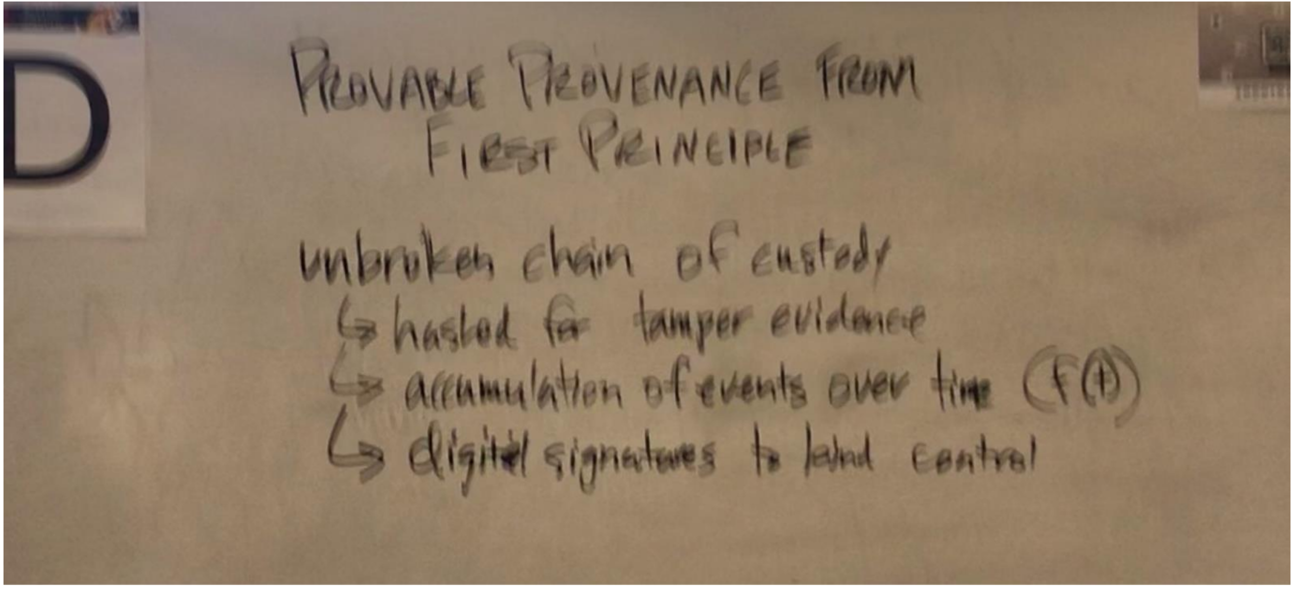
Content addressing ⟶ independent storage ⟶ IPFS. S3 http:/ <hash

digital signatures ⟶ bound to actors ⟶ EdDSA Threshold sigs Mof

self-describing data ⟶ Implementation independence ⟶ multiform

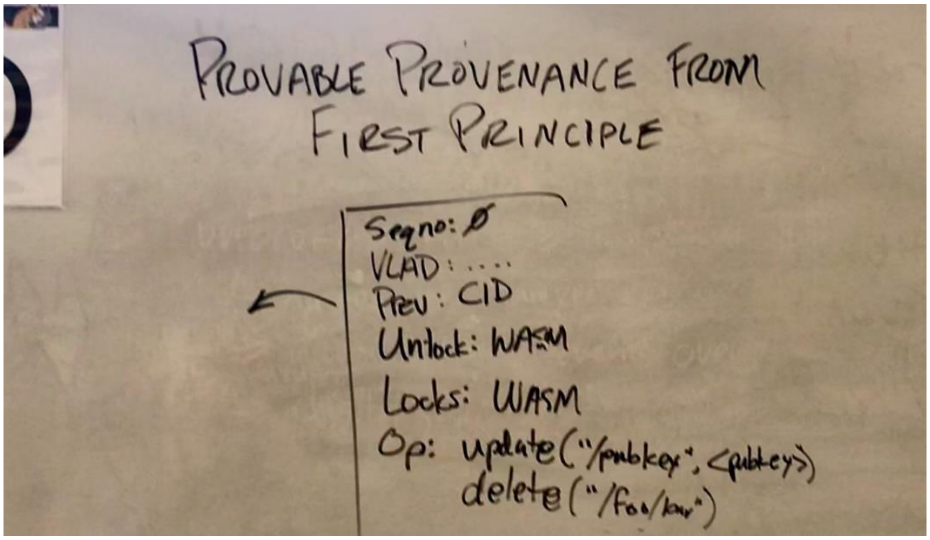
Varuint [u8;N] ⟶ Varbytes ⟶

Stack machines ⟶ execution independence WASM



PROVABLE PROVENANCE FROM
FIRST PRINCIPLE

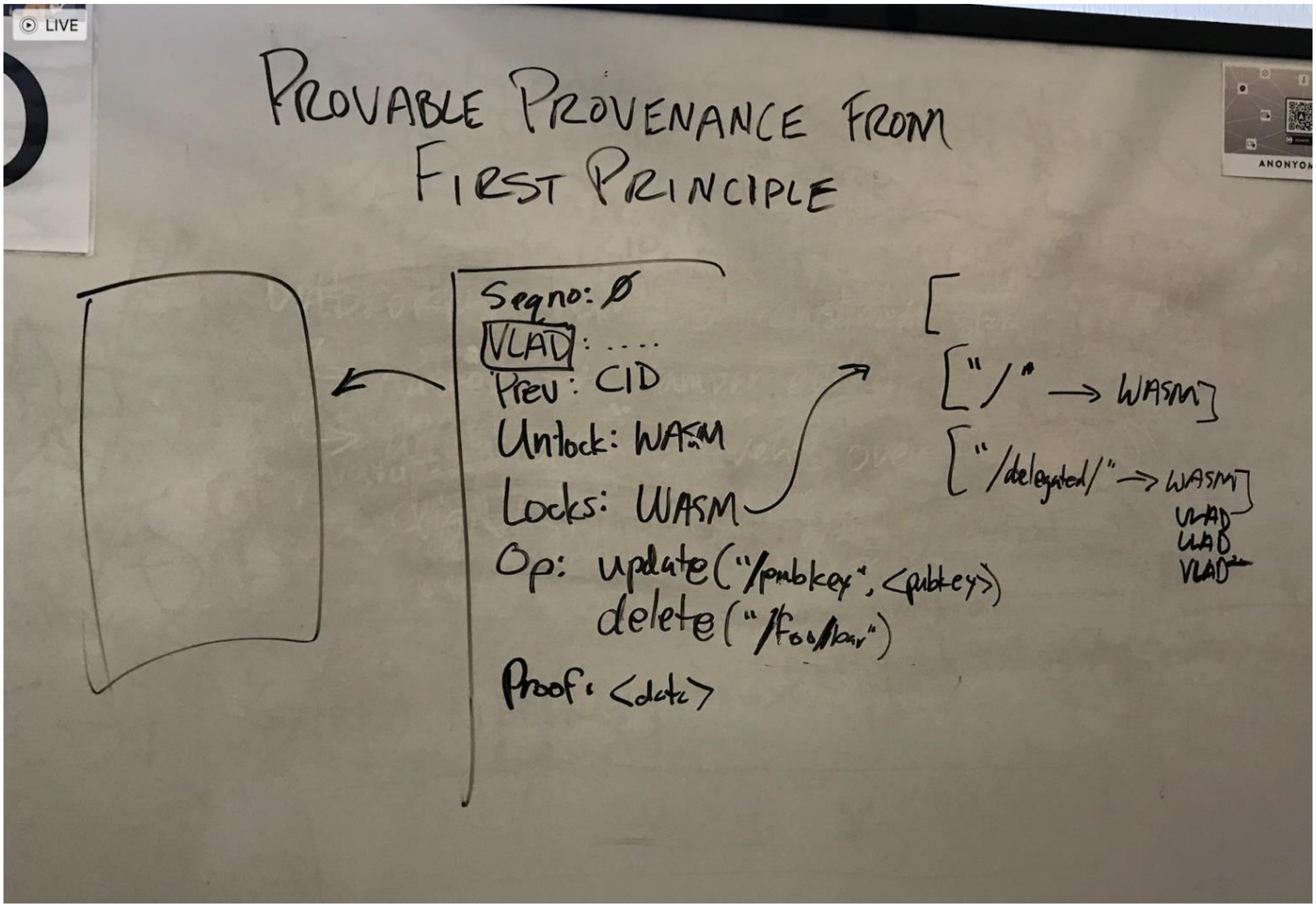
unbroken chain of custody
↳ hashed for tamper evidence
↳ accumulation of events over time (f(t))
↳ digital signatures to bind control

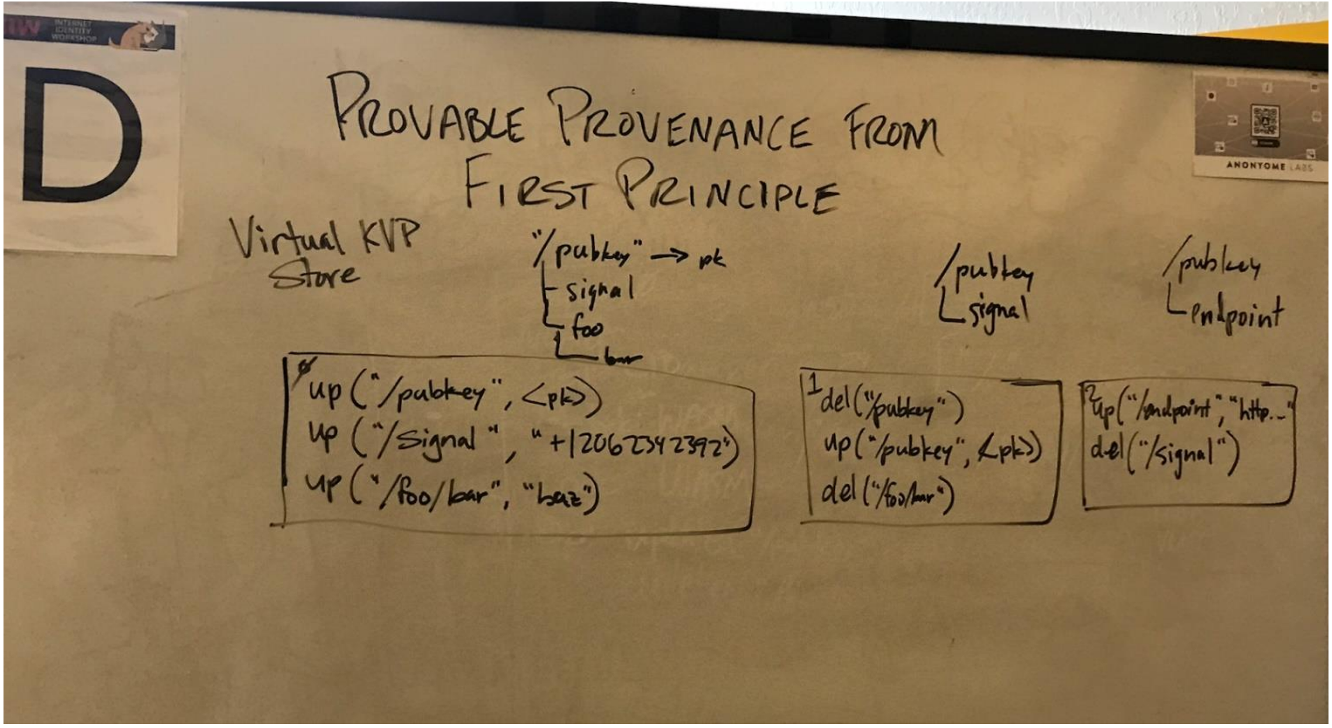


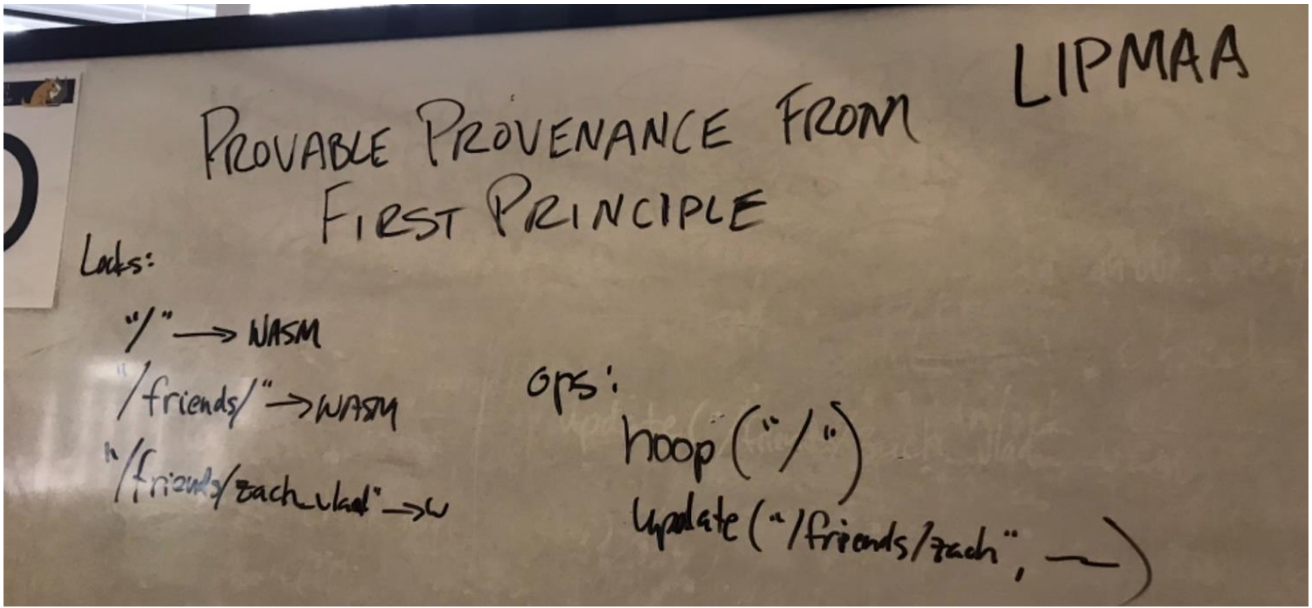
PROVABLE PROVENANCE FROM
FIRST PRINCIPLE

```
Seqno: Ø
VLAD: ....
Prev: CID
Unlock: WASM
Locks: WASM
Op: update("/pubkey", <pubkey>)
    delete("/foo/bar")
```

Adding Part 2 here for cohesiveness:





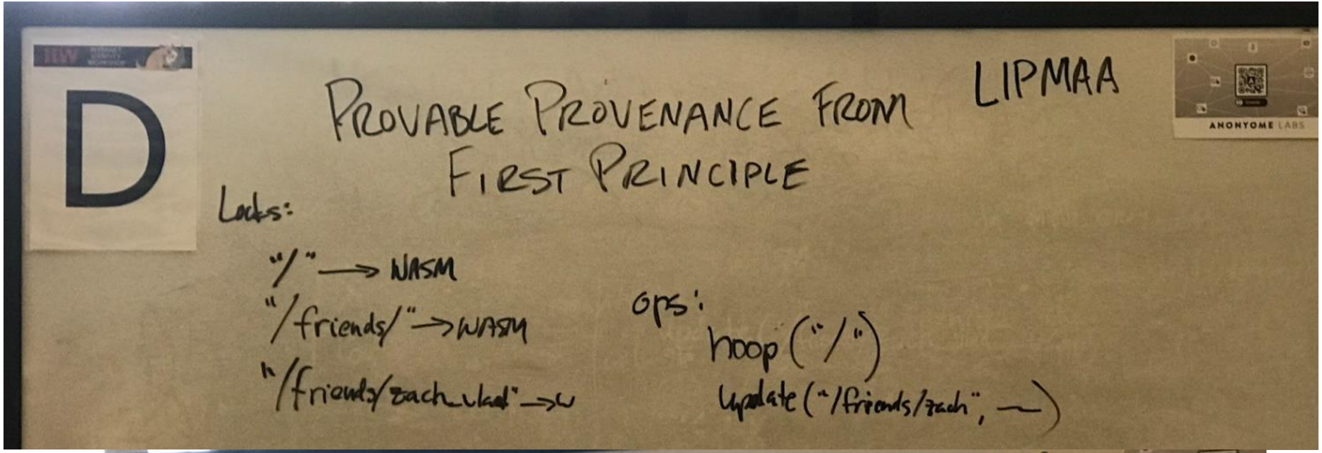


LIPMAA

PROVABLE PROVENANCE FROM
FIRST PRINCIPLE

Locks:
"/" → WASM
"/friends/" → WASM
"/friends/zach_vlad" → W

ops:
hoop ("/")
Update ("/friends/zach", —)

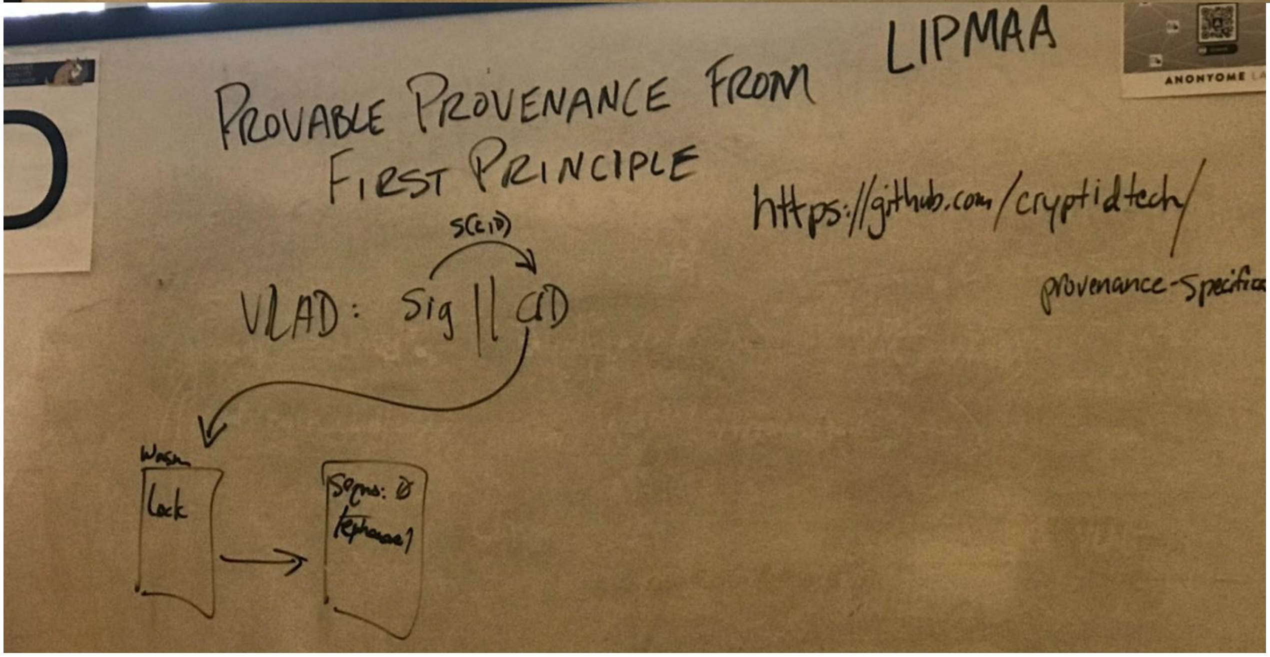


LIPMAA

PROVABLE PROVENANCE FROM
FIRST PRINCIPLE

Locks:
"/" → WASM
"/friends/" → WASM
"/friends/zach_vlad" → W

ops:
hoop ("/")
Update ("/friends/zach", —)



LIPMAA

PROVABLE PROVENANCE FROM
FIRST PRINCIPLE

https://github.com/cryptidtech/provenance-specifica

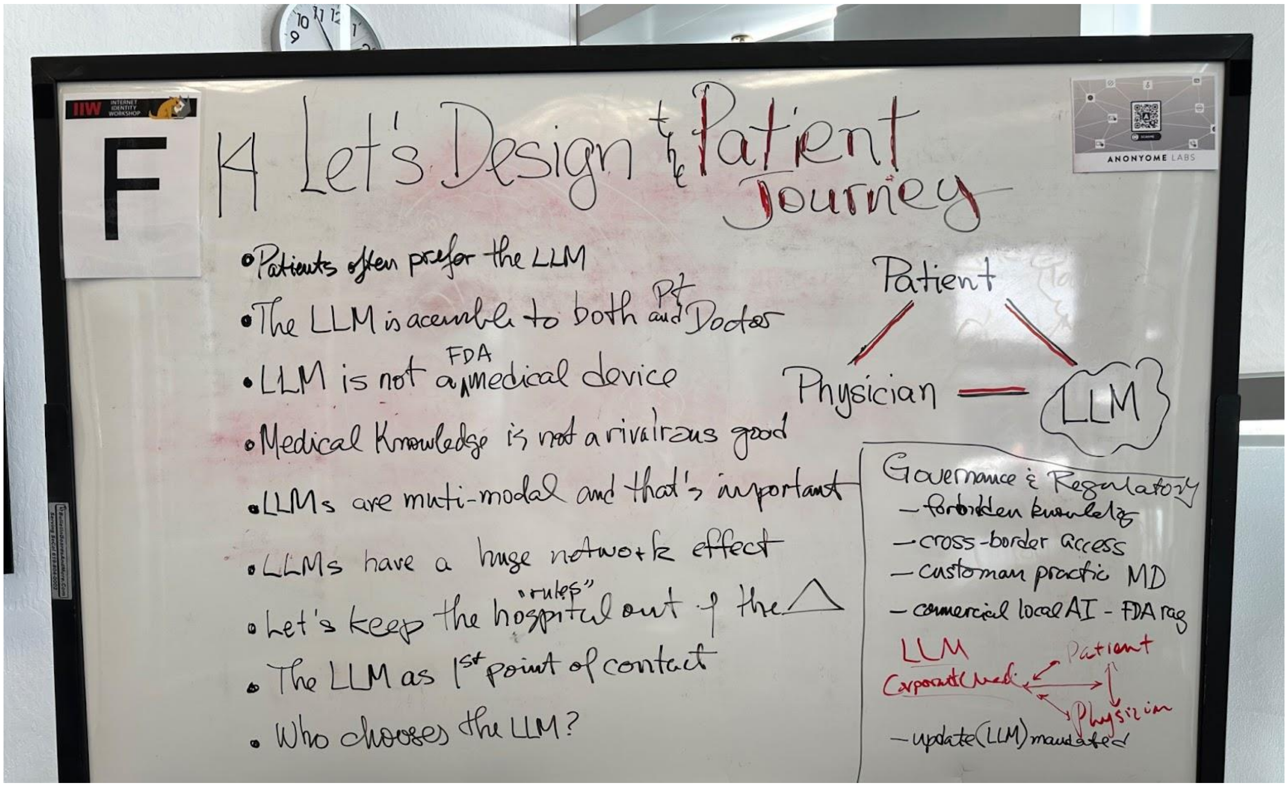
VLAD: Sig || CID

Design the Patient Journey

Session Convener: Adrian Gropper
Session Notes Taker(s): Adrian Gropper

Tags / links to resources / technology discussed, related to this session:

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



- Patients often prefer the LLM
- The LLM is accessible to both Pt and Doctor
- LLM is not a FDA medical device
- Medical Knowledge is not a rivalrous good
- LLMs are muti-modal and that's important
- LLMs have a huge network effect
- Let's keep the hospital out of the "rules" △
- The LLM as 1st point of contact
- Who chooses the LLM?

Governance & Regulatory
- forbidden knowledge
- cross-border access
- customary practice MD
- commercial local AI - FDA reg

LLM
Corporate/Medi
Patient
Physizian

- update(LLM) mandated

Board Transcript:

- Patients often prefer chatting with the LLM to a physician
- The same LLM is accessible to patient as well as the physician
- The LLM is not an FDA-regulated medical device. It's closer to a search engine.
- Medical knowledge, like science, is not a rivalrous good. The more you give away, the better.
- LLMs are multimodal (text, voice, photos, translation, etc…) and that makes them better than specialized AI.
- LLMs have a huge network effect. Like search engines or Amazon, the biggest get bigger.
- Let's keep the hospital from controlling the patient-physician dialogue.
- LLMs can be the first point of contact for the patient.
- Who chooses my LLM? Should the hospital choose the physician's LLM?

Verifiable Credentials with BBS+ and zk-SNARKs for Predicate Proofs

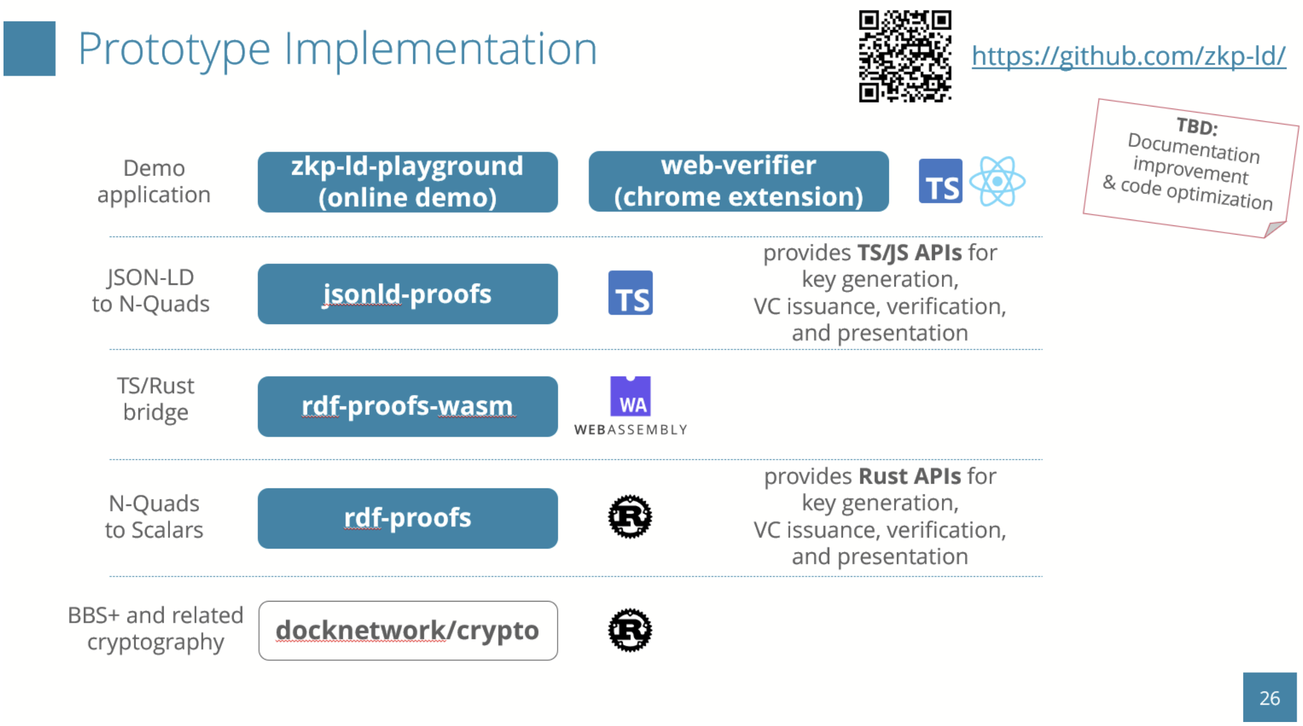
Session Convener: Dan Yamamoto
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

- Tags: Verifiable Credentials, Verifiable Presentations, BBS+ Signatures, Zero-Knowledge Proofs, zk-SNARKs, Pairwise Pseudonymous Identifier (PPID)
- Related session: Verifiable Presentation as a Signature (Day 1 / Session 5 / Room H)
- The playground website for the demo: https://playground.zkp-ld.org/

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

- The convener used ZKP-LD Playground https://playground.zkp-ld.org/ to demonstrate the following steps:
    1. Issuing a VC bound to the holder's secret key by using BBS+ blind signature scheme
    2. Composing a VP from the VC where the attributes are selectively disclosed by using BBS+
    3. Adding a predicate proof, which allows the holder to prove they are 21 years over without revealing their exact birthdate, to the VP by using zk-SNARK
    4. Adding a PPID (Pairwise Pseudonymous Identifier) generated from the holder's secret key and domain's identifier (e.g., bsky.social)
    5. Uploading the VP to GitHub to make it publicly accessible
    6. Embed the hyperlink to the VP (on GitHub) to Bluesky post for making it publicly verifiable
- BBS+ signature scheme provides blind issuance feature for key binding, selective disclosure, and unlinkable presentation, whereas zk-SNARKs enable predicate proofs.
- Currently there are six types of predicates supported, all of which are number comparisons. Attributes typed `date` and `datetime` are internally converted into UNIX timestamp so that they can be used for predicate proofs.
- In this demo, "private < public" predicate is used for age verification, where the private value is the holder's birthdate and the public value is `2003-04-18T00:00:00Z` that is the datetime 21 years before this session.
- More general predicates will be available; all you have to add a predicate is write it as Circom circuit and convert it to SNARK keys.
- Both BBS+ and zk-SNARKs are powered by Dock Network crypto library (https://github.com/docknetwork/crypto)
- Current implementation is using LegoGroth16, which is a zk-SNARK requiring trusted setup.



Prototype Implementation

https://github.com/zkp-ld/

TBD:
Documentation improvement & code optimization

Demo application	zkp-ld-playground (online demo)	web-verifier (chrome extension)	TS
JSON-LD to N-Quads	jsonld-proofs	TS	provides **TS/JS APIs** for key generation, VC issuance, verification, and presentation
TS/Rust bridge	rdf-proofs-wasm	WA WEBASSEMBLY	
N-Quads to Scalars	rdf-proofs	R	provides **Rust APIs** for key generation, VC issuance, verification, and presentation
BBS+ and related cryptography	docknetwork/crypto	R	

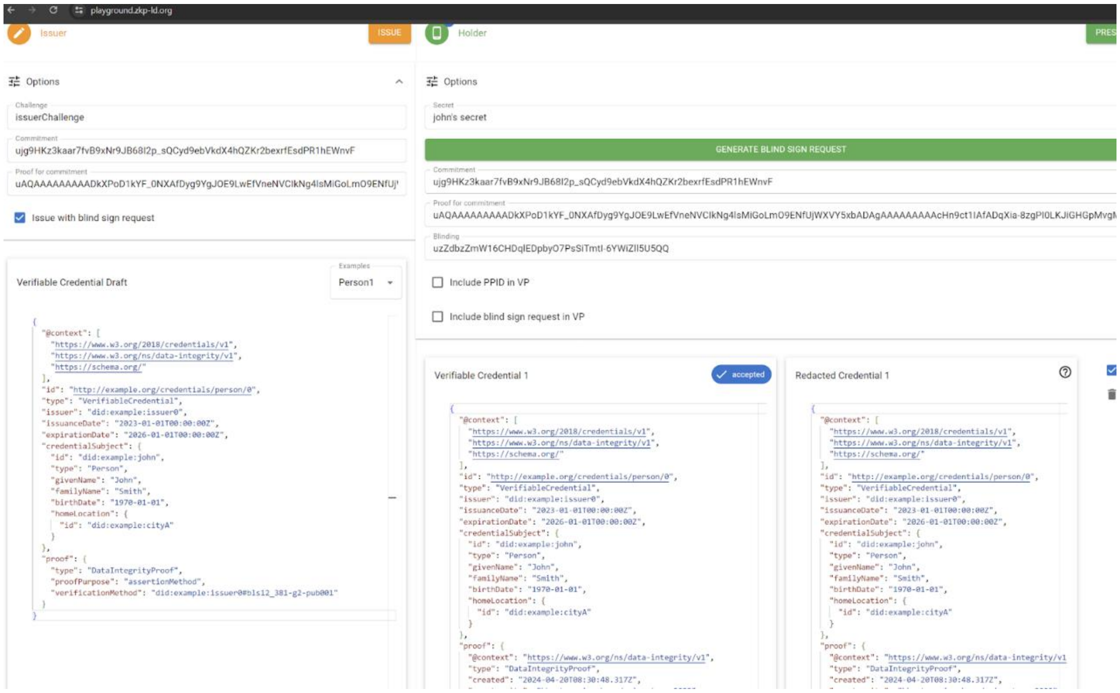
26

Discussion:

- If the birthdate in the credential does not meet the condition specified in the predicate, but a presentation is forcibly created anyway, what happens?
    - In that case, the presentation will be generated, but it will fail during the verifier's validation. The inability to create such malicious proofs is guaranteed by the soundness property of zk-SNARKs.
- Are predicates other than range proofs supported?
    - Currently, the playground only supports range proofs. However, it is possible to integrate any predicate that can be described in the circom language here. This is achieved by utilizing the circom processing capabilities provided by docknetwork/crypto's legogroth16 feature.
- How are BBS and zk-SNARK combined?
    - The method proposed in the LegoSNARK paper is used. Specifically, attributes in BBS and zk-SNARK (legogroth16) are linked through the Pedersen commitment values of attributes that appear in both (birthdate in this demo). The implementation utilizes those provided by docknetwork/crypto.
- We need to consider more specific mechanisms to securely represent identifiers for predicates (circuits) and the corresponding parameters for zk-SNARKs. Otherwise, there is a risk that the holder's privacy could be compromised by *malicious circuits* crafted like malware.
- When using the proposed method with Bluesky, it seems advisable to link the PPID in the VP with the DID of the Bluesky account.

Screen shots:

1. Issuing a VC bound to the holder's secret key by using BBS+ blind signature scheme



Options

Challenge
issuerChallenge

Commitment
ujg9HKz3kaar7fvB9xNr9JB68I2p_sQCyd9ebVkdX4hQZKr2bexrfEsdPR1hEWnvF

Proof for commitment
uAQAAAAAAAAADkXPoD1kYF_0NXAfDyg9YgJOE9LwEfVneNVCIkNg4lsMiGoLmO9ENfUj'

☑ Issue with blind sign request

Verifiable Credential Draft

Examples
Person1

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/ns/data-integrity/v1",
    "https://schema.org/"
  ],
  "id": "http://example.org/credentials/person/0",
  "type": "VerifiableCredential",
  "issuer": "did:example:issuer0",
  "issuanceDate": "2023-01-01T00:00:00Z",
  "expirationDate": "2026-01-01T00:00:00Z",
  "credentialSubject": {
    "id": "did:example:john",
    "type": "Person",
    "givenName": "John",
    "familyName": "Smith",
    "birthDate": "1970-01-01",
    "homeLocation": {
      "id": "did:example:cityA"
    }
  },
  "proof": {
    "type": "DataIntegrityProof",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "did:example:issuer0#bls12_381-g2-pub001"
  }
}
```

Options

Secret
john's secret

GENERATE BLIND SIGN REQUEST

Commitment
ujg9HKz3kaar7fvB9xNr9JB68I2p_sQCyd9ebVkdX4hQZKr2bexrfEsdPR1hEWnvF

Proof for commitment
uAQAAAAAAAAADkXPoD1kYF_0NXAfDyg9YgJOE9LwEfVneNVCIkNg4lsMiGoLmO9ENfUjWXVY5xbADAgAAAAAAAAAcHn9ct1IAfADqXia-8zgPI0LKJiGHGpMvgM

Blinding
uzZdbzZmW16CHDqlEDpbyO7PsSiTmtl-6YWiZII5U5QQ

□ Include PPID in VP

□ Include blind sign request in VP

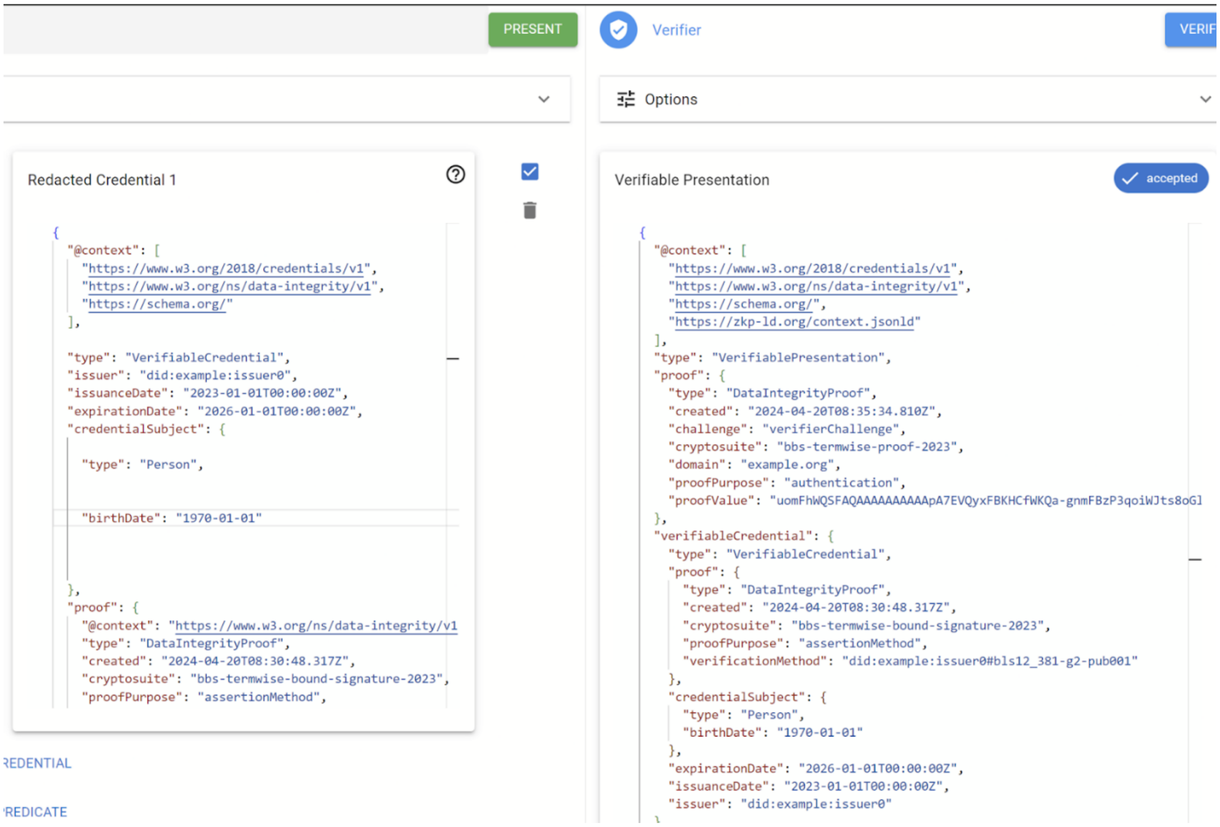
Verifiable Credential 1 ✓ accepted

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/ns/data-integrity/v1",
    "https://schema.org/"
  ],
  "id": "http://example.org/credentials/person/0",
  "type": "VerifiableCredential",
  "issuer": "did:example:issuer0",
  "issuanceDate": "2023-01-01T00:00:00Z",
  "expirationDate": "2026-01-01T00:00:00Z",
  "credentialSubject": {
    "id": "did:example:john",
    "type": "Person",
    "givenName": "John",
    "familyName": "Smith",
    "birthDate": "1970-01-01",
    "homeLocation": {
      "id": "did:example:cityA"
    }
  },
  "proof": {
    "@context": "https://www.w3.org/ns/data-integrity/v1",
    "type": "DataIntegrityProof",
    "created": "2024-04-20T08:30:48.317Z",
```

Redacted Credential 1

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/ns/data-integrity/v1",
    "https://schema.org/"
  ],
  "id": "http://example.org/credentials/person/0",
  "type": "VerifiableCredential",
  "issuer": "did:example:issuer0",
  "issuanceDate": "2023-01-01T00:00:00Z",
  "expirationDate": "2026-01-01T00:00:00Z",
  "credentialSubject": {
    "id": "did:example:john",
    "type": "Person",
    "givenName": "John",
    "familyName": "Smith",
    "birthDate": "1970-01-01",
    "homeLocation": {
      "id": "did:example:cityA"
    }
  },
  "proof": {
    "@context": "https://www.w3.org/ns/data-integrity/v1
    "type": "DataIntegrityProof",
    "created": "2024-04-20T08:30:48.317Z",
```

2. Composing a VP from the VC where the attributes are selectively disclosed by using BBS+



Redacted Credential 1

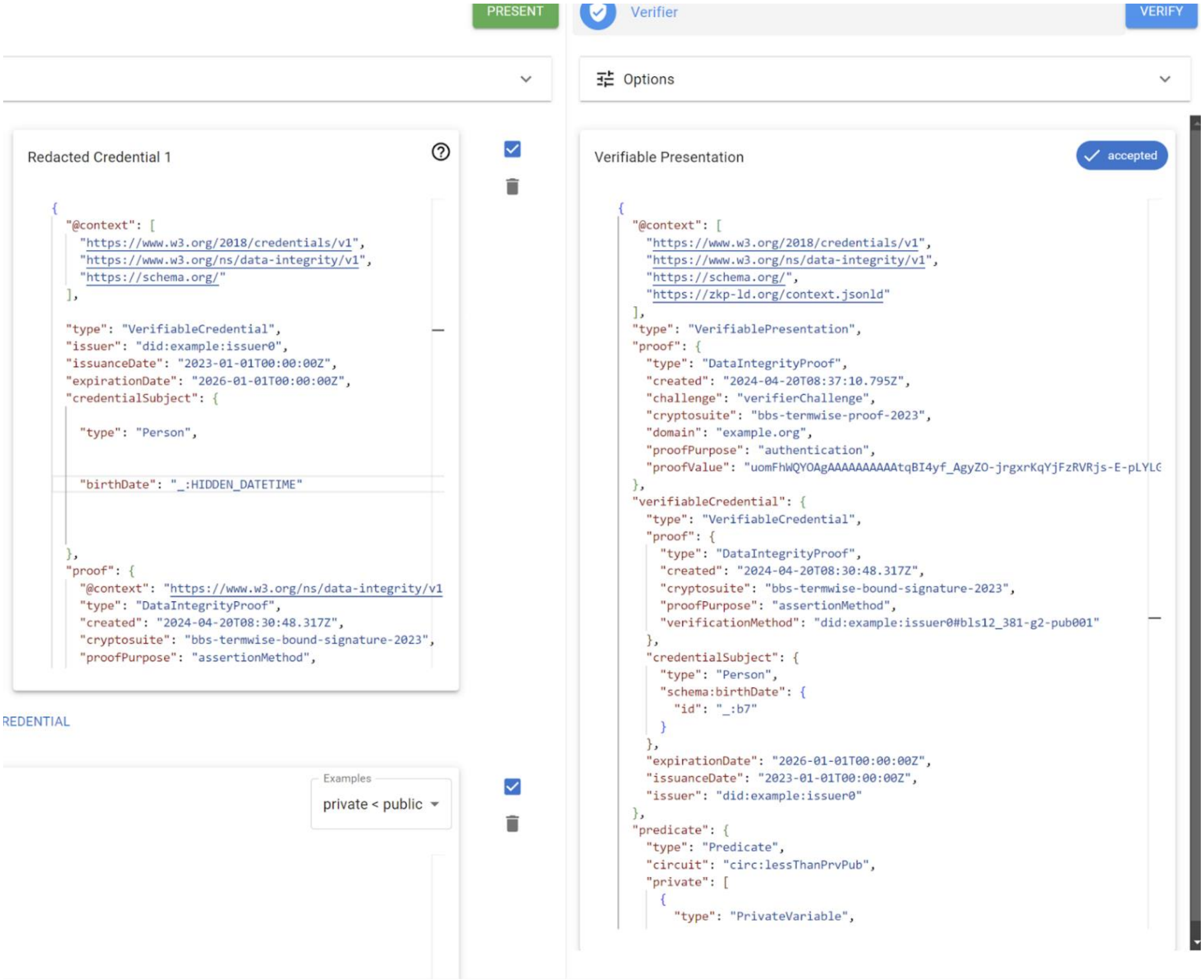
```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/ns/data-integrity/v1",
    "https://schema.org/"
  ],

  "type": "VerifiableCredential",
  "issuer": "did:example:issuer0",
  "issuanceDate": "2023-01-01T00:00:00Z",
  "expirationDate": "2026-01-01T00:00:00Z",
  "credentialSubject": {

    "type": "Person",


    "birthDate": "1970-01-01"



  },
  "proof": {
    "@context": "https://www.w3.org/ns/data-integrity/v1
    "type": "DataIntegrityProof",
    "created": "2024-04-20T08:30:48.317Z",
    "cryptosuite": "bbs-termwise-bound-signature-2023",
    "proofPurpose": "assertionMethod",
```

Options

Verifiable Presentation ✓ accepted

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/ns/data-integrity/v1",
    "https://schema.org/",
    "https://zkp-ld.org/context.jsonld"
  ],
  "type": "VerifiablePresentation",
  "proof": {
    "type": "DataIntegrityProof",
    "created": "2024-04-20T08:35:34.810Z",
    "challenge": "verifierChallenge",
    "cryptosuite": "bbs-termwise-proof-2023",
    "domain": "example.org",
    "proofPurpose": "authentication",
    "proofValue": "uomFhWQSFAQAAAAAAAAAApA7EVQyxFBKHCfWKQa-gnmFBzP3qoiWJts8oGl
  },
  "verifiableCredential": {
    "type": "VerifiableCredential",
    "proof": {
      "type": "DataIntegrityProof",
      "created": "2024-04-20T08:30:48.317Z",
      "cryptosuite": "bbs-termwise-bound-signature-2023",
      "proofPurpose": "assertionMethod",
      "verificationMethod": "did:example:issuer0#bls12_381-g2-pub001"
    },
    "credentialSubject": {
      "type": "Person",
      "birthDate": "1970-01-01"
    },
    "expirationDate": "2026-01-01T00:00:00Z",
    "issuanceDate": "2023-01-01T00:00:00Z",
    "issuer": "did:example:issuer0"
```

3. Adding a predicate proof, which allows the holder to prove they are 21 years over without revealing their exact birthdate, to the VP by using zk-SNARK



Redacted Credential 1

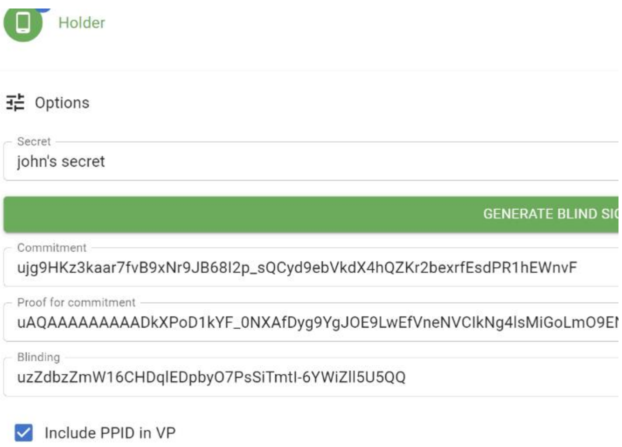
```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/ns/data-integrity/v1",
    "https://schema.org/"
  ],

  "type": "VerifiableCredential",
  "issuer": "did:example:issuer0",
  "issuanceDate": "2023-01-01T00:00:00Z",
  "expirationDate": "2026-01-01T00:00:00Z",
  "credentialSubject": {

    "type": "Person",


    "birthDate": "_:HIDDEN_DATETIME"



  },
  "proof": {
    "@context": "https://www.w3.org/ns/data-integrity/v1
    "type": "DataIntegrityProof",
    "created": "2024-04-20T08:30:48.317Z",
    "cryptosuite": "bbs-termwise-bound-signature-2023",
    "proofPurpose": "assertionMethod",
```

Verifiable Presentation ✓ accepted

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/ns/data-integrity/v1",
    "https://schema.org/",
    "https://zkp-ld.org/context.jsonld"
  ],
  "type": "VerifiablePresentation",
  "proof": {
    "type": "DataIntegrityProof",
    "created": "2024-04-20T08:37:10.795Z",
    "challenge": "verifierChallenge",
    "cryptosuite": "bbs-termwise-proof-2023",
    "domain": "example.org",
    "proofPurpose": "authentication",
    "proofValue": "uomFhWQYOAgAAAAAAAAAAtqBI4yf_AgyZO-jrgxrKqYjFzRVRjs-E-pLYLG
  },
  "verifiableCredential": {
    "type": "VerifiableCredential",
    "proof": {
      "type": "DataIntegrityProof",
      "created": "2024-04-20T08:30:48.317Z",
      "cryptosuite": "bbs-termwise-bound-signature-2023",
      "proofPurpose": "assertionMethod",
      "verificationMethod": "did:example:issuer0#bls12_381-g2-pub001"
    },
    "credentialSubject": {
      "type": "Person",
      "schema:birthDate": {
        "id": "_:b7"
      }
    },
    "expirationDate": "2026-01-01T00:00:00Z",
    "issuanceDate": "2023-01-01T00:00:00Z",
    "issuer": "did:example:issuer0"
  },
  "predicate": {
    "type": "Predicate",
    "circuit": "circ:lessThanPrvPub",
    "private": [
      {
        "type": "PrivateVariable",
```

4. <u>Adding a PPID (Pairwise Pseudonymous Identifier) generated from the holder's secret key and domain's identifier (e.g., bsky.social)</u>

(holder's secret = `john's secret`)   (domain's identifier = `bsky.social`)



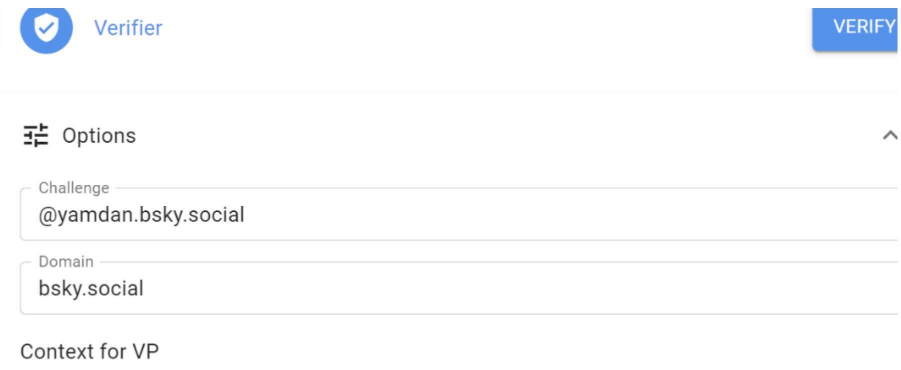
Secret
john's secret

Commitment
ujg9HKz3kaar7fvB9xNr9JB68I2p_sQCyd9ebVkdX4hQZKr2bexrfEsdPR1hEWnvF

Proof for commitment
uAQAAAAAAAAADkXPoD1kYF_0NXAfDyg9YgJOE9LwEfVneNVClkNg4lsMiGoLmO9EI

Blinding
uzZdbzZmW16CHDqlEDpbyO7PsSiTmtl-6YWiZIl5U5QQ

☑ Include PPID in VP

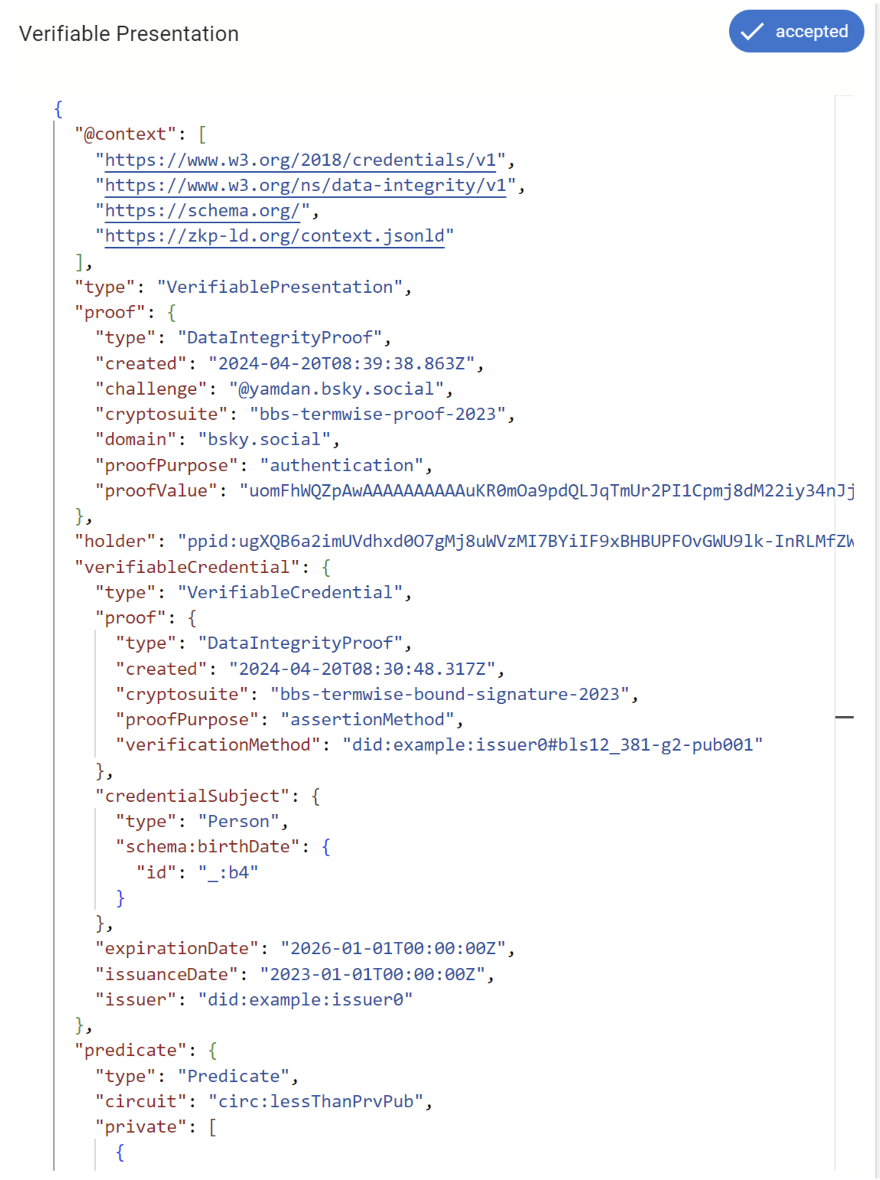


Challenge
@yamdan.bsky.social

Domain
bsky.social

Context for VP

(generated VP)



Verifiable Presentation

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/ns/data-integrity/v1",
    "https://schema.org/",
    "https://zkp-ld.org/context.jsonld"
  ],
  "type": "VerifiablePresentation",
  "proof": {
    "type": "DataIntegrityProof",
    "created": "2024-04-20T08:39:38.863Z",
    "challenge": "@yamdan.bsky.social",
    "cryptosuite": "bbs-termwise-proof-2023",
    "domain": "bsky.social",
    "proofPurpose": "authentication",
    "proofValue": "uomFhWQZpAwAAAAAAAAAAuKR0mOa9pdQLJqTmUr2PI1Cpmj8dM22iy34nJj
  },
  "holder": "ppid:ugXQB6a2imUVdhxd0O7gMj8uWVzMI7BYiIF9xBHBUPFOvGWU9lk-InRLMfZW
  "verifiableCredential": {
    "type": "VerifiableCredential",
    "proof": {
      "type": "DataIntegrityProof",
      "created": "2024-04-20T08:30:48.317Z",
      "cryptosuite": "bbs-termwise-bound-signature-2023",
      "proofPurpose": "assertionMethod",
      "verificationMethod": "did:example:issuer0#bls12_381-g2-pub001"
    },
    "credentialSubject": {
      "type": "Person",
      "schema:birthDate": {
        "id": "_:b4"
      }
    },
    "expirationDate": "2026-01-01T00:00:00Z",
    "issuanceDate": "2023-01-01T00:00:00Z",
    "issuer": "did:example:issuer0"
  },
  "predicate": {
    "type": "Predicate",
    "circuit": "circ:lessThanPrvPub",
    "private": [
      {
```

Talk Workshopping - Biometrics & Communication: Identity Implications

Session Convener: Kaliya Young
Session Notes Taker(s): Kaliya

Tags / links to resources / technology discussed, related to this session:

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

Kaliya talked through key elements of an upcoming talk about Biometrics and the communication failures that industry. The talk will be given at Identiverse. If you want to see it it will likely be online after that event.

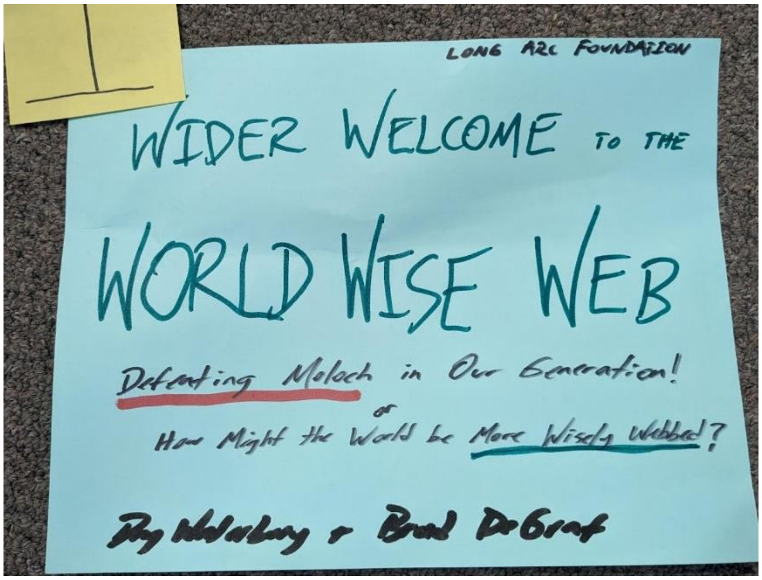
Wider Welcome to the World Wise Web

Session Convener: Day Waterbury
Session Notes Taker(s): Day Waterbury

Tags / links to resources / technology discussed, related to this session:

The World Wise Web

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


LONG ARC FOUNDATION
WIDER WELCOME TO THE
WORLD WISE WEB
Defeating Moloch in Our Generation!
or
How Might the World be More Wisely Webbed?
Day Waterbury & Brad DeGraf

Linking notes to all our woven sessions here (Proton Drive PW: Share->IIW38 or Signal me @deiim.69 in case I change the PW) to save time. If I can I'll pull the session-specific transcripts in.

State of eIDAS + German eIDAS Wallet Consultation Project + Wallet Challenge

Session Convener: Paul Bastian, Torsten Lodderstedt, Kristina Yasuda
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

URL eIDAS IIW.pdf

URL to the explanation of German EUDIW architecture proposal: Architecture Proposal V2 - OSW and IIW 2024.pdf

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

vLEI (verified Legal Entity Identifier) Demystified

Session Convener: Nuttawut Kongsuwan
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

Link to Slides
http://bit.ly/keri-iiw38

Link to Blog Posts
https://medium.com/finema/vlei-demystified-part-1-comprehensive-overview-212349c09643
https://medium.com/finema/vlei-demystified-part-2-identity-verification-519102614b8e

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

SESSION #15

Wallet Attestation + OAuthZ Attestation-based Client Authentication. IETF Draft

Session Convener: Paul & Tobias
Session Notes Taker(s): Jin Wen

Tags / links to resources / technology discussed, related to this session:

IETF OAuth 2.0 Attestation-based Client Authentication
https://datatracker.ietf.org/doc/draft-ietf-oauth-attestation-based-client-auth/

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

Legal requirements and how it is interpreted in ARF

eIDAS legal text
5. European Digital Identity Wallets shall, in particular:

(a) Support common protocols and interfaces
(viii) for relying parties to verify the authenticity and validity of European Digital Identity Wallets;

eIDAS ARF 6.2.2 EUDI Wallet Instance activation (eudi-doc-architecture-and-reference-framework/docs/arf.md at main)
eIDAS

- Main motivation and first intended use case
- Enable issuance of PID and other Credentials with Level of Assurance high/substantial
  - Prove the authenticity of the app (Wallet Instance)
  - Prove the authenticity and key type of the keys (Wallet Security Cryptographic Device, WSCD)
  - Enable provable hardware-bound credentials
  - Enable RPs to verify the Wallet Instance (in discussion)
  - Abstract and consolidate the various platform-specific attestation into a unified format
  - Provide a reliable, technology-independent long-term interface for Issuers/Verifiers

Architecture
Example of Client Attestation

- DPoP is used

- Requires confirmation

- New IETF request for Client Attestation, including new type “typ” = “wallet-attestation+jwt”
- client instance
- Example from HAIP

Progress Update

Two proposals for discussion today

1. Proposal to use DPoP for the PoP syntax, instead of defining our own
2. Proposal to support a header based syntax for the communication to the attestation to support other non-client authentication use cases

==== Start transcript via OpenAI Whisper and summarization via Perplexity ===============

The transcript primarily discusses the concepts of Wallet Attestation and OAuthZ Attestation-based Client Authentication, focusing on the technical and regulatory aspects of implementing wallet attestation in identity verification systems. Here are the key points highlighted in the transcript:

1. **Purpose of Wallet Attestation**: Wallet attestation is primarily used to enable identity credentials with cryptographic binding. It aims to attest the authenticity of wallets, ensuring that the wallet software and the cryptographic keys it manages are legitimate and secure.
2. **Technical Implementation**: The discussion includes details about how wallet instances, which are specific software applications for wallets, are attested. This involves the wallet provider issuing a wallet instance attestation, which can then be used by the wallet instance to authenticate towards an issuer.
3. **Trust and Verification**: The attestation allows issuers to verify that a wallet is legitimate before issuing high-assurance credentials like identity credentials. This process is crucial for maintaining the security and integrity of the identity verification process.
4. **Regulatory and Compliance Challenges**: There are complexities related to the legal and regulatory aspects of wallet attestation. The transcript mentions the European Digital Identity Wallet and the need for compliance with specific regulations that might require wallet attestations to be available not just to issuers but also to relying parties.
5. **Client Attestation in OAuth**: The discussion also touches on the integration of wallet attestation with OAuth client authentication. This involves using attestation in the OAuth flow, where a client instance proves its authenticity to a client backend using a key and attestation data.
6. **Security Considerations**: The security of the attestation process and the prevention of credential misuse are discussed. It is noted that high-assurance use cases, particularly in government applications, do not allow users to transfer credentials freely between wallets due to security risks.
7. **Future Directions and Challenges**: The transcript hints at ongoing developments and future improvements in wallet attestation practices, including the potential for standardizing certain aspects of the attestation process and addressing emerging requirements.

Overall, the transcript provides a detailed look at the technical, regulatory, and security considerations involved in implementing wallet attestation in systems that require high levels of identity assurance.

Citations: [1] https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/1617151/ef663afa-0777-4d73-8d88-b08e253e2a22/OAuth Client Authentication (Apr 18 14.01.45).txt [2] https://datatracker.ietf.org/doc/draft-ietf-oauth-attestation-based-client-auth/ [3] https://github.com/italia/eudi-wallet-it-docs/issues/33 [4] https://www.authlete.com/developers/oid4vci/ [5] https://www.w3.org/TR/webauthn-3/ [6] https://www.w3.org/TR/webauthn-2/ [7] https://blog.safeheron.com/blog/insights/safeheron-originals/demystify-remote-attestation-explore-the-dcap-certificate-chain [8] https://openid.net/specs/openid-4-verifiable-presentations-1_0.html [9] https://blog.ceramic.network/ceramic-ethereum-attestation-service-how-to-use-and-store-composable-attestations/ [10] https://webauthn.guide [11] https://backstage.forgerock.com/docs/am/6.5/authentication-guide/ [12] https://help.coinbase.com/en/coinbase/getting-started/verify-my-account/onchain-verification [13] https://discussions.apple.com/thread/253196652?sortBy=best [14] https://www.developer.tech.gov.sg/products/categories/blockchain/openattestation-wallet-app/overview.html [15] https://github.com/decentralized-identity/wallet-security/blob/main/agenda.md [16] https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html [17] https://arxiv.org/pdf/2102.12473.pdf

==== End transcript via OpenAI Whisper and summarization via Perplexity ===============

I don't sign my credentials and neither should you! Why unbound signatures (tokens) are insecure and how to use KERI instead. KERI for Enterprise

Session Convener: Sam Smith
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

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

No Notes Submitted

“No more Plaque Buildup” - Learning and Employment Credentials (LER’s) for Employees, Governance and User Adoption

Session Convener: Mahesh Balan
mahesh@pravici.com https://www.pravici.com
Session Notes Taker(s): Mahesh Balan

Tags / links to resources / technology discussed, related to this session:

The central issue around Learning and Employment records has been succinctly explained by the US Chamber of Commerce Foundation as follows:

“People often can’t communicate what they know and are able to do in ways that are meaningful to employers. Yet employers, trying to find the right talent to fit their needs, rely on a person’s ability to communicate the value of their skills and experience. Our talent marketplace is fragmented, preventing an individual’s record of learning from being transferable data. And any data that is collected is siloed. This is the data and technology challenge the T3 Innovation Network is working to solve to create more equitable and effective learning and career pathways for today’s learners and workers.”

1. US Chamber of Commerce Foundation T3 Network - https://www.uschamberfoundation.org/solutions/workforce-development-and-training/t3-innovation-network
2. T3 Network Hub, the LER Ecosystem Map - https://lermap.t3networkhub.org/
3. Besides the T3 Network, the Digital Credentials Consortium, a group of educational institutions spearheaded by MIT, has produced a lot of work, including developing open-source software for the issuance of digital credentials. Their stated goal is “We are building an infrastructure for digital academic credentials that can support the education systems of the future.” - https://digitalcredentials.mit.edu/
4. A White paper on the topic of the Employment Last Mile Problem - https://digitalcredentials.mit.edu/docs/Credentials-to-Employment-The-Last-Mile.pdf. A very thoughtful paper, pointing out all the issues but also good recommendations for digitizing credentials. Per Scholas is very much in the business of solving the last mile problem to employment, so I think Digital Credentials need to be part of your solution.
5. A lot of the standardization work on digital credentials is done by the World Wide Web Consortium (W3C). Inside the W3C, the Verifiable Credentials for Education Task Force (VC-EDU) meets every Monday morning; I have been a member of this task force for the last several years, I would encourage people from Per Scholas to join in and be part of the solution. VC-EDU chairs are closely allied with the Digital Credentials Consortium mentioned in points 2 and 3 above. “This effort was anchored in the Digital Credentials Consortium (DCC), consisting of 12 universities, as it sought to collaborate with potential partners, implementers, and the public to further develop use cases and requirements.” - https://w3c-ccg.github.io/vc-ed/charter/

6. ASU and the Trusted Learner Network, headed by Kate Giovacchini, is a driving force in Learning and Employment Records (LERs). Their charter is to get a million LER's issued in 2024 - https://tln.asu.edu/
    - The TLN is a **technology** that allows learners to collect, explore and share digital credentials that they have gathered across their lifetimes.
    - It is an environment guided by strong **governance** policies to ensure that the learner is always at the center of critical decision-making.
    - It is a **community** of digital credential experts and enthusiasts who are building an ecosystem to empower learners as they share their educational experiences.
7. Pravici RnR, as part of the goal of addressing all Employee Rewards and Recognition, will have the ability to issue LER's for employment-based experience and learning to a digital wallet. Initially we plan to issue to ASU Pocket, which is a direct product of the work done by ASU TLN. "A portable, secure and verified digital wallet for learning, work and life." - https://pocket.asu.edu/

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

We discussed the importance of 2 topics when it comes to employee Learning and Employment Records. In order to encourage employers to issue Verifiable Credentials for Employees we need to address:

1. Governance - How can we make sure that the credential is issued by a reliable issuer and the issuer adheres to some standards of excellence when it comes to the credential ?. ALthough efforts such as the X.509 to VC bridge go a long way in allowing Employers to use a well understood process to prove the authenticity of the issuer, there is still a need for Human Trust Networks in order to maintain standards for issuance and increase the value of the credential for the employee. At the end of the day, employee agency of their record of learning and employment can only be achieved if there is a backbone of trust networks backing it.
2. User Adoption - We discussed the slow adoption of VCs even in a university setting both in the USA and Japan. While educational institutions such as ASU can be an anchor to encourage the use of credentials, the true value is in learners getting work based credentials; this is because existing frameworks largely address the need of verifying educational credentials. One idea is to sell the idea that when employees advertise their achievements in linkedin, would it not be nice that it is verified that the employer issued it ?. This helps reduce fraud and avoids besmirching the employer's reputation with false claims. Second, the employer gets a reputation as being a desirable place to work because they recognize employee achievements.

Many thanks to Naohiro Fujie CHair of OpenID Foundation, Japan and Shigeya Suzuki, Project Professor, Keio University for their active participation and thoughtful inputs.

The "Official" Riley Session = What hasn't worked?

Session Convener: Dave Grantham
Session Notes Taker(s):

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

No Notes Submitted

Favorite & Hated Standardization Process Myths & Legends

Session Convener: Heather Flanagan
Session Notes Taker(s): Heather

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

We're collecting the myths about standards development
Myths

- You have to pay to participate in the W3C
  - Invited experts
  - open meeting notes, open GitHub issues
- Only big companies participate (or every individual from the company gets to vote)
  - If big companies aren't on board, then adoption is a problem, but they still only get one formal vote.
  - There does need to be commitment for implementation to get a standard passed
  - In some cases, the collection of smaller members adds up to more than any one bigger member
- SDO $x has full control over all levels of a process
  - protocols often happen at different layers, and an SDO may not own all of them. That said, if there isn't cooperation between SDOs, then working on just one layer doesn't help anyone.
- SDOs have the same incentives
  - they may have business models that influence the decisions
  - they may have specific aspects of the Internet they declare responsibility for
- People have no option if the proposed standard is not something they agree with
  - there are options for them to suggest something different by offering PRs or issues with suggestions.
- Big companies can buy the outcomes
  - more likely, they can put more resources towards the outcomes they want
  - bigger companies often struggle to have a cohesive standards architecture plan because there's too much going on

    - if the developers have a shared vision, they'll make more progress than any one company's goals
    - some SDOs have a limitation in their bylaws as to how many big companies are allowed to be members (ToIP). This can lead to inconsistency, however, as the smaller members tend to be more volatile.
- SDOs are interchangeable
    - they have very different cultures, somewhat different IPR arrangements, different (but sometimes similar) processes
- Every output of an SDO is used (i.e., the law of tech behavior)
    - HAHAHAHAHAH
- SDOs aren't welcome to new members
    - new members that haven't read the history will also feel the frustration of the people who have been arguing all the points and who don't want to argue those points again.
- The lawyers are always listening.
    - OK, this one is true.
- Individuals intentions are always aligned with their employers.
    - Definitely not always true.
    - Generally speaking, this is presented in a politically-correct way to try and indicate when there is individual disagreement for a corporate position.
    - It's hard to differentiate between individuals who happen to work for an org and individuals who are representing their org. The IETF is the only (?) SDO that insists people are participating as individuals.
- Corporations make decisions.
    - Corporations are not people. People make decisions.
- Standards are baked and deployed before they are standardized.
    - It's not uncommon for people to bring code they've tested out in the wild, but there still has to be consensus before a final product.
    - There's always a challenge of whether to build something that's still in flux through the standardization process.
- The only way to participate in an SDO is to physically attend meetings.
    - No, but SDOs do need to accommodate different modalities for how people consume information - some will do better by attending meetings, some will do better reading, etc.
    - Don't forget the value of spending some time early on just listening.
- It's all tech culture; it's all the same.
    - SDO culture (e.g., a drive for consensus across industry) and individual company's are often not the same.
- Only senior people get to participate in an SDO.
    - Unfortunately, often true. But if managers send junior people, they're not only going to increase their bench, they are also going to expose those junior people to how other companies/orgs things (which would be totally useful when dealing with a corporate merger and having experience with how different companies do things).

Bitstring Randomization for Privacy: Why and How

Session Convener: Kevin Dean
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

Python implementation
GitHub repository

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

Presentation here and copied below.

Decentralized Apps: Solid pods & picos

Session Convener: Phil Windley and Bruce Conrad
Session Notes Taker(s):

Tags / links to resources / technology discussed, related to this session:

About Solid pods: https://solidproject.org/
About picos: https://picolabs.io/
Combined: https://picolabs.atlassian.net/wiki/spaces/docs/pages/2460811281/Picos+and+Pods
The student project: https://github.com/Picolab/pico-pods

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

[Phil will link to the slides here]
Contact Bruce for a demo at picolabs@sanbachs.com

DIgital Identity: Who, how, and when does this all come together for people, customers, humans?

Session Convener: Kenneth Gantt
Session Notes Taker(s): Tchaikawsky “Troy” Samuels & Zaïda Rivai

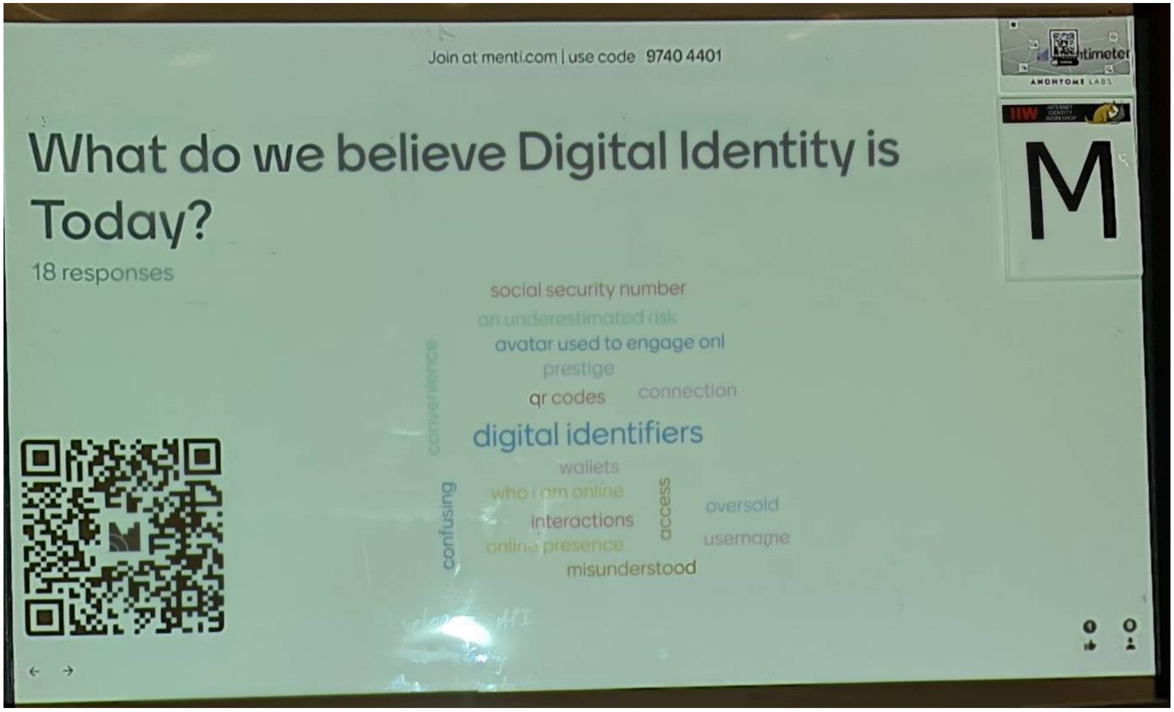
Tags / links to resources / technology discussed, related to this session:

public private partnership

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

Zaïda’s notes:
Erica Conell:

- It’s confusing because of the similarity. Digital identity isn’t a digital identifier. Identity has to do with who they are and get personal and precious.
- A Digital Identifier is just a tool.



Join at menti.com | use code 9740 4401

What do we believe Digital Identity is Today?

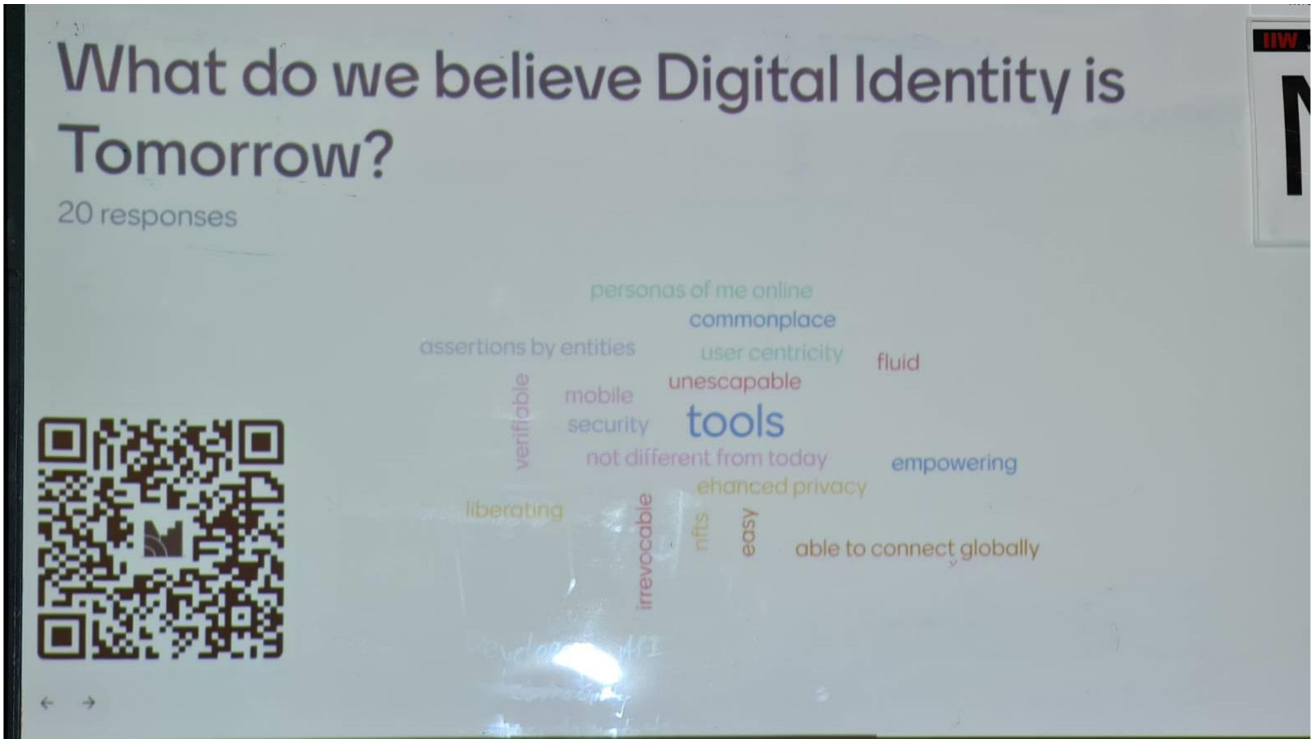
18 responses

social security number
an underestimated risk
avatar used to engage onl
prestige
qr codes
connection
convenience
digital identifiers
wallets
confusing
who I am online
interactions
access
oversold
online presence
username
misunderstood

Ken: Need more discussion on what it is.

- The more access increases liability.
- What about tomorrow?
- Over your lifetime, more documents that you’ll have throughout your lifetime. The evolution of a young person having their car keys all the way through and elderly person, we looked.
- We didn’t do where the digital aspect of your identity, social security etc… We continue on a story and bring in challenges you have to get over.

- What tools are you thinking about? —> Wallets, phone etc…
- Quality of life and quality of work.
- SSO: my laptop for my office is accessible on my phone. II
- Digital Travel:



What do we believe Digital Identity is Tomorrow?

20 responses

personas of me online
commonplace
assertions by entities
user centricity
fluid
verifiable
mobile
unescapable
security
tools
not different from today
empowering
ehanced privacy
liberating
irrevocable
nfts
easy
able to connect globally

Pal Axelsson

- Different way of using privacy. They don’t need to know your bday etc… They just need to know you’re 21+ (ZKP).

Troy Samuels
()
Mentimeter.com session results link:
https://www.mentimeter.com/app/presentation/blb3umaqh4vy8vs45xu3mzn2zjegn3eo

Question 1: What do we believe Digital Identity is TODAY?
Comments::

- Root Identity vs digital identity, so broad we have to narrow it down.
- By default we think of pur physical selves or personas. Its increasingly becoming more about authorization, access and the keywords mentioned in the brief.

Question 2: What do we believe Digital Identity is TOMORROW?
Comments:

- Tools that offer accessibility and life management.
- Digital travel vs Physical travel enabling global connectivity.

- We operate under the privacy act of 1974 which couldn't imagine what life is like today.
- Public announcement "Work a voting station if you have the time to get the experience"
- Tomorrow, identity can be functional in a way that it only reveals the information that is applicable to the event. I.e. when going to a bar, the person should only have to verify their legal age; not address, name, etc… as one would find on a driver's licence.

Question 3:
How does Digital Identity differ within the public/private sectors?

Comments:

- Global Entry is worth the extra $15
- The government follows strict rules with how it can share and use the data.
- 1:1 vs 1: small-N vs 1: large-N
- Is there a biometric consumer agency that can be used to redress the collection of biometric data or otherwise address issues. YES: https://www.dhs.gov/step-1-should-i-use-dhs-trip
- The Goal: We need to get the right people together to build the framework that will get the latest tech into operations within government services sooner than the current life-cycle.

[]

- Absence of technology ()
- When I think about digital privacy, think about ability to temper. Not complete anonymity, but maining certain degree of privacy.

Ken

- How does Digital Identity differ within public/private sectors?
- Differences between "not giving my data to gov cause who knows what they are going to do with it, but put my fingerprint etc… so that I can do this.

Kaliya

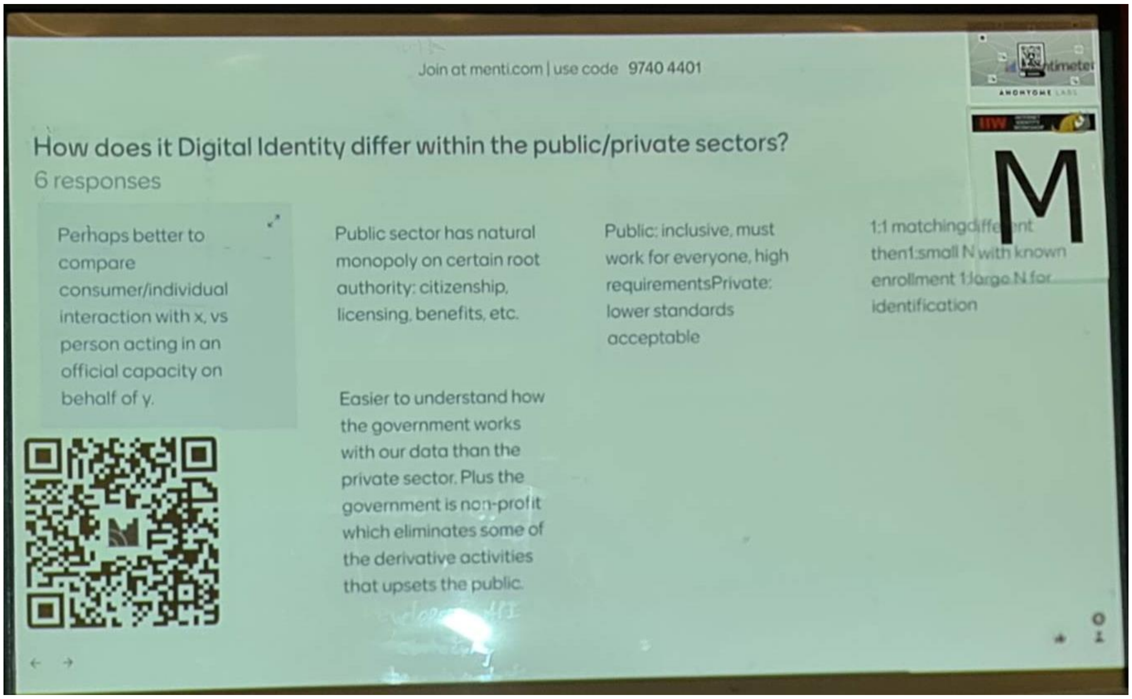
- On device matching

Sam

- TSA: decided to institute.
- Biometrics and walk through

Kaliya

- Digital Identity
- In a yesterday's session they meant " Citizen has a digital record in a DB somewhere".
- "My biometric associated with my ID"
- It means different things



Join at menti.com | use code 9740 4401

How does it Digital Identity differ within the public/private sectors?

6 responses

Perhaps better to compare consumer/individual interaction with x, vs person acting in an official capacity on behalf of y.

Public sector has natural monopoly on certain root authority: citizenship, licensing, benefits, etc.

Easier to understand how the government works with our data than the private sector. Plus the government is non-profit which eliminates some of the derivative activities that upsets the public.

Public: inclusive, must work for everyone, high requirementsPrivate: lower standards acceptable

1:1 matchingdifferent then1:small N with known enrollment 1:large N for identification

Ken

- Face: different from fingerprint. Legal aspect of biometrics; can it go into court.
- Face: 1:1, up to end user

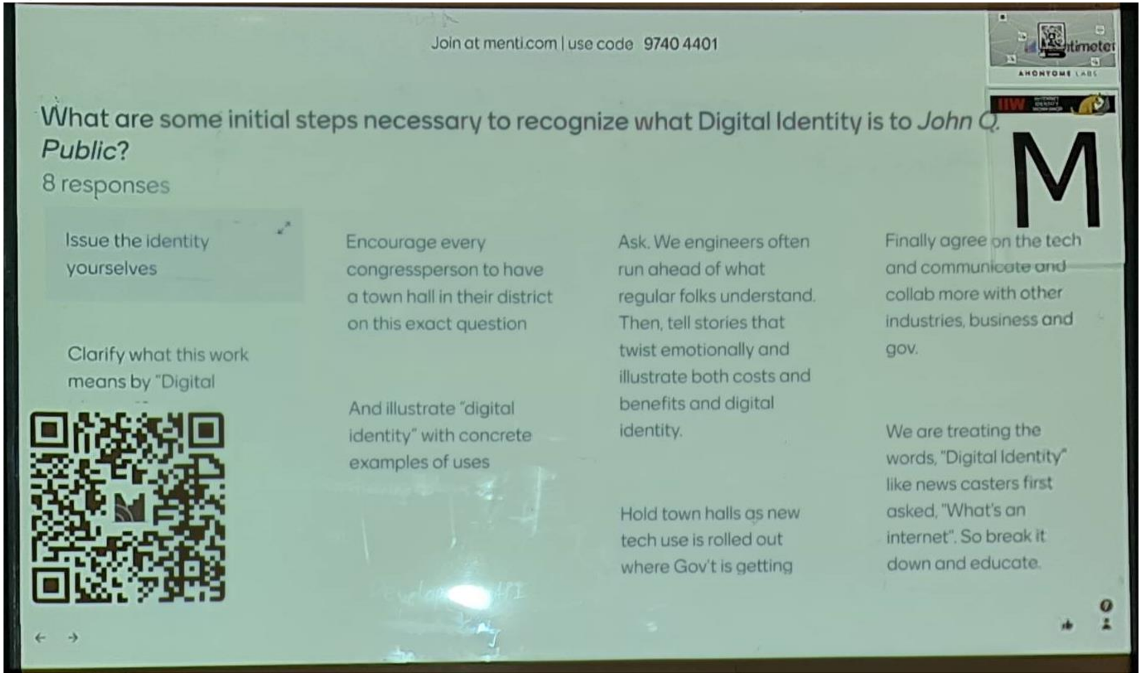
Kaliya:

- No signage, no communication, no one had to scan passport
- Biometrics aren’t going away, but we as an identity management industry must (). The systems should be much more clear about how biometrics work.
- All these tools are great

Ken:

- We don’t have the capability, CBP has the capability

Besides trying to improve, what is it really what we need to be thinking about or do that makes this aspect



Join at menti.com | use code 9740 4401

What are some initial steps necessary to recognize what Digital Identity is to *John Q. Public*?

8 responses

Issue the identity yourselves

Clarify what this work means by "Digital

Encourage every congressperson to have a town hall in their district on this exact question

And illustrate "digital identity" with concrete examples of uses

Ask. We engineers often run ahead of what regular folks understand. Then, tell stories that twist emotionally and illustrate both costs and benefits and digital identity.

Hold town halls as new tech use is rolled out where Gov't is getting

Finally agree on the tech and communicate and collab more with other industries, business and gov.

We are treating the words, "Digital Identity" like news casters first asked, "What's an internet". So break it down and educate.

The 4 Parts of Access Control

Session Convener: Alan Karp (alanhkarp@gmail.com)
Session Notes Taker(s): Alan Karp

Tags / links to resources / technology discussed, related to this session:

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

Access control is divided into 4 parts denoted IZNA

I: Identification - assigning a responsible party, usually a person
Z: authoriZation (authZ) - specifying the rights of the responsible party
N: autheNtication (authN) - allowing a program to prove it represents the responsible party
A: Access decision - deciding if a request is authorized

Where and when each step is done depends on both the context and the access control approach.

Consider an example of an employee of Acme, Inc., Alice, using a service provided by Salesforce. Where and when does each part of the access control process get done?

Identification: This step was done when Alice was onboarded by Acme. That means it was done in the Acme domain before she made any request of the Salesforce service.

Access decision: Clearly, there's no way to know if a request is authorized until it is made, and most service providers wouldn't trust anyone else to decide for them. Hence, the access decision is made at request time in the service domain.

When and where the other two steps are done depends on the access control mechanism.

In an identity-centric approach, such as federated identities or some authz systems, such as Cedar, Alice presents her authentication along with her request. A component at Salesforce looks up the policy associated with Alice's authentication to decide if her request is authorized. In this case, the authentication and authorization steps are done in the service domain at the time the request is received.

In an authorization-centric approach that uses access tokens, Salesforce has given Acme an access token granting permission to the services covered by its contract with Acme. Alice authenticates to Acme and receives one or more access tokens representing her authorizations. Alice presents her access token to Salesforce when making her request, which Salesforce uses to decide if her request is authorized. In this case, the authentication and authorization are done in Alice's domain before the request.

There are significant advantages to the authorization-centric approach.

- There’s no need to federate identities.
- Attenuated delegation is easy.
- Acme does not need to coordinate its policies with anyone else.

Using the authorization-centric approach doesn’t mean you have to throw out your existing infrastructure. For example, you can use your Role-based policy to hand out access tokens.

What is the Naivest Identity Solution you have heard lately?

Our Opening Question that attendees discussed and shared around tables before Opening Circle

User-Name and Password for nearly 30 years
Too Hard: Something easy to remember but hard to guess REALLY?
Too Easy: Basic Familiar stuff - for developers at least

FaceID

SSIN - super stupid identity number - e-mail privat key to user

Any solution which does not address the fact that we will soon be outnumbered by Artificial humans (bots) 100:1

Contact management system used solely as the trusted attribute management system

Home organizations thinking that users don't find other ways to login if the organization doesn't allow users to cooperate over organizations

Public cloud is a safe place for your sensitive personal data.
People misunderstood what cloud actually means. Cloud is just someone else's servers. So how do you know where your data is and who looks after it.

Input Credentials into ChatGPT AS if valid

Louisiana Wallet that (as of '22) provides a credential that calls/tracks every use of the credentials holds [It will be shut down when people fight back - it is wrong]

Using google as the second auth for a product.
Relying on google to do the right thing and no way to validate.

Just trust Google to manage your Identity
A - is it real
B - is it verified
C - can you trust it
D - Can you trust google and what they're doing.

Privacy Personal OIDC by Multi-Party Computing via Tore using Authorization code of Gov

Mobile wallet for smart phones to villages - they don't have phones

A Credit Union authenticates withdrawals from a paper card with account number on it and a (physical) signature.

Phone numbers unable to truly verify the other person, the only means is voice not AI/spam resistant and not sybil resistant.

x.com wants to charge for likes + post for new accounts to ensure proof of humanity

Twitter blue checkmark - money should not be able to bury such identity. Conflict of interest - dehumanizing reduces meaning of communication

Social media identity AKA twitter/x Bots

Blue Check mark on X -

IRS Crypto Broker Rule
Requires people to give personal information redundantly to many crypto companies increasing risk data theft or loss of personal info rather than other secure methods

AI drone that attacks an enemy with stored identifiers

The idea that DIDs can serve as universal identifiers is naive

- DIDs are an anchor for attestations
- DIDs as universal identifiers would be too much correlation across use case domains
- The work required to retrofit existing identification frameworks is far to expensive

Building Solutions before understanding problems "if you build it they will come"
Crystal Towers vs Mud Pits

X509 Certificates for everyone

1. Does not scale
2. Too expensive
3. Centrally Governed
4. Doesn't Interoperate
5. Difficult to provision

Uber driver says you are so and so when they pick you up

UnSAFE DID SEX!!!!
DID: Web
Implementing DID:WEB and thinking you have sufficient security.
But that is getting fixed with DID high assurance and DID:TDW (aka DID:SCID) and DID:WEBS

If only everyone adopted my tech everything would be perfect. Its frustrating people won't come along. Bonus solve homelessness with NFT

Using Google FB etc as Identity system for login to multiple accounts. They own it. You can loose it if you are kicked off their platform.

An Appostille (Misspelled) as any sort of reasonable official documentation that should be relied on. Or a Digital Signature with a self-signed cert (an individual)

Consumers -> Executives don't understand identity

Non-directed passwords that allow consumers to create weak passwords.

Pleas epic a user name

Implicit trust that people are telling the truth during initial greetings

Magic links used for IIW Agenda

NFTS

Paper utility bills as proof of address

Paperless email account management (reliance on digital only solutions)

Putting PII on a blockchain

Email Magic Link + Passkey

- Communication channel to the user
- SSO via passkey
- Never have to login again with this device

That there will ever be a complete ID solution that starts with a giant

We are going to implement PAM in 6 months

The NSW state government (in Australia) digital ID are requiring an active connection to show your licence. If you have no internet or the NSW servers are down you have no ID

Considering token exchange (eg JWT) leaving to the application developer to introduce risk if done in clear text with HTTP. There is always another layer of security required that is fundamental to ensuring tokens aren't exposed eg HTTPS is fundamental to prevent Man-in-the-middle

Commercial director asking "how can we use attributes from a decentralized ID for marketing?"

Australian Government "skills passport" being on centralized platform

An institution sending a photo of their employee ID as an "identity verification"
Institutions not being ready or able to verify themselves in a phone call (not new but still a problem!)

Multi-Factor TOTP using Mobile phone number

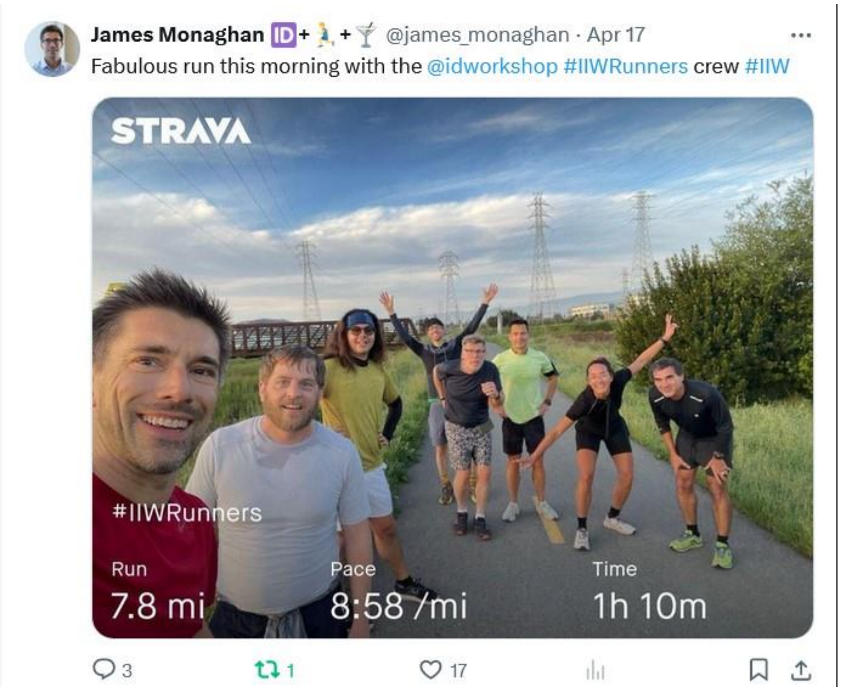
Worldcoin:

- Naive to think they can get 100% of living humans.
- Naive to think it won't be abused
- Naive to believe they can reach reasonable accuracy for 100%
- Naive to think permanent life-long identifiers are a good idea

I don't want the owners of identity platforms / infrastructure to appropriate and use my identity for their benifit.

Too many to ennumerate but sourcing your identity encrypted on a blockchain

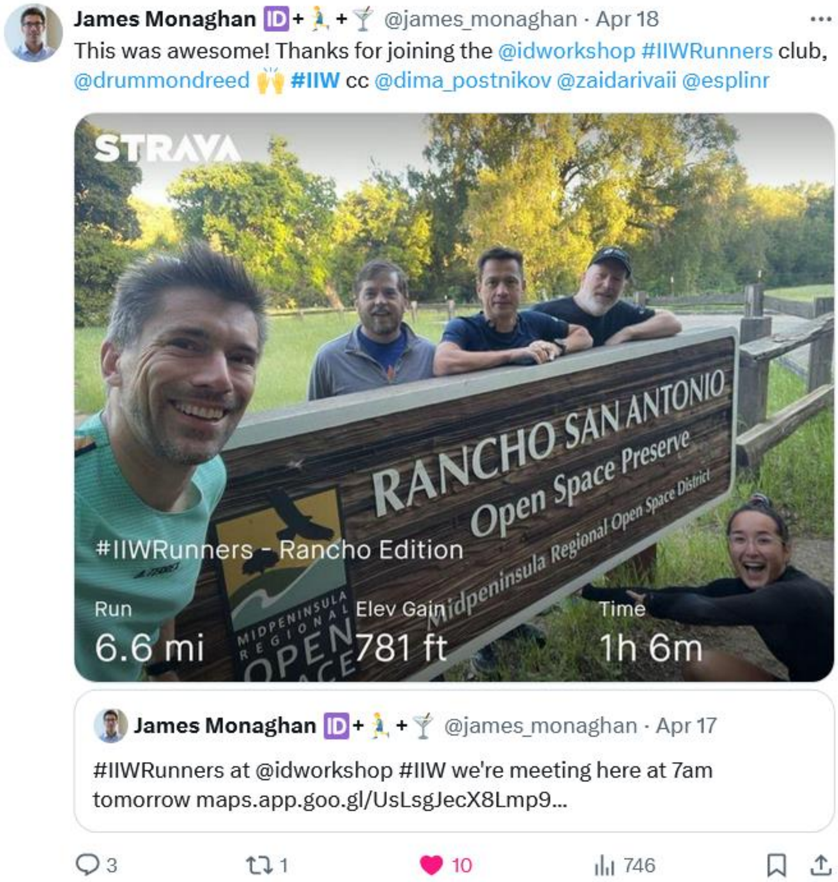
The answer to all problems "use DIDCOMM"



James Monaghan 🆔+🏃‍♀️+🍸 @james_monaghan · Apr 17

Fabulous run this morning with the @idworkshop #IIWRunners crew #IIW

#IIWRunners Club Run in #OpenSpace



James Monaghan 🆔+🏃‍♀️+🍸 @james_monaghan · Apr 18

This was awesome! Thanks for joining the @idworkshop #IIWRunners club, @drummondreed 🙌 #IIW cc @dima_postnikov @zaidarivaii @esplinr

STRAVA
#IIWRunners - Rancho Edition
Run
6.6 mi
Elev Gain
781 ft
Time
1h 6m
RANCHO SAN ANTONIO
Open Space Preserve
Midpeninsula Regional Open Space District
MIDPENINSULA REGIONAL OPEN SPACE

James Monaghan 🆔+🏃‍♀️+🍸 @james_monaghan · Apr 17

#IIWRunners at @idworkshop #IIW we're meeting here at 7am tomorrow maps.app.goo.gl/UsLsgJecX8Lmp9...

Demo Hour / Wednesday April 17

Thanks to our Demo Hour Sponsor!

The **IIW Speed Demo format** involves each person Demoing giving a **5-minute demonstration** of their service, product, physical device, **10 times** to 10 different small groups, rotating through to view them over the course of the hour. **Demo Hour takes place on Wednesday after lunch from 1:30 - 2:30.**

There will be 20 Demo Tables in the Grand Hall each with a # Sign on it that corresponds to the Demo taking place at that table. People rotate through the tables/Demo's in a self-organized way ~ that's a little loud, seemingly chaotic and free flowing, but works!

See the list of Demos via the Demo List below and decide ahead of time the Demo's you'd like to see. You'll be able to see 10 of the 20 Demo's over the hour.

TABLE	Demo Description	More Info
#1	**OpenID Foundation conformance tests for OpenID for verifiable credentials:** Joseph Heenan URL: https://openid.net/how-to-certify-your-implementation/ OIDF has tests that issuers and wallets correctly & securely implement OpenID for Verifiable Credential Issuance / OpenID for Verifiable Presentation specifications, with ISO mDL or SD-JWT VC - we demo them, explain their limitations and how you can test your own implementations.	More Info Here
#2	**Infisign Inc./ Infisign Identity and Access Management:** Aditya Santhanam (CPO, Infisign) URL: - https://www.youtube.com/watch?v=gcAEEgfA7js Infisign is a cutting-edge identity and access management (IAM) platform that revolutionizes digital security by leveraging decentralized identity, passwordless authentication, federation, and privileged access management (PAM) capabilities. With its unique approach, Infisign addresses the challenges of traditional IAM systems and offers a comprehensive solution for modern identity management. We will showcase its Verifiable credentials issuance and wallet store and also demonstrate selective disclosure and verification using OpenID for VP protocols.	More Info Here
#3	**Trinsic Connect - Reusable identity verification using many types of trusted credentials:** Michael Boyd URL: trinsic.id/connect - product info & pearbnb.app - demo site Showcasing how Trinsic Connect can verify new users from a number of sources including digital identity wallets, eID schemes, mDLs and verifiable credentials.	More Info Here

#4	**Cardano Foundation - Keri Mobile Wallet:** Thomas Mayfield, Fergal O'Connor, Jaime Caso URL: https://identity.cardanofoundation.org/ Demonstration of KERI mobile wallet multi-sig AID and ACDC issuance. Demonstration of KERI secure tunnel browser extension.	More Info Here
#5	**2060.io - Enabling trust in B2C conversational services**: Fabrice Rochette & Ariel Gentile URL: https://2060.io Trust is becoming a serious issue in our day-to-day digital life. Discover how to provide secure chatbot-based Decentralized Trusted Services.	More Info Here
#6	**Credence ID:** Navya Kumar & Yash Shah *URL:* https://credenceid.com/digital-id Verify with Credence™ (VwC™) is a digital ID verification solution designed for relying parties to accept and verify reusable digital IDs, such as Mobile Driver's Licenses (mDLs) issued by various states and presented via digital wallets. The VwC™ platform comprises Credence ID IoT hardware device (Tap2iD™), Mobile Apps (Tap2iD Mobile™), and SDK for integrating relying party software, supporting multiple use cases. It ensures secure and privacy-preserving verification of digital ID documents, offering a smooth and intuitive user experience.	More Info Here
#7	**GoDiddy.com - Universal DID Services:** Markus Sabadello - Danube Tech **URL:** 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 & Registrar.	More Info Here
#8	**cheqd Creds Studio:**Alex Tweeddale URL: https://studio.creds.xyz/ No-code issuance platform for Verifiable Credentials. Claim your IIWXXXVIII credential and issue a credential to another person at the event.	More Info Here
#9	**The Vngle Grassroots News Agency (nonpartisan org):** Blake Stoner - Founder of Vngle and Journalism Fellow at Stanford & USC's Starling Lab for Data Integrity URL: www.vngle.com Decentralized provenance-based grassroots reporting on the 2024 American Battleground States Before the election, Vngle seeks to get more citizens involved in using provenance tools to help report on underrepresented issues that need more coverage. We want to demo & critique our process as we expand how we source verified local info for newsrooms from underreported areas.	More Info Here
#10	**Procivis AG/Procivis One (360° Decentralized Identity Solution):** Kai Wagner, Head of Products & Partners URL: https://www.procivis.ch/procivis-one Procivis One, the multi stack Identity solution built with flexibility, performance, and compliance in mind. Its future proof API allows integrating identity interactions using any kind of Credential Format, Protocol, Identifier, etc..	More Info Here
#11	**Curity Identity Server - Verifiable Credential Issuance and Presentation:** Pedro Felix and Tomas Micko URL: https://curity.io/ Showcase verifiable credential issuance and presentation using the OpenID DCP protocols, including a demo wallet.	More Info Here
#12	**Dfinity Foundation, demoing verifiable credentials on a decentralized authentication platform:** Kai Peacock URL: https://identity.ic0.app Internet Identity is an authentication platform for decentralized identities. It allows apps to "Log in with Internet Identity", receiving an anonymous identity on each website for privacy purposes. To solve the problem of sharing information across websites that a user has logged into, we have introduced Attribute Sharing, a standardized strategy for sharing verifiable credentials across platforms, with user approval. I'll demo an example of KYC and age verification.	More Info Here

#13	**Csign, built by Good Future, LLC:** Jon Bauer URL: https://www.csign.io Csign is a platform for 100% private signing, certifying and verifying agreements between parties using SSI and Blockchain	More Info Here
#14	**AyanWorks: Bhutan National Digital Identity & CREDEBL Platform:** Ajay Jadhav, Kalyan Kulkarni **URL:** https://credebl.id **Demo Description:** This demo will help explain how the Bhutan National Digital Identity has rolled out Foundational Identity & other functional credentials by using CREDEBL Platform.	More Info Here
#15	**demo.didcomm.org - In Browser DIDComm Education and Testing Tool:** Colton Wolkins, DIF DIDComm Users Group co-chair **URL:** http://demo.didcomm.org The DIDComm demo is a fully browser based tool that demonstrates the basics of DIDComm. We'll demo the tool, what it teaches, and how it can be used for light testing.	More Info Here
#16	**moda, Ministry of Digital Affairs, Taiwan; Taiwan DID-Wallet Project;** mashbean (Yen-Lin Huang) **URL:** The TW-DIW Project Draft (English, Chinese) https://moda.gov.tw/en/digital-affairs/democracy-network/operations/6621 Taiwan is initiating a national-level DID/VC project called the TW-DIW Project. As part of our digital public infrastructure, we are formulating domestic verifiable credential standards to assist various government departments in issuing VCs and integrating them into wallet services. A demo will be presented outlining preliminary project details.	More Info Here
#17	**The Planet Earth Society Inc:** Blaine Garst, Wizard URL: Http://theplanetearthsociety.com Sign up for The Dew - a point to point hardware personal everything system. Space, Grid, Social - we need identity from our friends & neighbors!	More Info Here
#18	**Polygon ID - ZK Powered Identity Tools:** Otto Mora **URL:** https://www.polygonid.com/ Polygon ID is a set of tools for developers that can be used to facilitate trusted and secure relationships between apps and users. It enables the exchange of verifiable credentials and private information secured by zero knowledge cryptography and the blockchain.	More Info Here
#19	**FISE Technologies, demo-ing platform functions:** Nara Lau, CEO & Founder **URL:** DNS: https://fiseportal.com/ ENS: fisetech.x Create your digital identity, and control your data in less than 2 minutes.	More Info Here
#20	**Turtle Shell as SensiNM, LLC:** Moises E. Jaramillo URL: https://www.youtube.com/watch?v=4FJXnpMU2JQ A Portable Personal Data Management Wallet and Platform which allows us to own, manage and view all our data regardless of its type.	More Info Here

AYANWORKS @ayanworkstech · Apr 19

Sharing a sneak peek from our demo table at the @idworkshop!

Our team is showcasing the future of innovative #digitalidentity solutions and paving the way for securely building #digitaltrust. Explore the snapshots capturing moments of collaboration and discovery.

Kalyan Kulkarni and 5 others

Diversity and Inclusion Scholarships

Thank You to Our
Diversity & Inclusion Scholarship Sponsors
SpruceID and tbd

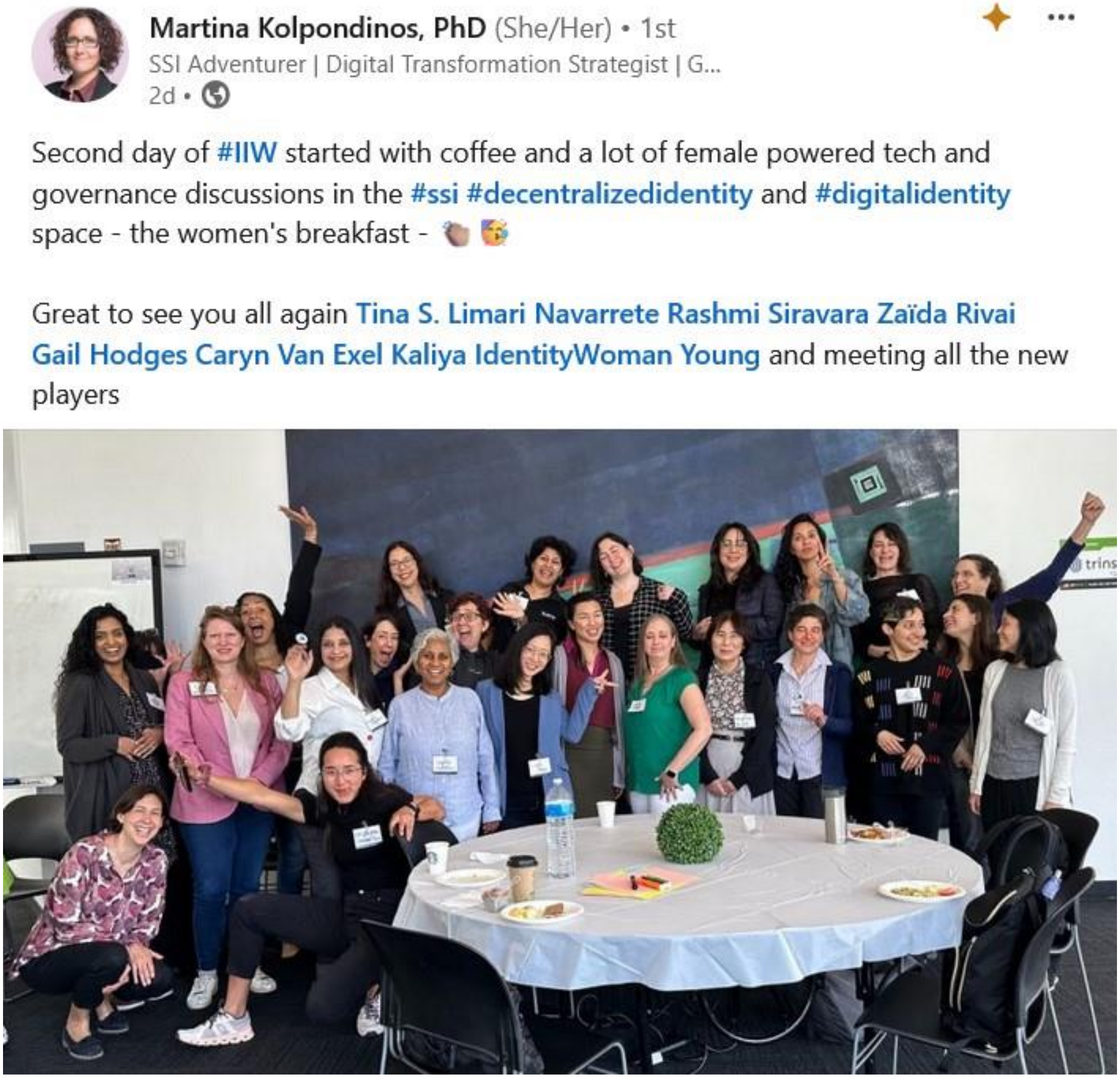
Through these sponsorships we gave reduced price & complimentary tickets and/or travel and lodging reimbursement to new attendees to IIW who otherwise would not have been able to attend and participate.

> *We care about increasing support for women, black, and other starkly underrepresented technologists in our ecosystem. We can't build identity for everyone when demographics are homogeneous.*

Several of our IIWXXXVIII Scholarship Recipients

Read Blake Stoner and Dolores-Mai Macaulay LinkedIn Posts about their experience

Thank You to our Women’s Breakfast Sponsor Curity



Martina Kolpondinos, PhD (She/Her) • 1st
SSI Adventurer | Digital Transformation Strategist | G...
2d •

Second day of #IIW started with coffee and a lot of female powered tech and governance discussions in the #ssi #decentralizedidentity and #digitalidentity space - the women's breakfast - 👏 🥳

Great to see you all again Tina S. Limari Navarrete Rashmi Siravara Zaïda Rivai Gail Hodges Caryn Van Exel Kaliya IdentityWoman Young and meeting all the new players

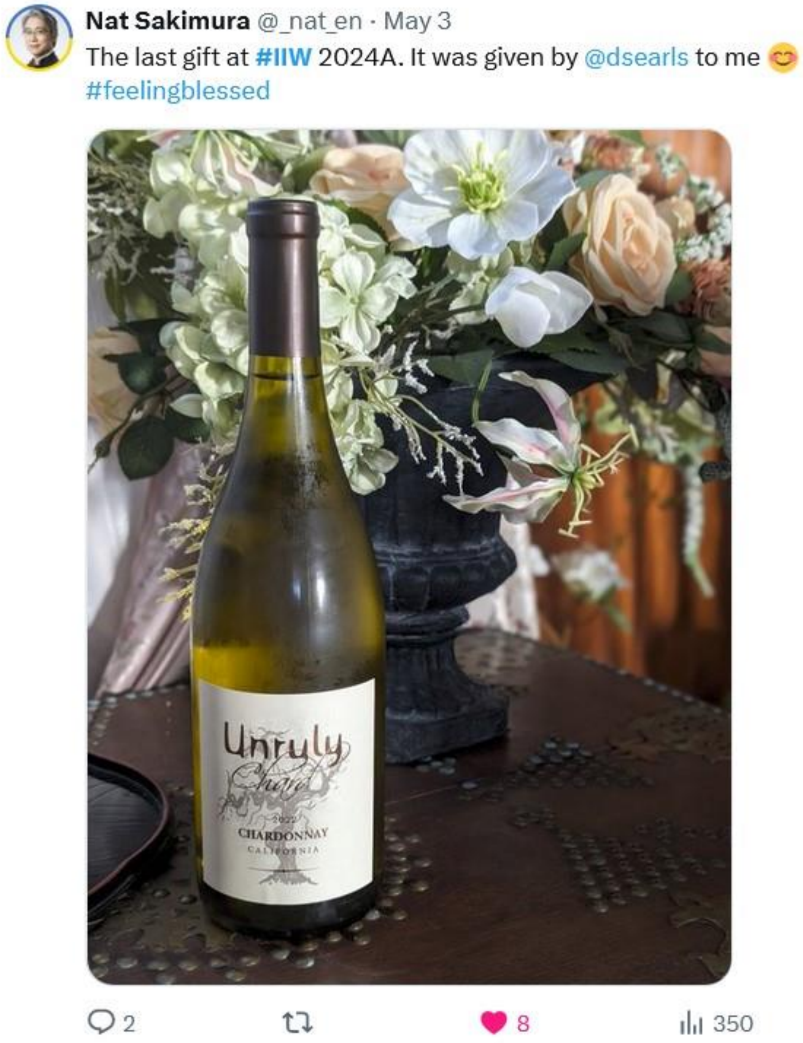
Event Photos taken by Doc Searls

Doc Searls has several hundred candid photos from IIW #38 on his Flickr account

Day 1:
https://www.flickr.com/photos/docsearls/albums/72177720316609417

Day2:
https://www.flickr.com/photos/docsearls/albums/72177720316577534

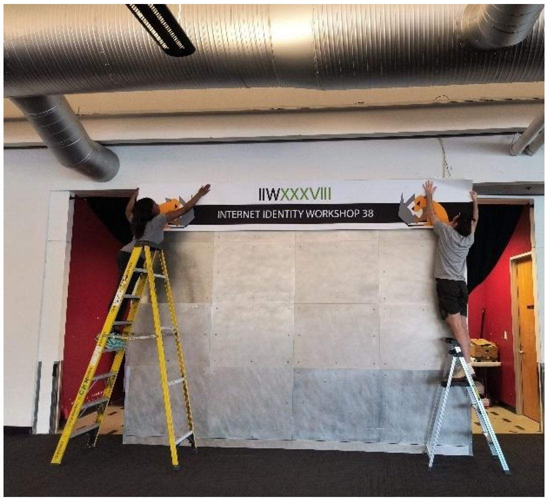
Day 3:
https://www.flickr.com/photos/docsearls/albums/72177720316988073/

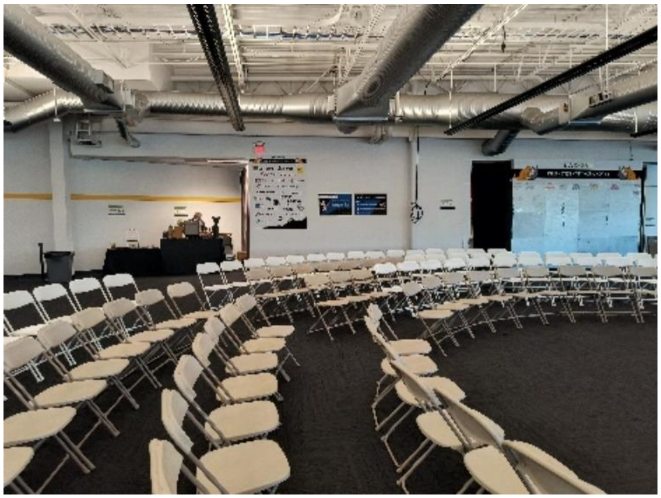


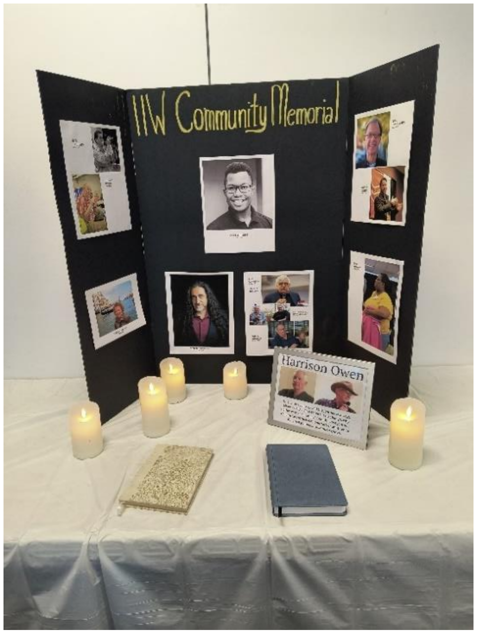
Nat Sakimura @_nat_en · May 3

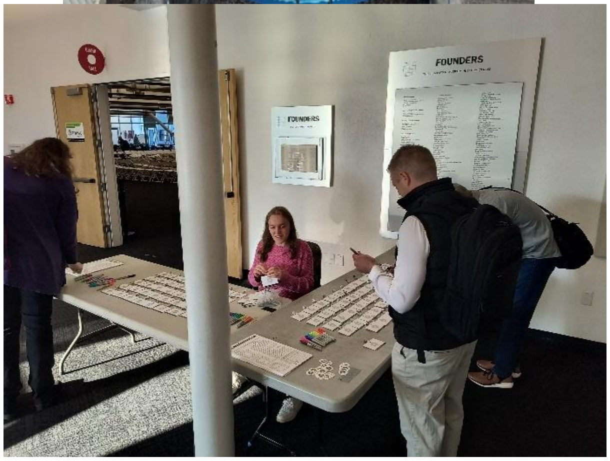
The last gift at #IIW 2024A. It was given by @dsearls to me 😊 #feelingblessed

Behind The Scenes









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/

Upcoming IIW Inspired™ Regionally Focused OpenSpace unConference Events

Digital Identity unConference Europe

Fostering Collaboration on the digital identity between governments, citizens, and companies across Europe

June 17 – 19, 2024 #DICEurope 2024 Zurich

With Our Partner TrustSquare

Did:unConf Africa

Bridging the Digital Identity Gap in the SADC Region

September 25 – 27, 2024 Cape Town, South Africa

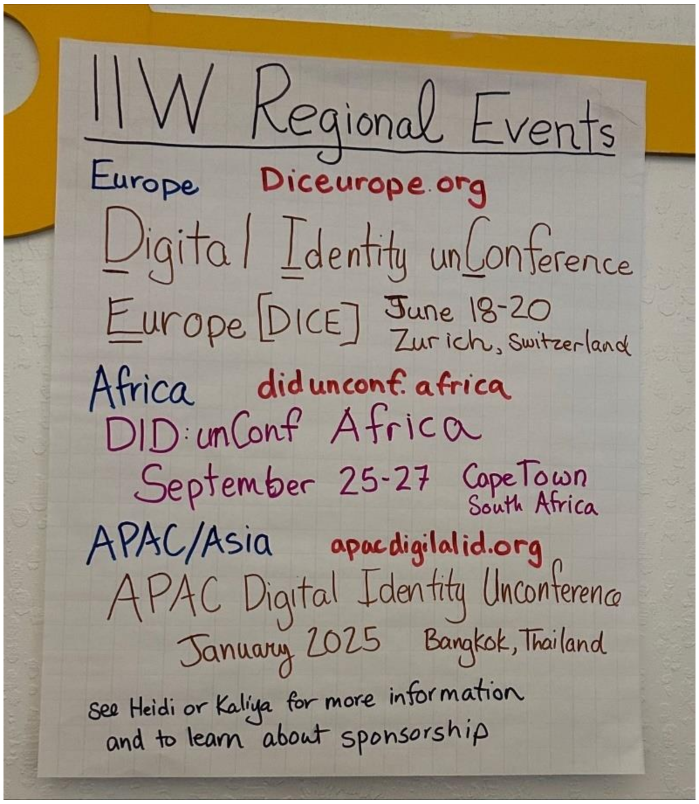
With Our Partner DIDx

APAC Digital Identity unConference

Fostering innovation and collaboration between emerging digital identity companies and projects across the APAC region

January 22 – 24, 2025 Bangkok, Thailand

With Our Partner NewLogic



IIW Regional Events

Europe Diceurope.org

Digital Identity unConference

Europe [DICE] June 18-20

Zurich, Switzerland

Africa didunconf.africa

DID:unConf Africa

September 25-27 Cape Town

South Africa

APAC/Asia apacdigitalid.org

APAC Digital Identity Unconference

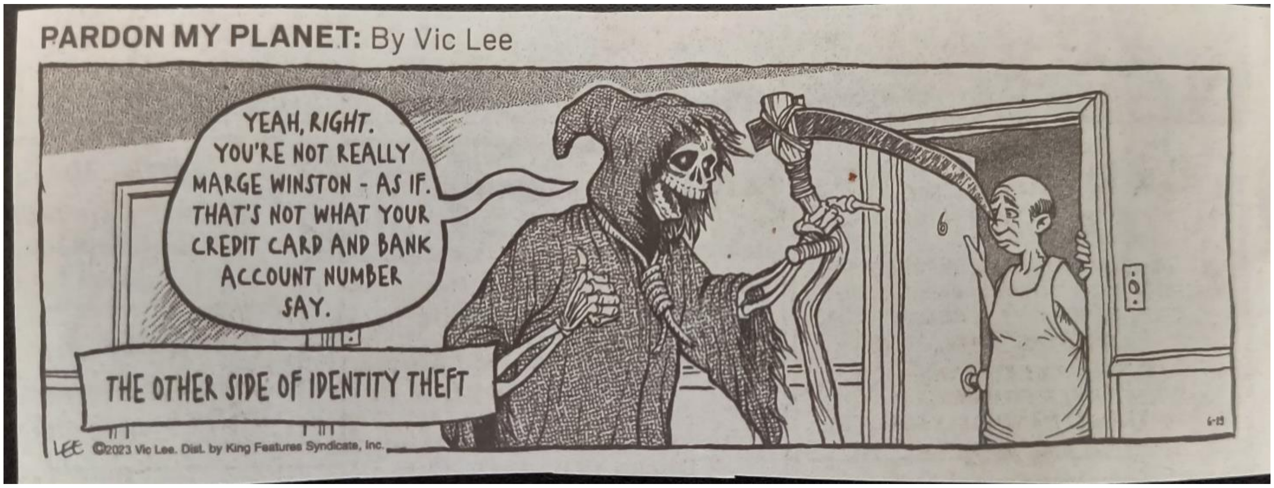
January 2025 Bangkok, Thailand

see Heidi or Kaliya for more information

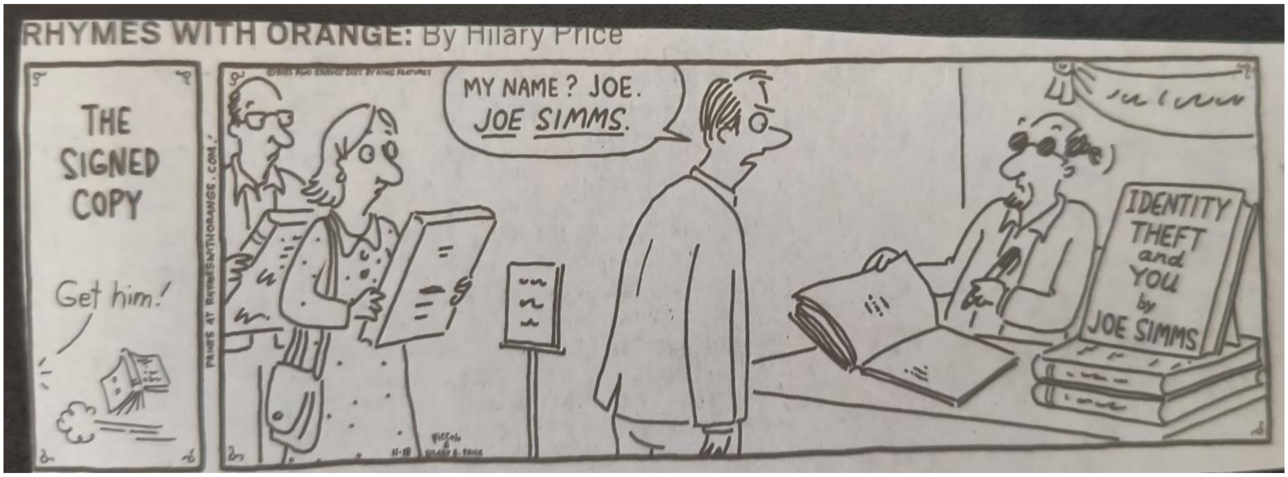
and to learn about sponsorship

Identity 'Funnies' (comic strips) Shared by Alan Carp!

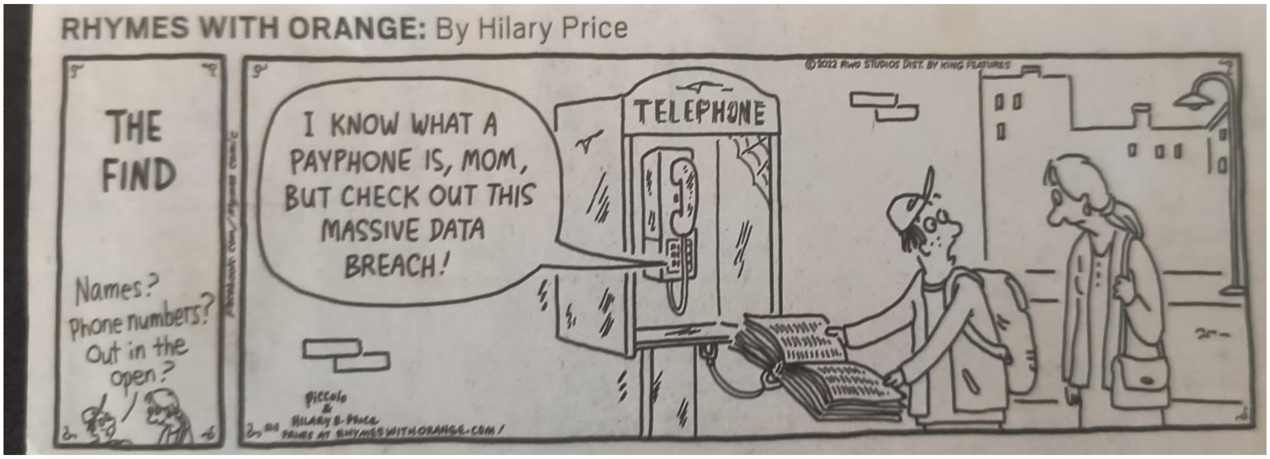
The Other Side of Identity Theft


PARDON MY PLANET: By Vic Lee
YEAH, RIGHT. YOU'RE NOT REALLY MARGE WINSTON - AS IF. THAT'S NOT WHAT YOUR CREDIT CARD AND BANK ACCOUNT NUMBER SAY.
THE OTHER SIDE OF IDENTITY THEFT
6
LEE ©2023 Vic Lee. Dist. by King Features Syndicate, Inc.

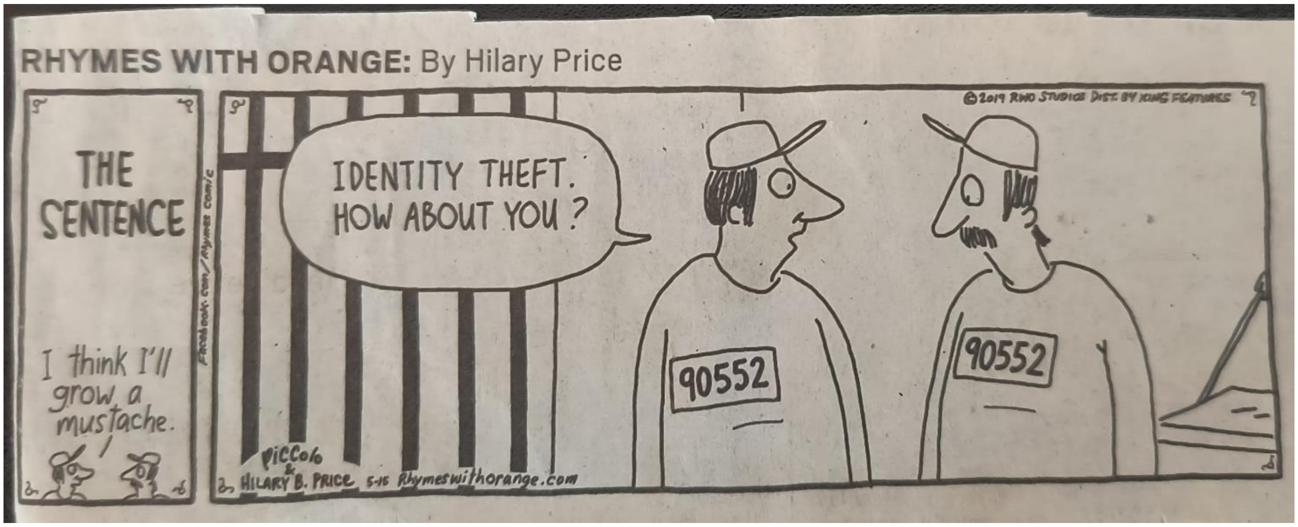
My Name? Joe. Joe Simms.


RHYMES WITH ORANGE: By Hilary Price
THE SIGNED COPY
Get him!
MY NAME? JOE. JOE SIMMS.
IDENTITY THEFT and YOU by JOE SIMMS
PRINTS AT RHYMESWITHORANGE.COM!

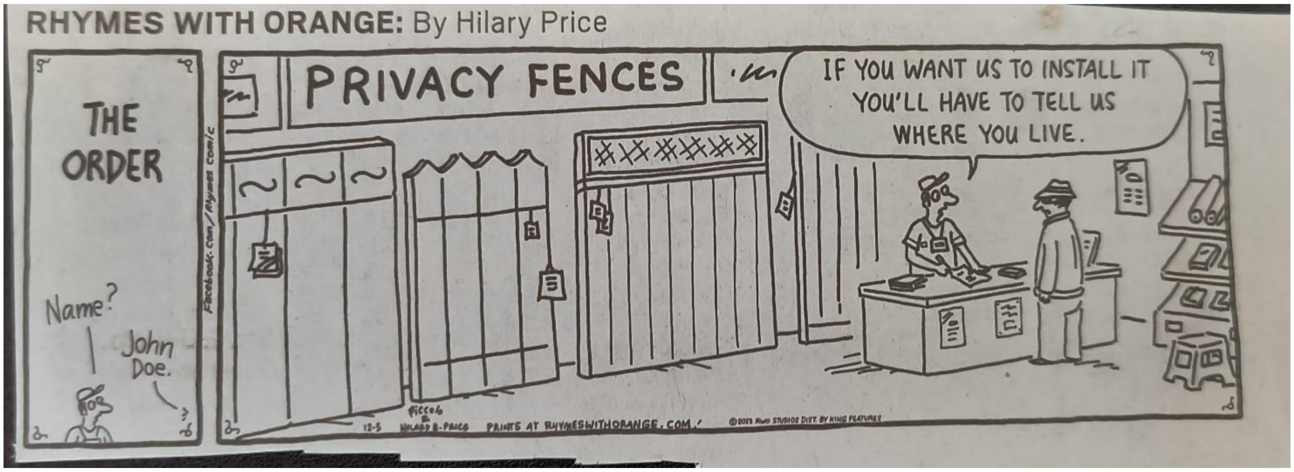
Massive Data Breach!


RHYMES WITH ORANGE: By Hilary Price
THE FIND
Names? Phone numbers? Out in the open?
I KNOW WHAT A PAYPHONE IS, MOM, BUT CHECK OUT THIS MASSIVE DATA BREACH!
TELEPHONE
©2022 RWO STUDIOS DIST. BY KING FEATURES
PICCOLO & HILARY B. PRICE
PRINTS AT RHYMESWITHORANGE.COM!

What are you in for?


RHYMES WITH ORANGE: By Hilary Price
THE SENTENCE
I think I'll grow a mustache.
Facebook.com/Rhymes comic
IDENTITY THEFT. HOW ABOUT YOU?
90552
90552
PICCOLO & HILARY B. PRICE 5-15 Rhymeswithorange.com
©2019 RWO STUDIOS DIST. BY KING FEATURES

You have to tell us where you live.


RHYMES WITH ORANGE: By Hilary Price
THE ORDER
Name?
John Doe.
Facebook.com/Rhymes comic
PRIVACY FENCES
IF YOU WANT US TO INSTALL IT YOU'LL HAVE TO TELL US WHERE YOU LIVE.
PICCOLO & HILARY B. PRICE 12-5 PRINTS AT RHYMESWITHORANGE.COM
©2023 RWO STUDIOS DIST. BY KING FEATURES

Hope to See you October 29 - 31, 2024

IIWXXXIX / The 39th Internet Identity Workshop

REGISTRATION OPEN in JUNE

www.InternetIdentityWorkshop.com

Heidi Nobantu Saul 🐝🦋 @nobantu · Apr 18

IIW38 is a wrap ~ thanks to all participants for co-creating another great workshop!

See you in October with your Halloween 🎃 Costumes 👻

#iiw @idworkshop #iiw38