IIWXLI

INTERNET IDENTITY WORKSHOP 41

October 21–23, 2025

Book of Proceedings

Computer History Museum / Mountain View CA

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

Thank You! Documentation Center & Book of Proceedings Sponsors: GLEIF and Spherical Cow Consulting

Contents

Digital Identity Advancement Foundation
1,183 followers
3w •

We had 4 DIAF winners at the **Internet Identity Workshop** last week! **Frederico Schardong**, **Chris Phillips, CIDPRO**, **Apoorva Deshpande** (2024-5 Vittorio Bertocci Award winners) and **Sachin Mamoru** (2025 Kim Cameron Award winner) were all there, calling sessions and collaborating with peers. We look forward to seeing what happens next in their projects! And we are so grateful for the partnership with IIW **Kaliya Young Doc Searls Phil Windley**

Ian Glazer Arynn Crow Allan Foster Sarah Cecchetti Michael Jones

Alex Chiaranda • 3rd+
Senior System Architect | Forensic Computer ...
3d •

Last day of IIW 41 (Internet Identity Workshop) 💡

It's hard to put into words what it feels like to be here for the first time. These past few days have been filled with meaningful conversations, new friendships, and eye-opening insights about the future of digital identity. There's something truly special about being surrounded by people who are passionate, curious, and willing to share and build together. I'm leaving inspired — and grateful for every chat, idea, and connection that happened here.

I can't wait for the next one!

#IIW #IIW41 #DigitalIdentity #Community #Learning Int Identity Workshop

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 21st year and is Co-produced by Phil Windley, Heidi Nobantu Saul and Kaliya Young. IIWXLII (#42) will be April 28 - 30, 2026.

 Phil Windley @windley / Co-Founder of the Internet Identity Workshop

Phil Windley 's IIWXLI Report!
https://www.technometria.com/p/internet-identity-workshop-xli-report

🐝 Summary: IIW XLI brought 287 people together at the Computer History Museum in Mountain View for three days of dynamic sessions on identity, personal agents, and the agentic internet. As always, the agenda was created live each morning, reflecting the priorities of a passionate, deeply engaged community. 🦋

Thank You to our Sponsors!

IIW 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.

Coming Up!

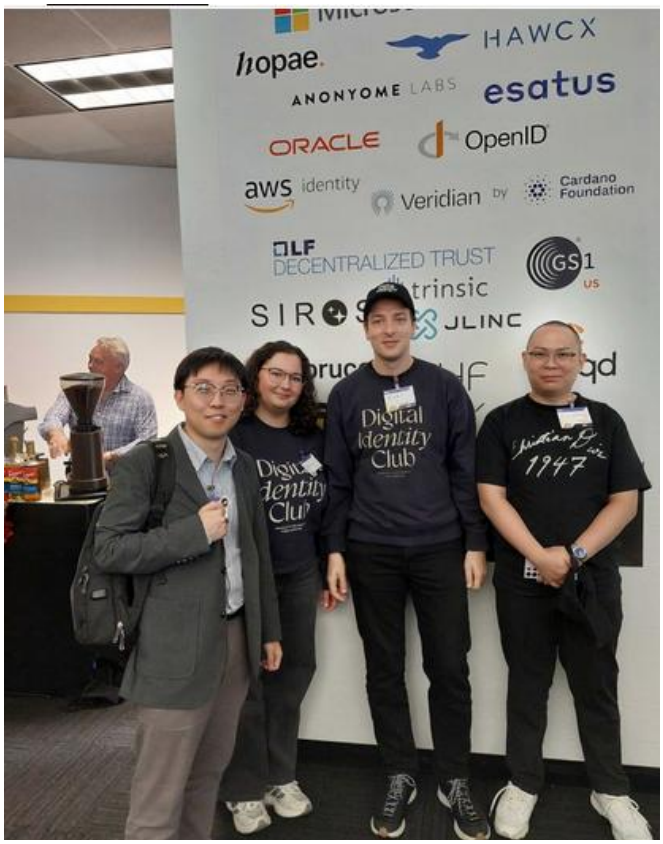
IIWXLII #42
April 28 - 30, 2024 / Mountain View, CA
https://internetidentityworkshop.com/

Paul Ashley, P... • 2nd **Connect** ...

Digital Identity at Anonyome ...

4d •

Great to back at the **Internet Identity Workshop**. Catching up on the latest developments in digital identity. Proud that **Anonyome Labs, Inc.**is a sponsor again.



Hopae
1,714 followers
4d • Edited •

Big steps toward more trusted and interoperable digital identity at the **Internet Identity Workshop**.

Our team is at IIW, joining insightful sessions on web-based open-source identity wallets, OpenID4VC, and the upcoming HAIP 1.0 launch, all marking strong progress toward a more trusted digital identity ecosystem.

We also shared about our work on the K-ARF, South Korea's framework driving global alignment in digital identity. This initiative brings us a step closer to cross-border interoperability.
Learn more: **https://lnkd.in/gasA-9Rh**

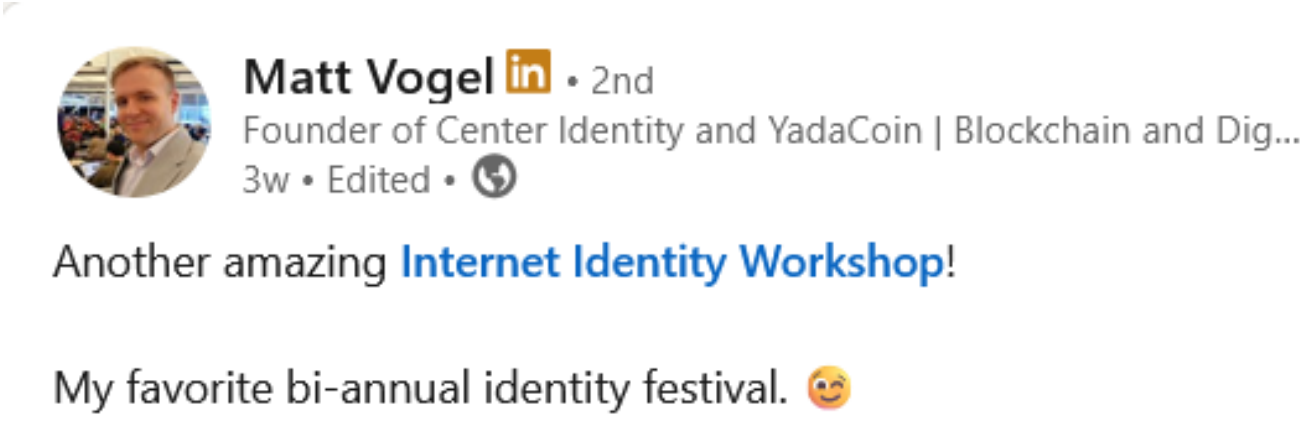
👋 If you're around, come say hi to **Lukas.J Han**, **Alena Kazakova**, **Bart van der Geest**, **Jinyoung Jun**.

IIWXLI 3 Day Schedule

TUESDAY, October 21 / Doors Open at 8:00 AM for Registration Barista! Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme Donuts - Fruit - Cheese - Boiled Eggs 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 Drinks by AWS Identity & Dinner by You 6:00 **NEW LOCATION!** *Michaels @ Shoreline Golf Links 2960 N Shoreline Blvd*			

WEDNESDAY, October 22 / Doors Open at 8:00 Barista! Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme Donuts - Fruit - Cheese - Boiled Eggs etc.			
IIW Women's Breakfast Roundtable's	**7:45 - 9:00**	Demo Hour	1:30 - 2:30
Opening Circle / Agenda Creation	8:45 - 9:30	Session 4	2:30 - 3:30
Session 1	9:30 - 10:30	Session 5	3:30 - 4:30
Session 2	10:30 - 11:30	Closing Circle	4:30 - 5:30
Session 3	11:30 - 12:30	Conference Dinner	6:00 ~
Lunch	12:30 - 1:30		
Conference Drinks by Oracle & Dinner by Microsoft BackAYard Caribbean Grille (w/plenty of V&V options) - Here at CHM!			

THURSDAY, October 23 / Doors Open at 8:00 Barista! Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme Donuts - Fruit - Cheese - Boiled Eggs etc.			
Opening Circle / Agenda Creation (SHARP)	8:45 - 9:30	Session 4/Working Lunch	12:30 - 2:00
Session 1	9:30 -10:30	Session 5	2:00 - 3:00
Session 2	10:30 - 11:30	Closing Circle	3:00 - 4:00
Session 3	11:30 - 12:30	**IIWXLII April 28 - 30, 2026**	
Drinks/Dinner 5'ish No Host @ Das Bierhauz 135 Castro Mountain **View** https://dasbierhauz.com/			



IIW 41 Agenda Creation = Schedule & Workshop Sessions

Agenda Wall being created on Day 2 (8x speedup) Tuesday

Click to View!

149 distinct sessions were called and held over 3 Days. We received notes, slide decks, links to presentations and photos of whiteboard work for 115 of these sessions.

October 21, 2025 ~ Day 1

Session 1

1A/ SEDI Summit 0 calories, All caffeine / Utah - Sam Smith, Steven McCown, Phil Windley, Chris Bramwell
1B/ OAuth 101, Why OAuth? OAuth for MCP! New OAuth Specs? / Aaron Parecki
1C/ Please Teach Me Web Wallet / Hideaki F
1D/ Server User-Agents (vs Client User-Agents) A Fundamental Missing Piece of Infrastructure / When Leggett
1E/ NO SESSION
1F/ Passwordless Authentication w/ 100% Adoption / Andy Swett, Mike Jones, Ravi Ramaraju
1G/ NO SESSION
1H/ NO SESSION
1I/ Self Sufficient Software Connecting Canoe Paddlers / Tyler Childs
1J/ NO SESSION
1K/ Native App to Webb SSO / Matt MacAdam BECU

1L/ KYAPAY - A Protocol for Agent Identity and Commerce / Ankit Agarwal @ Skyfire
1M/ Introduction to the First Person Project / Drummond, Margeigh Novotny, Martina Kolpondinos and others
1N/ NO SESSION

Session 2
2A/ SEDI - GUARDIANSHIP - DEMO-META + ROBLOX INTEGRATION / Veridian
2B/ Intro to Open ID Connect / Mike Jones
2C/ My Private AI Agent as Authorization Server / Adrian Gropper
2D/ IIW Testimonial w/Pete the Videographier - He is doing short recordings - go make one! :-)
2E/ Neither SOCIAL nor ENTERPRISE SSO and Federation when I only kinda trust you / Justin Richer
2F/ IEEE P7012 (My Terms) and the End of Corporate ToS / Justin Byrd
2G/ Building trustworthy AI / MCP ecosystem - finding ways forward / Chris Phillips
2H/ HARMS We Care About / Erica Connell & Joe Andrieu
2I/ OpenID4VC 101 & ….. / Kristina Yasuda, Joseph, Paul
2J/ NO SESSION
2K/ NO SESSION
2L/ Drivers License Demo (live) / Francisco Corella Joint work with: Suhni Chuhad, Pema Selden. Veronica Wognas
2M/ Swiss e-ID “the least worst centralized government identity system?” & The Failure of Decentralized Identity (and what to do about it) / Christopher Allen
2N/ What Are Transaction Tokens? (secure identity context propagation} Ashay R.

Session 3
3A/ Email Verification Protocol / Sam G & Dick H
3B/ Authorization 101 / Steve Venema
3C/ Content Authenticity 101 / Eric S
3D/ Building a Multi-Agent Research tool for Blockchain Governance & Standards using First Person Project / Mitchell Travers
3E/ NO SESSION
3F/ SEDI Guardianship & Delegation (for dummies) / Timothy Ruff
3G/ Your WORDS Are Your Identity , VCONs tracking everything you say. / Ben Curtis
3H/ First WEB Based Open Source Passkey Enabled Identity Wallet / Stina and Leif Johansson
3I/ Presenting CoralKM - A protocol for decentralized Key Management + Recovery (help needed to give feedback and design) / David Gildeh
3J/ NO SESSION
3K/ Four MCP Use Cases (with distinct identity considerations) / Atul Tulshibagwale
3L/ Tools for Traps *Expanding the Language* / Jeff Orgle
3M/ NO SESSION
3N/ NO SESSION

Session 4
4A/ Threats + Mitigations Persistent State-Issued Citizen Entitlements (SEDI) Trade-offs (KERI-ACDC) Security / Sam Smith
4B/Passkeys 101 / John Bradley
4C/ K-ARF Open Framework Digital Identity Infrastructure for ‘South Korea’ / Jinyoung Jun - Hopae
4D/ The Six Inversions - The systematic transformation of legal protections into Platform Feudalism! / Christopher Allen
4E/ Digital Fiduciaries - What should they KNOW? / Joe Andreau
4F/ VLEI Ecosystem Upate - GLEIF / Karla McKenna

4G/ DIDComm Intoo, CBOR encoding, New Protocols / Sam Curren
4H/ Multi - Subject OAuth / Sarah C
4I/ Scaling the Agentic Web / Andor Kesselman
4J/ Verifying Desktop Applications for localhost redirects / Paul C
4K/ “Who’s Responsible?" Authorization and Liability in AI Agents / Emu Iizuka
4L/ Beyond the Blue Check - from Social Verification to Verifiable Relationships / Brendan M + Alberto L
4M/ Proximity Presentation for SD-JWT using 18013-5 / Lee, Kristina, and more
4N/ IIW Testimonial for Pete! Any time in room N

Session 5
5A/ How to use Keri/ACDC for SEDI Infrastructure Distributed Decentralized Signing Infrastructure / Sam Smith
5B/Decentralized Identity 101: elements and applications / Steve McCown
5C/ Anastasia: Cinderella’s Stepsisiter - Turning X.509 certs into Anonymous Key Attestation / Dan Yamamoto
5D/ Gen AI Phishing! Using AI for Bad Things! / Yuriy A
5E/ NO SESSION
5F/ Passkeys PQC and Beyond / John Bradley
5G/ Gordian Autonomy Stack / Christopher Allen Blockchain Commons
5H/ Use cases in North American Real Estate / Michael Krotscheck
5I/ Identity 4 Groups “real decentralized?” Sideways. Earth verifiable community (nor social graph) / Kaliya Y
5J/ Natural vs. Verified Person? / Luke Nispel
5K/ Technical Approaches to Delegation and Guardianship / Richard Esplin
5L/ Women in Identity - What does our community need to help *Women/underrepresented communities depending on ID systems? * YOU / Elizabeth Garber Exec Dir. WiD
5M/ If Bitcoin had Identity Layer - first person network for retroactive UBI & solving $338T Glogal Debt Crisis / Nivas Sivaprakasam
5N/NO SESSION

Wednesday October 22, 2025 ~ Day 2

Session 6
6A/ Is Compromising a SEDI Treasonous? / Rep. Chevrier
6B/ MY TERMS for Dummies / Doc & Joyce and Customer Commons Team
6C/ When Patients and Doctors write their own Software… / Adrian Gropper.
6D / NO SESSION
6E/ NO SESSION
6F/ Data Unions & Labor Laws w/James Felson Keith running for congress on Data & Labor Platform / Kaliya Y
6G/ Presenting VSs based on Natural Language Instructions - Offline LLM for DCQL on Mobile / Ken Watanabe
6H / OpenID 4 VC Conformance Testing Deep Dive / Joseph Heenan
6I/ On Behalf of use Authorization for AI agents (draft spec) / Hasintha Indrajee & Sachin Mamoru from WS02
6J/ NO SESSION
6K/ Driving Adoption vLEI + KERI - GLEIF vLEI Learning Modules - GLEIF Global Hackathon / Esteban Garcia
6L/ KYAPAY - A protocol for Agent & Principal identity & Payments / Ankit Agarwal @ Skyfire
6M/ OPAQUE Passwords RFC 3807 / Michael Krotscheck
6N/ NO SESSION

Session 7
7A/ Native Client Attestation Grant & Key Binding / Frederik Krogsdal Jacobsen & Attestation-based Client Auth
7B/ Verifiable Relationship Credentials (VRS's) and R_Cards: A Design Session / Brendan Miller +++
7C/ Interop KERI + W3C Libraries (reuse not rewrite) / Kent Bull
7D/ NO SESSION
7E/FIGHT CLUB - The Kids are online! Plain Language discussion on children on the internet / Swan Black
7F/ State Endorsed Decentralized Identity (SEDI) for Dummies / Timothy Ruff
7G/ SD-JWT How it works? Entry Level / Lukas Han
7H/ State of the State: Tracking and coordinating Public Policy / Ethan Veneklassen
7I/ Biometric Bound Credentials / Richard Esplin
7J/NO SESSION
7K/ NO SESSION
7L/ NO SESSION
7M/ Password Auth w/PQL in the Quantum Era / Bryce Frey
7N/ NO SESSION

Session 8
8A/ OpenID 4VC - Issuance over W3C DC API / Kristina, Paul, Lee
7B/ HARMS -> STORY 'Digital Identity Mad-Libs' / Erica Connell
7C/ NO SESSION
7D/ New Data Paradigm - US Chamber of Commerce use case: U.I. (unemployment insurance) @ VC issuance to Employees / Phil Long
7E/ Non-Binary Approaches Human Verification - from 0/1 to 0.0/1.0 /Discussion Session / When Leggett
7F/ OAUTH for MCP (client ID metadata document) / Aaron Parecki
7G/ vLEI Authentication Organizational Login (vLEI) with ecr credentials / Christoph S, Vincent V, Stefan I
7H/ NO SESSION
7I/ Trust Registry Query Protocol / Andor, Darrell, Drummond, Phil
7J/ NO SESSION
7K/ NO SESSION
7L/ Death and the Digital Estate / OPEN ID Foundation Community Group - George Fletcher
7M/ Women in Identity? - What should an organization focused on inclusion be doing with and for the community of ID Professionals? / Elizabeth Garber
7N/ NO SESSION

Session 9
9A/ OpenID4VC "server-to-server' mode / Kristina, Joseph, Paul, Lee Christian,
ACDC Blindable Registries - How to minimize correlation + detect compromises - Proof of Age non-zkp / Sam Smith
Alternative traffic stop authentication safer for the officer / Francisco Corella
NO SESSION
NO SESSION
My Terms Practical Experience - Customer Commons / Iain Henderson
If bitcoin had an identity layer 2.0 / Nivas Sivaprakasam
What are DIF Recommended DID Methods? / Jonathan Rayback
Build It Yourself Agent Espert *live* Building an agent to talk to a spec / Chris Phillips
NO SESSION

Cross-border interoperability of VC's with demo of Japan's My Number car on iPhone / Hideaki Furukawa
Agentic Identity Gateway / Teng and Authorization and Liability in AI Agents / Emu Iizuka
Hologram Messaging Verifiable Chatbots P2P + Ai / Ariel Fabrice
The End of the Global Internet / Heather Flanagan

Session 10

10A/ OpenID4VC "server-to-server' mode / Kristina, Joseph, Paul, Lee Christian,
10B/ ACDC Blindable Registries - How to minimize correlation + detect compromises - Proof of Age non-zkp / Sam Smith
10C/ Alternative traffic stop authentication safer for the officer / Francisco Corella
10D/ NO SESSION
10E/ NO SESSION
10F/ My Terms Practical Experience - Customer Commons / Iain Henderson
10G/ If bitcoin had an identity layer 2.0 / Nivas Sivaprakasam
10H/ What are DIF Recommended DID Methods? / Jonathan Rayback
10I/ Build It Yourself Agent Espert *live* Building an agent to talk to a spec / Chris Phillips
10J/ NO SESSION
10K/ Cross-border interoperability of VC's with demo of Japan's My Number car on iPhone / Hideaki Furukawa
10L/ Agentic Identity Gateway / Teng and Authorization and Liability in AI Agents / Emu Iizuka
10M/ Hologram Messaging Verifiable Chatbots P2P + Ai / Ariel Fabrice
10N/ The End of the Global Internet / Heather Flanagan

Thursday October 23, 2025 - Day 3

Session 11

11A/ Malnets - Understanding Malware Networks / Jacob Siebach
11B/ OIDF AI Identity Management Community Group Call
11C/ Storytelling - The Art of the "Lie" Utah's Biggest Liar / George McEwan
11D/ NO SESSION
11E/ Help Wanted - Seeking Practical Advice for Implementing SEDI / Alan Fuller
11F/ Future of Work meets Identity and Data Portability / Brad Topliff
11G/ Perspectives from the United Nations from Refugee Registration to Self-Sovereign Identity / Besem Obenson
11H/ ZKP - Overview - Getting to Deployments / Leif Johansson, Chris
11I/ Human Alignment in Agent to Agent Authorization / Adrian G
11J/ NO SESSION
11K/ NO SESSION
11L/ KERI Auth Browser Extension demo/discussion / Ed Eylcholt
11M/ Notarized Verifiable Relationship Credentials (VRCs): The "Virtual Selfie" - Harvard Applied Social Media Lab / Brendan Miller, Alberto Leon, Drummond and others
11N/ Phone Home - An Update / Timothy Ruff, Joe Andrieu, Steve McCown

Session 12

12A/ SEDI Guardian Demo, Roblox + Social Book / Veridian
12B/ WTF is a "client_id" / Justin Richer
12C/ NO SESSION
12D/ NO SESSION
12E/ NO SESSION
12F/ FeDIDeration DIDs in OPENID Federation / Lukas and Fraser
12G/ You've Got The Wrong Use Case / Alan Karp

12H/ per-Credential Metadata (by the issuer…) / Paul, Gareth, Leev, Kristina, etc
12I/ NO SESSION
12J/ NO SESSION
12K/ NO SESSION
12L/ Domains of Identity - 16 Subdivisions of Use Cases… walking through them + considering developing intersections between domains. Book + Practice Talk 4 Taiwan / Kaliya Y
12M/ What Identity can Learn from Home Assistant and Home Automation - interop - privacy / Sam Curren
12N/ Privacy in a Surveillance World / Steve McCown

Session 13
13A/ Working Session - How to add VC, VP and maybe mDL to CAWG identity / Eric Scouten, Andrew D
13B/ KERI's Post Quantum Story Surprise Quantum Attack Capture New Decryp Cater Crypto Agility / Sam Smith
13C/ How to Drive Adoption of Fairest Universal Basic INcome Currency with Inevitable AI Job Disruption (using identity tech) / Nivas
13D/ NO SESSION
13E/ NO SESSION
13F/ Getting Started on MY TERMS Deployment - Who wants to help? Starting work groups TODAY! / Doc, Joyce, Kari
13G/ Credential Usage Policy / Paul, Tobias, Kristina
13H/ Tools for Traps *Expanding the Language* / Jeff Orgle
13I/ RP Architectures & ID Token Audiences / Frederik
13J/ Mechanics of Running and Open ID Federation (I'm struggling!) / Nicole R.
13K/ The TXNS are coming from inside the house! How do we think about minting tokens for in-clutter transactions / Andrew Todd, Mongo DB
13L/ CorpLKM & Key Recovery Part 2 / David G
13M/ NO SESSION
13N/ NO SESSION

Session 14
14A/ What's your p(doom) and why? / Omri G
14B/ NO SESSION
14C/ NO SESSION
14D/ NO SESSION
14E/ NO SESSION
14F/ Server-to-Server issuance / Hicham, Martijn, Gareth
14G/ KERI Suite (ACDC CESR SEDI) Ask me anything / Sam Smith
14H/W3C/ Why? A research projects findings / Emily L?
14I/ Defining Policies for AI Agents - Is Auth Policies enough?! / Andor
14J/ NO SESSION
14K/ NO SESSION
14L/ Crowd-Designed Software Session: BYOE architecture, Social Network for IIW / Dmitri, Ty, Bengo
14M/ Building a National-Scale IOP with OIDC: Short comings OP OIDC / Fredrico
14N/ NO SESSION

Session 15
15A/ German EUDI Wallet / Kristina Paul, Christian
15B/ Resource wonder PASSKEY credential Flow for Agentic AI'S / Hideaki F.
15C/ Can YadaCoin Help Keri? / Matt V

15D/ Privacy Dissolution or Redamation - How do we redain data practically speaking and attach data to a strong ID? What are the protocols? / Beth P
15E/ NO SESSION
15F/ Cross-Pollinate - Bring Your Ideas to “Server User-agents” / When Leggett
15G/ Sorta Kinda Digital ID - adding digitally signed printed elements to physical IDs and documents / Elaine Wooton
15H/ NO SESSION
15I/ Local First Software + Bridging Communities / David Gilden
15J/ NO SESSION
15K/ NO SESSION
15L/ Authorization and Liability in AI Agents / Emu Iizuka
15M/ NO SESSION
15N/ CfP Brainstorming for EIC, Indentiverse / Heather F

OpenID Foundation
6,515 followers
4d • Edited •

🌐 Where the Future of Identity is Built

The OpenID Foundation is pleased to see the start of another **Internet Identity Workshop** this week — a truly unique unconference that has been driving innovation in digital identity since 2005.

Held twice a year, IIW brings together developers, policy experts, researchers, and technologists to collaborate openly on the technologies & standards shaping decentralized identity, digital credentials, authentication, and trust frameworks.

What makes IIW special is its format — participants set the agenda in real time, engaging in deep, peer-led discussions that move the industry forward. It's a space where ideas become standards and collaboration drives a more secure, user-centric digital future.

OIDF wishes all participants a productive and inspiring week at **#IIW**!

#DigitalIdentity #OpenIDFoundation #IIW #IdentityStan

Notes Day 1 / Tuesday October 21 / Sessions 1 - 5

SESSION #1

SEDI Summit (State Endorsed Digital Identity)

Session Convener: Christopher Bramwell
Session Notes Taker(s): Kent Bull

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

Summit Link:
https://www.uvu.edu/herbertinstitute/data_governance/state_endorsed_digital_identity_summit.html

privacy.utah.gov - great tools and resources

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

Attendance count: 58

The whole point of SEDI was to answer the question, "what is the American version of identity?" It is an innate right to you, not something the government controls. How do we protect our rights, families, children, and ourselves?

Who is in the audience? We have some call outs.

- One of the representatives from Utah
- Utah Privacy commissioner Steve Mcown
- George McEwan
- Sam Smith
- Phil Windley - why we're doing decentralized in Utah
- Timothy Ruff
- Veridian Team - demoed guardianship with SEDI last week

Highlights from the summit last week:

There is an identity crisis. Identity is going to be compromised, you have to assume that from the start. It is also a tool that can be used for surveillance.

Utah is one state with comprehensive IT and identity technology.

Some states sell surveillance datasets about citizens to very large vendors, some of the household-level data updated hourly.

Goal is not to create or control identity but to endorse and protect it as a matter of public trust.

Identity that can be taken away is not individual digital identity.

Individual brings their identity to the state, the state verifies who it is (identity proofing), and then the state gives a credential to that identity (the endorsement).

We have to get back to the governments role is to protect individual rights. We can do it, we're doing it in Utah.

If you do identity right it's going to be amazing. This is an issue everyone agrees with.

The challenge: trust has collapsed online.
There is no real control or privacy online. Cindy George told a compelling story at the SEDI summit about her son that committed suicide due to online sextortion. A fraudster from a call center in the Philipines pretending to be a girl sent pictures, got him to send pictures, and then the trap was sprung.

This all happened between a Sunday and a Thursday. This is a real harm that must be addressed.

Timothy comment: this fraud started in a game. A male in the Philippines masquerading as a pretty girl. The fraudster got the person to leave a game and engage outside of a game.

Why? Why is SEDI needed?
Lots of people have said, we have mDL, we have W3C, we have Sam/KERI. Why do we need more?

This is what every technology has skipped. We've maximized interoperability and efficiency yet nothing we've done has gone back to our values, to the constitution, and to mind and fill those gaps. SEDI ensures we answer the essential question. What are the technology and policy requirements to ensure rights are protected?

A member of the ACLU has said that what we are trying to do with SEDI is like sending a camel through the eye of a needle. If we don't make it happen then we need to slaughter the camel and send the ashes through the eye of the needle. We won't do digital identity if we can't do it right.

Nothing gives the government the authority to compromise rights in favor of things that are not rights. We don't to balancing between rights and lesser interests. We protect and prioritize rights first. We will create the freedom respecting digital identity and export that to the world.

It was horrible to do age verification without something like SEDI.

Utah is not afraid to go after the companies who prioritize profit over rights. Many companies prioritize profit in exploitative ways.

We are having discussions with other states.

Question: How do you deal with data brokers in this context?
Break the question into two parts.

- You are a first party transaction doing things.
- You are a surveillance party observing a transaction.

Our approach with digital identity has very strong language on what can or cannot be done with a person's data. We are likely to come down hard on corporations and third party relationships that exploit first party data.

Comment from the audience (: I am skeptical that the federal government will adopt something like SEDI because with their national security imperative they usually add backdoors and all the things we do not like.

Identity is already decentralized through happenstance in the driver license system. There will likely never be a national identifier.

There is a national security side where the federal government will come into this. There does need to be interoperability and reciprocity between states which is where the federal government can come in and help. There needs to be a high assurance credential that respects constitutional rights. SEDI meets this need.

Comment from the audience (Phil Windley): there are a few perspectives on federal involvement. They are putting their fingers into the pot. RealID is the federal government putting their finger into the pot. There is no guarantee they won't put their finger in the pie, though it is likely they will accept this (SEDI).

Chris: this is the only model being presented as a comprehensive model of American identity. SEDI is the only model that mentions constitutional rights at the base of it.

Comment from Christopher Allen: Switzerland passed national ID with 50.34%, which is not a mandate and is actually a problem. Switzerland is interested in doing a more state endorsed model. It would be fairly easy for the Swiss to move to a state endorsed system.

Question from the audience: how do we avoid too many standards? What does it look like in avoiding creating too many standards?

Answer: SEDI is not a standard, it is a public policy approach. The standards then need to come to be updated to the public policy requirements. We don't let technology dictate our values. Public policy dictates what values are to be protected and technology is supposed to meet that. This is brand new (SEDI) yet it is public policy, not a technology standard. I don't care what the tech standards are, just make sure they can meet the requirements of the public policy.

Comment from the crowd: #1 Government should never have a kill switch to turn off your identity. That is you. Government should never monetize your existence. It's not a technology problem, it's a culture shift.

Question from the crowd: Is there any technical protection on government abuse of data or is this just a policy solution?

Comment from Timothy: a few words have been said that are hard to reduce to practice. SEDI boils down to one thing that breaks the risk of government taking advantage of the identity system and that is tracking. The ability to track becomes the ability to control. If government becomes the point of tracking that says yes or no then it becomes control. You can make it possible technically that tracking verifications is not possible. Combine that with policy that prevents correlation and data sharing through identity use and now we're talking.

I like to think of SEDI as digital ID without tracking - that's what the rights means.

Comment from the crowd: we're having a vocabulary issue between public policy and technical standards. Government ends up being local. You have to create value systems first. Once we have that then we can make technological standards. Confusion can come into play when technical standards are created without considering the underlying value systems at play.

Comment from Doc Searles: can we talk about the terms in the most recent terms?

privacy.utah.gov - great tools and resources

Chris: we are talking about vehicle data privacy in Utah. What are the purposes and uses of your data?
Nationwide there are only six states nationwide with comprehensive data governance laws. You can go on our website and see this broken down by states.

It's much easier to constrain government than private companies.

With SEDI what I am envisioning is that SEDI will give us that tool to flip the script to not just control their identity but when a citizen engages in government we get to reimagine the purposes and uses of the data. You will know the provenance of data and there will be separate terms and uses for each piece of data.

Once you give people a taste of freedom then the tend to demand it.

Steve Mcown: this is a bit of a back to the future moment. Usually tech would go from the military to commercial use. Now, as of the 90's, things created by corporations like WiFi are now being introduced into the military.

We're taking a step way back and saying "government for identity purposes needs to meet these standards." Go find your tech standard, if it meets these needs, then we're interested.

Chris: Legal Entities in Utah are no longer allowed to misuse data in Utah. We've learned from our mistakes. Now we're aware. We're done not prioritizing individual rights.

Question from Paul Dietritch: is there public policy around how to deal with the longevity of identities and data?

Answer: we are saying you can't monetize the existence of an individual. A birth certificate is for a child that is delegated to a parent. Some lifecycle management of data is something that can come from the private sector. What Utah is looking for is, if we are going to start to do this right, something that allows better service delivery using trustable digital identity that can be proliferated everywhere.

Clarifying question: how is something paid for?

SEDI, what does it mean to have public infrastructure?
You need trust for a free market to flourish.
We don't have a free market anymore, we have a monopolistic, exploitative market right now.
Identity is at the basic level as public infrastructure and should be treated as such.

A driver license is not a right, it is an entitlement. We know what critical public infrastructure is. Does everyone get it for free? Everyone can create their own identifier. The state can add an endorsement on top of that. Our goal is to give everyone an IAL3 verified identity. The goal is for it to be ubiquitous. I told the legislator that this will be expensive.

George: If we truly believe it should be P2P between you and the verifier then it needs to be open source and verifiable.

Question: what policies do you have for making sure identity cannot be spoofed or stolen?

Answer: this is being defined right now. As much as possible we rely on existing standards such as by NIST. This is part of how we get the federal government to accept it.

We're looking at a culture change we need to make in society. Right now you don't have an expectation of privacy from government or companies. We need to build this right into the new policies and technical implementations. It's going to be incremental.

This is a reverse trojan horse. We are going to make the policies so good that the only way to meet them is with freedom respecting technology implementation.

Christopher Allen. Focusing on privacy is a mistake, needs to be anti-coercion. We need to talk about resilience and stewardship.

Chris B.: We've presented this as a security-first approach. This centers on who has agency control of the keys. You control the keys, you can reclaim your identity if your keys are compromised.

Joyce Searles: MyTerms is the other side of this, it sounds like.
Rashmi Siravara: Endorse and Protect- Unique Digital Identifier per state _SEDI.

OAuth 101

Session Convener: Aaron Parecki
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:

Example: Hotel key.
The hotel key doesn't represent an identity. It's a key to access resources in the hotel.

OAuth: access token
OpenID: ID Token

Please teach me web wallet

Session Convener: Hideaki. F
Session Notes Taker(s): Ryo. N

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:

Comparison between blockchain-based credential systems (e.g., Aries, DIDComm) and OpenID for Verifiable Credentials (OpenID4VC).

Clarification of terminology:

- Subscriber-controlled device (digital wallet) = locally controlled.
- Hosted service (cloud wallet) = remotely managed wallet.

Hosted wallets (web/cloud) raise issues about key storage, security, and recovery mechanisms across devices.

Participants note no clear consensus yet on reliable cloud-based credential storage and recovery.

Complexity arises when wallets must handle proof presentation requests (verifier asking for credentials).

Issuer typically does not see presentation actions; privacy preserved.

The Open Wallet Foundation is working on defining wallet–issuer protocols and interoperability (e.g., APIs for credential exchange).

Mention of VC Exchange API, OIDF4VCI, and VC API as relevant protocols.

Example: issuer shows a QR code → wallet scans → initiates credential issuance or presentation based on supported endpoints.

Discussion of ZCAPs (Capability Delegation) for fine-grained authorization and multi-device key management:

- Enables delegation without key export.
- Useful for multi-device setups or cross-application access.

Debate over whether credentials should be used for authorization (not recommended by W3C CCG) vs. using ZCAPs or other models.

Concern that users may not understand authorization implications, suggesting need for strong UX design or AI agents to assist decisions.

Argument that over-restraining innovation to protect users may hinder development.

General agreement that presentation-based models (user-consented credential sharing) are currently the safest and most comprehensible approach.

Future direction may involve delegation protocols, AI-assisted user consent, and chip-based secure key storage (e.g., mobile secure elements).

Server User-Agents (vs Client User-Agents) A Fundamental Missing Piece of Infrastructure

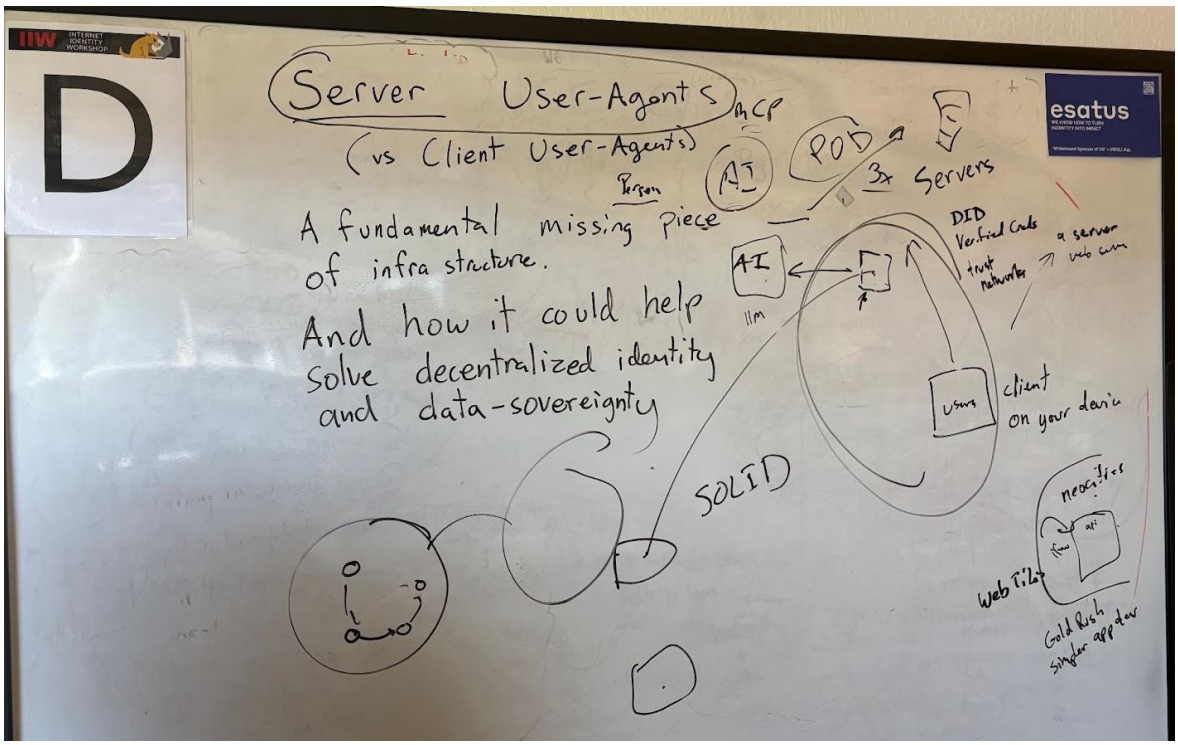
Session Convener: When Leggett
Session Notes Taker(s):

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

A summary of Server User-Agents and notes on IIW

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

This session was the first time introducing the term and concept of "Server User-Agents" to the group. There was a minimal introduction of the concept on the board before a Q&A and discussion session to refine the idea and discuss its relationship to other projects.



Passwordless Authentication w/ 100% Adoption

Session Convener: Andy Swett, Mike Jones, Ravi Ramaraju
Session Notes Taker(s): Nicole Roy

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

https://www.hawcx.com/

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

Participants included:

- Andy Swett (Hawcx) - Mike Jones - Ravi Ramaraju (Hawcx) - Riya Shanmugam (Hawcx)
- Nicole Roy - Dick Hardt Hellō - Jim Fenton - Bryce Frey (Google) - Ashy Koshy (Yahoo)

Self Sufficient Software

Session Convener: Tyler Childs (Sillyz.Computer)
Session Notes Taker(s): Tyler Childs (Sillyz.Computer)

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

https://sillyz.computer
https://sillyz.computer/app/plan98-ide
https://sillyz.computer/app/was-code?src=/public/elves/sillonious-brand.js

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

My approach to identity has been to create a single player video game and then go to networking events to find networkers to bridge out of my video game with.

Sillyz.Computer is my personal identity, personal computer, and personal comedy. From making friends, they were able to break me out of my local file system and into a personal crypto wallet.

I write experiences for humans and my friends keep me safe. The sillonious-brand component is my personal DNS that i use to route traffic within my personal intranet, which leverages the web layer of the internet.

Native App to Web SSO

Session Convener: Matt MacAdam
Session Notes Taker(s): Matt MacAdam

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

https://www.ietf.org/archive/id/draft-ietf-oauth-identity-assertion-authz-grant-01.html
AsWebAuthenticationSession
https://www.w3.org/TR/digital-credentials/
FedCM

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

Specific use case Matt is trying to solve for:

-Native App uses ASWebAuthenticationSession (with the "ephemeral" flag) or Android equivalent, so web session is gone after initial login.
-App has a long-lived refresh token ("tens of months")
-Native app user needs to be able to access authenticated resources in an in-app browser ("webview") without signing in again

"Identity assertion spec" was mentioned (note from Matt on later research: The app already has a refresh token so it can just get an ID or access token from our own IdP–no need to swap for another token). probably this one: https://www.ietf.org/archive/id/draft-ietf-oauth-identity-assertion-authz-grant-01.html

It is possible to write a cookie into a webview. So if you could procure a cookie out of band, or had a long-lived session cookie, you could use it as a session identifier.

PingFederate has something called a "drop off" that can be used to bootstrap a web session. Basically a trusted party can "drop off" some attributes, the platform returns a unique web URL, and a browser can navigate to that URL to "pick up" the session. It sounds like there are similar patterns, on other platforms or created internally, in use by at least a couple other folks at this session. One person referred to their pattern as "OTP".

Related question: Some IdaaS solutions offer SLO, but require an id_token and valid session cookie to trigger it without user interaction. Using the above mechanism, how could I get the id_token back into the app so the app could trigger SLO? Possible solution: schema or universal link–same as we do for a regular login. But can this be done without transferring control back to the app? Maybe do that when the webview is torn down? Possible?

Maybe some mobile SDKs could help solve this problem?

DC (Digital Credentials, w3c spec) API was mentioned. The DC API as I understood it: App can store stuff in special OS storage. JS API to call credential store that can look into OS credential store. One attendee said using the DC API may require a contract with Apple and "the contract is a secret". Not sure about Android requirements.

Someone mentioned CIBA (Client-Initiated Backchannel Authentication) could be useful here, but requires session binding.

Someone said George Fletcher might have a draft for native browser SSO

We pretty well covered the initial case (bootstrapping the session into an in-app browser). So someone posed the question:

What about the case where we want to establish the session into the *system* browser? Much harder. Basically Apple doesn't want you to do this.

Cross-domain identity grant type? Aaron working on cross-application. Not sure if this is the same as the "identity assertion" spec referenced earlier.

One idea the group came up with for bootstrapping system browser

1. App generates nonce, sends to browser with the user
2. Browser creates its own nonce (or keypair). Stored in session or cookie etc.
3. Signs nonce and sends back to app
4. App sends public key to the backend service
5. User back to browser, browser sends request signed with key to backend.
6. Sends ID to browser
7. Browser generates ID for itself

User experience would be odd….user would not have to do anything but browser and app would flip back and forth a few times. (note from Matt: I recall something about Apple not letting certain types of redirects like this happen without user interaction so I am not sure if this would work–that's a question for Rita Z at Okta–she wasn't at IIW but she would know). (another note from Matt: Apple could also just not approve your app if you did this).

FedCM does browser level cred storage. FedCM can get native accounts, but only in Chrome. We didn't explor this idea too much.

Interesting idea: For financial institutions…if there was a card in the wallet (apple or android) could it be leveraged for authentication?

KYAPAY - A Protocol for Agent Identity and Commerce

Session Convener: Ankit Agarwal @ Skyfire (ankit@skyfire.xyz | ankit@tryskyfire.com)

Session Notes Taker(s): -

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

2.2 KYAPay - A Protocol for Agentic Commerce - IIW/AIW - Oct 2025

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

Introduction to the First Person Project

Session Convener: Drummond Reed
Session Notes Taker(s): Eric Scouten

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

https://www.firstperson.network/white-paper

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

Drummond Reed, First Person Project

Reviewing version 1.1 of the First Person Project White Paper, just published yesterday. It's 86 pages long. This talk is an overview of the major sections. Since it's in the document, I won't transcribe everything, but will instead focus on some highlights.

There's also a slide deck if you prefer that format.

Fundamental goal: Establish a person-to-person trust layer for the internet.

Ability to impersonate real people and real situations with current generative AI tools has led to an accelerating degeneration of trust.

An essential part of this is to establish and facilitate person-to-person secure channels.

Reference out to personhood credentials paper.
See https://ericscouten.dev/2025/iiw41/#session-1m-first-person-project for photos. 😳

Computer History Museum, Mountain View, California

Talk through how people have multiple personas that they might want to disclose selectively, for example:

- political
- religious
- neighborhood
- work
- medical
- online dating

At the end of the session, attendees shared other First Person Project related sessions:

- Harvard Applied Social Media Lab (HASML) — General introduction, Tuesday
- Introduction to the First Person Cooperative — first session Wednesday
- HASML: Verifiable Relationship Credentials (VRCs) and R-Card Schemas — Wednesday
- HASML: Notarized VRCs — “The Virtual Selfie” — Wednesday

SESSION #2

SEDI - GUARDIANSHIP - DEMO-META + ROBLOX INTEGRATION

Session Convener: Wayne Cheng, Thomas Mayfield, Fergal O'Connor, Jeremy Firster, Cardano Team
Session Notes Taker(s): Kent Bull

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

Video from the SEDI Summit showing both the guardianship platform and the KERIBLOX integration with it (State Endorsed Digital Identity)

https://www.youtube.com/live/1LzYMm572Lo?si=kmqscgRlqdb0WL5A

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

Attendance count: 32

We don't consider an mDL to be a SEDI-compatible credential.

Demonstration:

GETMobile: where Utahn's can get their mDL into an app
GETMobile Verify

Showing the SEDI Wallet and Credential and how it will work with the existing verifier app for the state.

The demo shows the ability to select or deselect what is shared. We don't need to worry about server retrieval. We just need to worry about the bluetooth transmission P2P.

Comment from the audience (Judith Fleenor): SEDI is policy, not technology. What do we do now to give the ability to have selective disclosure since it is the verifier who says what it is that they need? How is the policy being set so that I am not asked to disclose things not relevant to a context?

Chris B.: Yes, minimization is a universal privacy principle. Combining selective disclosure and contextual minimization has not yet been done in public policy. Any technology must allow you to selectively disclose what you want and entities are required to collect only the minimum needed for a purpose.

Sam S.: Woodrow Harzog, a leading privacy legal scholar, came up with a legal concept called "wrongful engagement" which is something companies use to drive profit. Driving engagement drives profit. This legal doctrine stops you from being exploitatively engaged by a company because the corporations begin to socially engineer you. The people maximizing their profits have been training us to do what they want us to do. We need policy smart enough to understand this and have policy controls, not technical controls, to correct this.

Question from audience: do we need to have entities register their purposes and uses of data?

Chris B: Utah is more libertarian and we allow private entities to transact how they wish. We are with SEDI focusing on organizational identity as well as individuals. There needs to be a contract, data provenance, and identity for organizations and people.

Presenter: if you look at the most pro user way of doing this you ask "how does the verifier ask for the data in the right way?" Simplest way is not to show a list of items being selectively disclosed but rather baked into something the user cannot change that is a good preset. It really takes a village to think through these things.

Next demo:
Demonstrating the Digital Credentials API from W3C showing an operating system level for mDL.

The Digital Credentials API is protocol agnostic. You can use it with W3C, mDoc, CESR, or anything.

Using a phone to sign up with a bank using mDL

Next demo from Thomas Mayfield et. al.

Today we are showing what is possible and how these things may be used, on how to use KERI and ACDC to create the individual identifier, to change the keys, and to create cryptographically chained credentials.

Birth certificate issued to a child, parent requesting a guardianship credential from the state. This allows a child to have a safe experience online. Fergal will demonstrate issuance of a birth certificate to a child.

There is no centralized server processing verifications.

Although we are a blockchain foundation we have decided as a foundation that identity should not reside on a blockchain. Protocols should be paramount over platforms.

Mary is going to present, P2P, a guardian credential to the portal.
Request made to Mary to present her SEDI credential. Mary issues a guardianship credential to her child, Oliver.

Issuance request sent to the mother. Once the mother signs it then a request is sent to the child.

Social Media Access credential anchored into the KEL for Oliver. He will use that to log into a new way of doing social media called “socialbook” for this demo. This is a P2P connection between people.

Oliver is asked to present a credential to the system. The system calls out to a decentralized verification process and confirms that the credential (ACDC) data was anchored to the appropriate KEL and that it was delegated from Oliver’s mother.

A child can request permission to talk to a given person.

KERIBLOX
Games are a serious topic due to the fact they are now hunting grounds. This next demo shows the ability to log into social media and games.

The in-game chat shows that P2P chat is only allowed with other verified, age appropriate children.

Similarly, in-game purchases can be restricted with these credentials as well.

This is GLEIF for parents.

Comment from Sam S.: Privacy is not about secrecy, it is about setting boundaries that modulate the flow of information.

Question: How scalable is this solution?

Answer: In our simulators we tested 100,000 concurrent users and it worked just fine.

Introduction to OpenID Connect

Session Convener: Michael B. Jones
Session Notes Taker(s): Michael B. Jones

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

The presentation posted at https://self-issued.info/?p=2758 was presented and discussed.

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

A small group of interesting, engaged, attendees participated.

Rashmi Siravara: Insightful .The overlap of logins on a specific site was discussed at length and the lag between which creates datahack is to be discussed to solve further.

My Private AI Agent as an Authorization Server

Session Convener: Adrian
Session Notes Taker(s): Mitchell Travers

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

test.agropper.xyz

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

My Private AI Agent as an Authorisation Server

moving towards more rapid standards creation and implementation using Private AI systems

authorisation servers are a point of 'trust'

MAIA (medical assistant AI)
what we've actually built ^

what do you actually mean by private ai agent?

in order to run an auth server, you need control over resources

the resource is the health record in this case (a pdf in most cases) could be between 400 - 2k pages ‘original’

when the information ‘requesting party’ come to the auth server, give me this for that reason, this is who i am.

give the resource directly or give the token to access the resource

whoever is handing the resource needs access (indexd) into the knowledge base.

directly or by a token they trust - chat interface are required to have 5-10 second retrieval

compiled from source -> controls the knowledge base
define private ai agent as this ^
hosting is a commodity thing

digital ocean is what we use for this use case

comparison between the DiD / DiF community - as opposed to having the AI Agent as the auth server

non-commerical

implement VC’s but not DiD as of yet.

The private AI agent IS the authorisation server.

how do you expose the private ai agent to 3rd parties ?

deep links

standard chat interface is used - purely natural language based interactions

to ensure that it is **patient-centric** - natural language is important and why the agent being the auth is important

when you are a doctor and receive a deep link from your patient - you get a choice / you can open it or share it with the next person down the line.

if the doc needs access to your agent, they must open the deep link.

this use case is transferable

how do you explain to a person who is **computer illiterate**, the benefit to them?

expect people to be illiterate with chat interfaces*

the chat gpt moment is actually a good one for dealing with private information

interoperability of the chat.

does this have privacy issues around the group chat,

support and administration

vibe code interoperability - using the private agent

Trusting open source - verifying the github, a movement to self-administration of the integration of these tools. moving away from using dashboards > just prompting > via api.

ongoing battle between openai / visa mastercard - giving information to eachother.
llms are a commodity / public good

hosting will also be a commodity

there is no switching cost between the models >> within the system you can switch question by question.

ensuring privacy across the chat context > building the knowledge base.

all of the knowledge is opensource already. 'discovery is what is unique'

Privacy and context

context - when you get multiple experts to work out the risk/benefit >> you want to control the datasource as well as well as creates bias >> the person needs to control the context.

everything is **editable** > the question > the patient summary > guardrail (in a general sense) > protect from halluciations

The private agent accepts the guardrails and instructions

the inference and the query, you can delete
how do i deal with errors? how do i deal with admissions

each deep link represents a context

the wallet DiD problem still persists

patient requested certain information >

mutual storage of the ‘chat’

you move to the next doc > health summary request >

user choice, if you want them to be in the same or separate contexts’

the next phase, MCP / A2A - is still being worked out.

there is no api into whats going on, there is only the **authorisation server, the chat and the deep links**

how do you do the ‘governance?’ choosing what is exposed by the llm (ai agent) the prompt attack.

who is responsible - the patient is responsible… there is no other party.

demo patients which are opensource (deployed with synth patients) skin in the game . you have an understanding of the knowledge base and context.

governance is within the patients / decentralised

hardware is the only way to be decentralised >

cloud is needed for linkage.

running it within the TEE > homomorphic encryption is future*

there are degrees of decentralization of the confidential compute

‘quality of care’ > this could have a bigger impact on

The ability for the ai to digest massive context and information.

the control of their own knowledge bases and authorisations > there is no longer an ability to control the ‘statistics’ on what is going on in healthcare.

US spends 5.5trill on Healthcare per year > this could disrupt that large load/responsibility of govt.

the redistribution of resources is what we are solving for

IT IS WONDERFUL

‘show me page n’

vibe code does have redundancy in the code > AI must write a document which explains how ‘i dealt with that problem’

its pay per token and the indexing (is where the payments are) the storage, and the website persists

you select the machine, (what you wana store locally you do so) but the Host will be a ‘commodity’ its stored in 3 places:

1. the running code (git build)
2. the files you used to create the knowledge base
    a. takes the pdf binary and expands it by 50% by annotating it (index), understanding of the clustering. thats the token expense.
3. The thing the rag uses (the knowledge base itself)

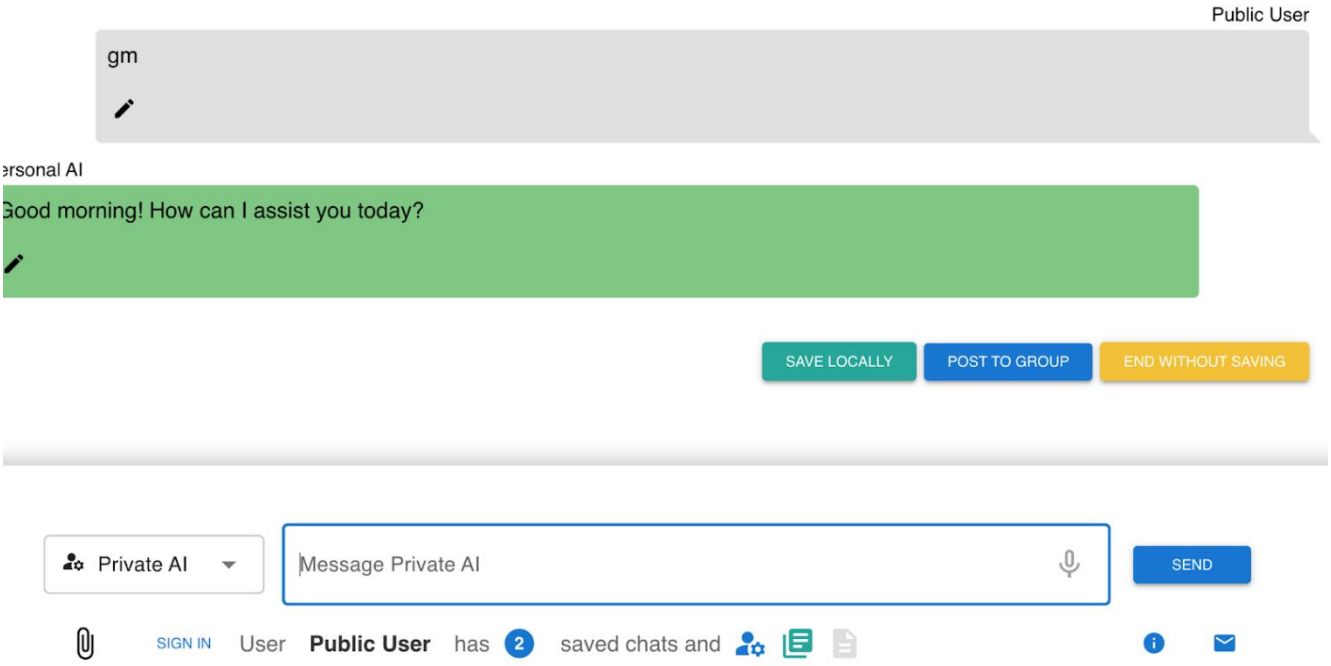
one more thing: for next time (tomorrow)
how do you automate what the LLM can do with the auth server to define the context.

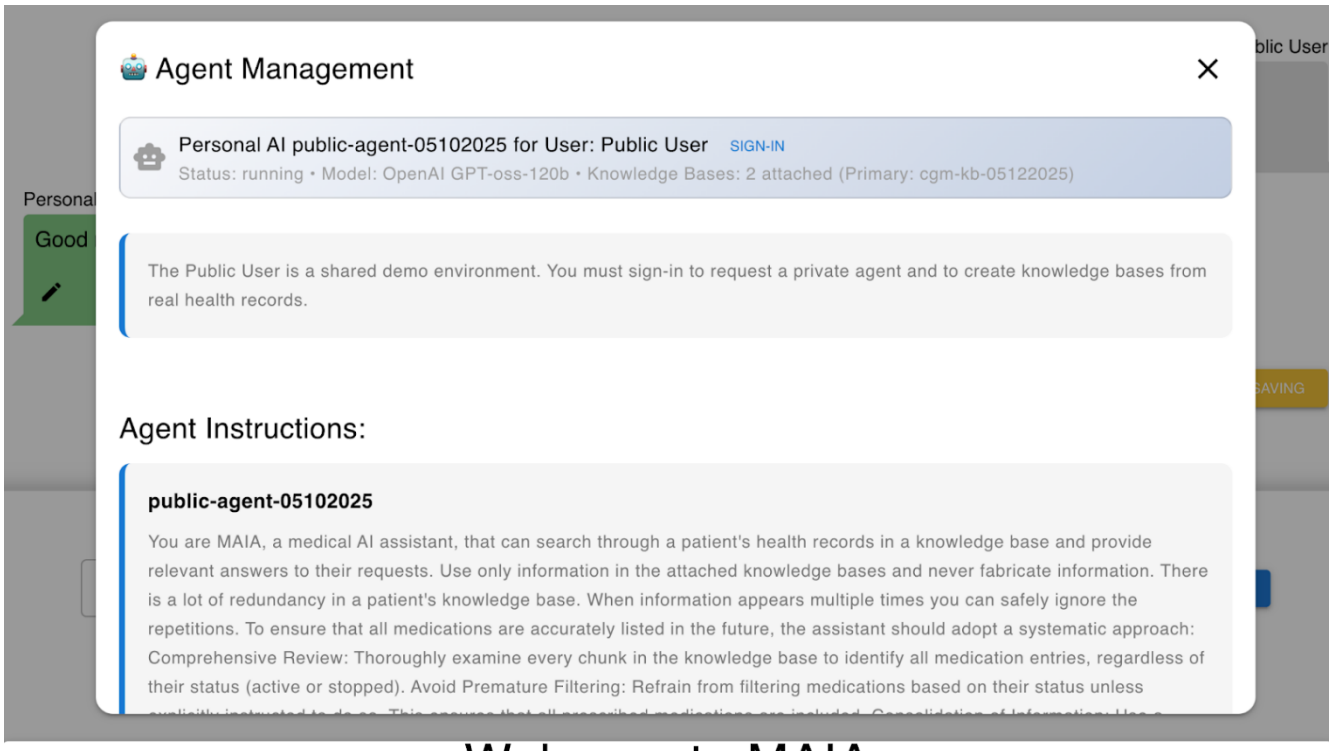
1. no limit to how many private ai agents you can have in the environment
2. different results from different agents
    a. multi agent system. for specific medical intelligence.

‘best diagnosis at the lowest cost’

are you willing to connect the llm to the system without the chat is an open question.

demo time: test.agropper.xyz





Welcome to MAIA

Your Medical AI Assistant

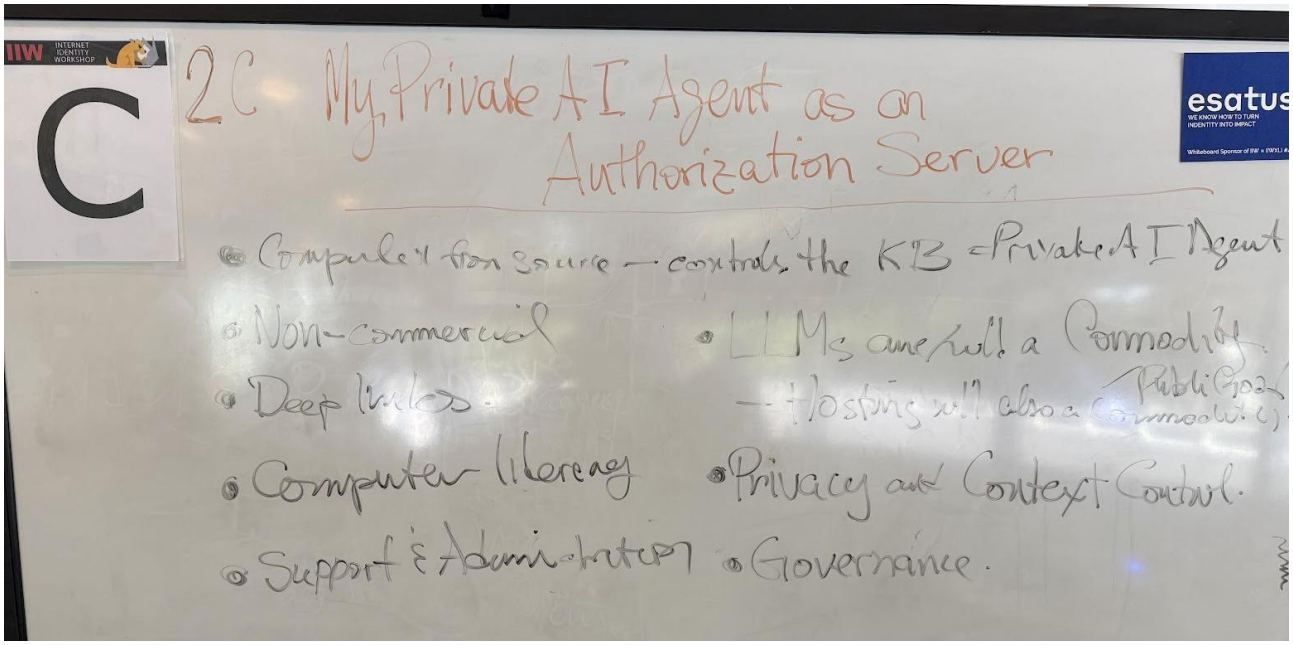
The Medical AI Assistant (MAIA) lets you choose from different privacy modes: Public, Supported, and Private.

Public is the default for new users. It allows you to become familiar with privacy features such as the differences between a private AI and a commercial AI like ChatGPT. A private AI has access to your health records and acts as a gatekeeper, so you can control what you share with commercial AIs.

Supported lets you use MAIA at no cost to you. When you sign in, the MAIA administrator agrees to pay for and maintain your private AI and records knowledge base. The administrator approves new accounts and provides technical support only. Your records will be private to you, the administrator and people you share a chat with. As with the public option, you and your private AI control what commercial AI can see.

Private puts you in complete control of your private AI. You will need to pay for hosting costs at Digital Ocean or another hosting service. For support, you will need to set up an administrator or participate in a community. Only you and the people you specify will be able to access to your MAIA.

I UNDERSTAND AND AGREE



Neither Social nor Enterprise

Session Convener: Justin Richer
Session Notes Taker(s): Frederik Krogsdal Jacobsen

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

OpenID Connect Distributed and Aggregated Claims: https://openid.net/specs/openid-connect-core-1_0.html#AggregatedDistributedClaims

Identity assertion grant type draft:
https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/

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

There are traditionally two classes of SSO.

In Social SSO, the user selects which IDP they want to use. There is very little trust, and the user can just sign up.

The user at the RP can be created just in time. User accounts can be merged based on e.g. email.

In Enterprise SSO, users can only login if they are allowed to by a specific IDP.
The customer is the enterprise, and they want to enforce policies, use SCIM, etc.

Problem: In partner-based integrations, there is a mix of both classes. As the RP, you only partially trust the IDP. E.g. you might want to allow them to login, but not to create new users or link existing users.

One option: some users can be marked as restricted such that they MUST use a specific IDP, while other users can login with either their enterprise IDP or their partner IDP.

If someone logs in using a partner IDP, how can you restrict the access appropriately?
You want more than *just* the user information to get authorization context.

There might be interactions between three parties: enterprise IDP, partner IDP and relying party. The hard interaction is for users that have an enterprise account, but want to do something in the context of the partner IDP. If a user with both types of accounts (unlinked accounts) comes from the partner and wants to SSO to the enterprise, how will that work? The accounts should be linked in a way that is understandable for the end user.

The GitHub model where a user can be added to an enterprise without the enterprise gaining control is sometimes problematic for enterprise compliance because it only allows for certain assurances (e.g. MFA restriction, but not physical location of user).

This might be solvable using OpenID Connect Distributed or Aggregated Claims (but nobody supports those). Also, this will almost certainly be SAML implementations.

Question: are there many partners? Potentially.

Question: why can't authentication and authorization be split? It kind of can be done using an identity proxy.

Could you use an identity assertion? Maybe, but not for SAML.

One design: anyone can authenticate with any IDP. Authorization is a separate process which is unrelated to the entrypoint of the authentication. But the session, applications, etc. do know which authentication was the origin of the session and can use this for authorization.

Question: What should enterprises be allowed to control?

Could it be done using a federation setup with the enterprise as the root of trust? Probably not, because the enterprise and the partners do not have a relationship.

Another problem: what if a user is part of several enterprises?

One solution: first ask for a user email, then display a selection of which enterprise IDPs are connected. This requires mapping between group concepts in the various IDPs.

Some partners also want to pass authorization information to the relying party. This is different from enterprise IDP because the “contract” of the enterprise situation is that the enterprise takes over all responsibility for mapping authorization correctly. With partners there is no insight into the authorization decisions on their end.

A problem is that when you have a “layer” of IDPs, how do you handle the ordering? One way is to merge all of this into one user concept, but that becomes a lot of work that scales badly.
If it was just about accepting multiple IDPs and merging them all together, that would be easier. The problem is whether the enterprise allows merging, and in what ways.

The problem is really an enrollment pattern. You want to first authenticate, then maybe allow the user. The problem is that CIAM platforms don’t support this in a good way. Keycloak can do it, but it is very complicated.

The solution to the problem is a way to inject some decision flow into the authentication flow to make a decision on how to proceed. One way to do that is by having many kinds of sessions, but that requires a lot of management.
Some people who have done this before.

It might be that only a few partners have requirements where this is a problem. The best way might be to solve the problem for most customers, then leave a few partners with “special” handling.
In the “weird” cases, it might be fine to do step-up authentication through the enterprise IDP.

Billing integration is another difficult problem which can be exacerbated if ownership of the account is unclear.

IEEE P7012 (My Terms) and the End of Corporate ToS

Session Convener: Justin Byrd
Session Notes Taker(s):

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

Link to slides (passcode: **IIW25b**): https://machisystemsllc-my.sharepoint.com/:b:/g/personal/justin_machi-systems_com/ETwWMG5RqVdPkgIO6hUnufUBGIvKF-p1zZhsOm0V1B2QXw?e=V6JYdb

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

🌐 **Stay tuned for more MyTerms sessions from Customer Commons & friends — where we turn privacy principles into real-world practice. Join the conversation, share your insights, and help shape what's next!**

Workshop Session: IIW XLII - Fall 2025 (VRM Day)
Title: How IEEE P7012 Obsolesces Corporate Terms of Service and Privacy Policies

Duration: 1 hour

Date: Monday, October 21, 2025 (VRM Day)

Time: 11:00 a.m. – 12:00 p.m. PT (Please arrive or join by 10:50 a.m. PT for setup and audio check.)

Location: Computer History Museum
1401 N. Shoreline Blvd, Mountain View, CA 94043

Agenda

- Opening remarks and introduction to IEEE SSIT and the P7012 initiative
- Overview: The concept of user-proffered privacy requirements and machine-readable contracts
- Guided discussion on the evolution of terms, policies, and negotiated digital relationships
- Open floor dialogue for participant insights and collaboration
- Summary and next steps

Facilitator
Host (In Person): Justin Byrd — Machi-Systems / IEEE SSIT 📧 justin@machi-systems.com

Session Description
This workshop will examine how IEEE P7012, Machine Readable Privacy Terms, challenges the dominance of corporate Terms of Service and Privacy Policies by enabling a user-driven model of consent and data control.

Following recent collaboration and discussions with Doc Searls and members of the VRM

community, this session builds on a central question:

When contracts proffered by customers to companies start with customers' own privacy requirements — and companies agree to those requirements — how far to the sidelines do corporate Terms of Service and Privacy Policies move?

We will explore how P7012 provides a technical and ethical foundation for negotiated digital relationships, shifting online agreements from one-sided corporate declarations to mutually respectful data terms defined by individuals.

The conversation will consider how this paradigm affects digital identity, AI ethics, and interoperability across trust frameworks, as well as the potential impacts for developers, policymakers, and standardization efforts.

Key Discussion Prompts

- What happens when individuals, not corporations, define the starting point for digital contracts?
- How can machine-readable privacy terms become a practical tool for consent management?
- What cultural and regulatory shifts are necessary to support negotiated digital relationships?
- How can P7012 interoperate with related efforts in VRM, MyData, and consent receipt ecosystems?
- What does implementation look like for organizations that agree to user-proffered terms?
- How can open-source communities contribute to early prototypes and interoperability testing?
- What challenges might arise in reconciling machine-readable standards with human-readable legal frameworks?
- Open discussion: Where should this work go next?

Closing Remarks

As we begin treating privacy as a proffered agreement rather than a compliance obligation, IEEE P7012 offers a concrete way to operationalize user agency in the digital world. This session invites practitioners, developers, and policymakers to consider what it means when the user, not the platform, starts the conversation.

Session Notes

1st Day, Wednesday

Second Session, Noon-1 PM

Led by Justin Byrd

This is the QR code to join a Signal group for those interested in info and helping.

Justin, co-lead of IEEE 7012, presented by sharing questions for the Customer Commons board to field.

- What happens when individuals define the starting point for digital contracts?
- How can machine-readable privacy terms work as a tool for consent management?
- What cultural / regulatory shifts support this change?

Doc Searls shared about the terms of service and privacy policies and how they do not work.

Nitin shared about how individuals regain agency. He shared the enterprise perspective. Sharing agency from the customer side, so you get a better signal. It's a creedo over time. You aren't suddenly going to get better information, but you do get better information by not surveilling the customer.

Bad theory says Doc Searls. He continued, "Loyalty cards, we want to know you better than you know yourself, and it doesn't work. Doc says I've gotten no good recommendations."

Nitin spoke about VRM converging with 7012. He talked about the demon of Ad Tech. How it came in and is now collapsing with the ad blocking. MyTerms is a start.

Comments

Curious about pilots, things being contemplated.

Silona (who used to work for the IEEE) had a question about third-party stuff and how it is so often hidden, especially with AI and the sneakiness with EULAs. No transparency and no traceability.

Joyce answered, the first thing is that when you offer your terms, the entity cannot track you off the site because you are the first party proffering the terms.

Proof of concepts and aspects of third-party to be shown off tomorrow, cryptographic contracts using a JLINC protocol with a QR code. Each third party has an identifier identifiable with the machine-readable terms. It's hashed and in the protocol layer.

There are a massive number of websites that are not involved in the economy and do not have terms, and they are the first market. Silona said she had to strip a ton of code that wasn't pertinent, so this would help.

A business case is for startups using this when they don't have privacy policies *now* at all. Simplifies and makes it straightforward.

Human-readable is nothing on this site.

The technical specs have to spell out what that means to me as a developer.

What can I do? Can I use cookies, give a cookie to someone else? Phil asks: Does the spec address this?

Is there any part of the spec for people in the previous world of privacy where people can transition? Is there a recommendation to transition on the customer entity side? We did talk about ways to help with adoptability.

Iain Henderson fielded some questions. He has been on the journey for 8 years with IEEE and years before that with VRM. "Current model is broken. Need to build a new state over there where things will work and is equitable, where two parties get together and have a healthy agreement. Essentially need to build a new world over there, built correctly. Contracts are built on 3 simple principles. We are gathering data. 1)Be Transparent (tell what doing). 2) Minimize what you are doing (don't gather more than you need). 3) Don't do more with the data than you need for your service. Bottom line. Let's get back to where we started in the 1980s.

Essentially, there are 13 agreements evolving, which is a bit too many rn/confusing. Probably 4 out of the gates. It's not for Amazon/big guys. The vast majority of the services in the world are not doing surveillance. Those not doing it are great early adopters.

The first organization to do it is MyData, a Helsinki-based non-profit organization. The team has been heads down on the mechanics with the specification. Now we have to build it. 4000 members with w/MyData – we have four months to get it going.

Brendan Miller with the Applied Social Media Lab at Harvard. He believes it could be a great place to try it out.

Joyce said we just tell you what the contracts are and don't say how it is supposed to be.

Marti Smith from the State of Utah says we can't control users who sign up for things. Policies and principles are essential.

JS – This is the moment in time. There are people ready for this. There are people in public spaces who want to protect their data.

There are some good nuggets in GDPR, the precision of definitions.

Q, I am an org and I take in content from a chat content and I meta tag it, share with an external 3rd party. 'Taking data beyond the expectation of the end user is what we are talking about.'

In legal terms, a lot of companies are using a 3rd party. If I'm a user, and I say no sharing, what happens with the 3rd party situation? Can that be proffered in the terms?

Definitions are in the standard. (Iain Henderson)

The individual is the first party in the contract, which is a complete flip to what is being talked about right now (Doc Searls)

Russ asks about partnering with Wix or Square or Shopify, or WordPress?

Nitin answered, Yes, all of these are places where we would want the technical aspect of this to be put into development while we work on the policy side.

Iain – we've been working on this for a long time. Coming out in Jan to a world that needs it. Need to increase the size of the team.

Day Waterbury – need to reinforce that there are lost causes and then move on. 100% to empower people to be the first power, but as the first party, I have locked down terms and that translates to magic loss. Won't that lead to people having more promiscuous terms because they don't want to lose out on the shiny objects? Won't it just revert to today's acceptance of the cookies.

Iain, yes, need to build up the whole ecosystem.

Phil – the other side of the convo with SETI, there is a whole policy question… state says this is what you have to do that prevents that kind of practice. Broader societal approach.

In the UK, the equivalent of Consumer Reports. Why do people keep checking the box? Ans. They are rationally disengaged. Bad signals, and the whole thing is bad. This is why I think we need to build this whole good thing over here.

Day – people are structurally in duress.

MyTerms can be an expectation as long as people like us push it forward right now.

Doc – we need to scaffold up another section of the Internet that is MyTerms-based and not surveillance-based. Lots have been written over the years. Market Intelligence that flows both ways. Use this info about our purchases to improve your stuff, but under MyTerms. You are in our loyalty program and get spammed forever. There could be a much richer system that is based on good faith.

Brendan Miller: Can we force companies to deal with our terms?

Yes, that is the idea of the contract.

This is perfect for Apple, btw, but we want to develop this further first.

The no's are recorded, and perhaps once it gets to the point of pain (Kari's interpretation), they will pay attention.

Jeff B: Flipping the switch by a little startup's idea. Set-top box concept. It might have been too early to market. Now it's distorted.

Link to slides (passcode: **IIW25b**): https://machisystemsllc-my.sharepoint.com/:b:/g/personal/justin_machi-systems_com/ETwWMG5RqVdPkgIO6hUnufUBGIvKF-p1zZhsOm0V1B2QXw?e=V6JYdb

Building Trust with AI / MCP Ecosystems

Session Convener: Chris Phillips
Session Notes Taker(s): Nicole Roy

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:

Chris Phillips
Nicole Roy
Chris Hubing
Paul Ashley
Jason Stoops
Alan Karp
Alan
Emu Izikawa
Fraser
David Trece
Gail Hodges
Sam Goto
Dmitri Zagidulin
Leif Johansson
Lisa Dusseault
Sarah Chechhetti
et. al

Building trust using OpenID Federation in the AI context - Chris will also have a demo table at noon tomorrow to show and tell.

Roughly 50% in the room are developers
Everyone in the room uses AI

“I want to be able to plug in different things” - MCP, A2A – extra layers of outreach / interconnections between “stuff” and AI.

Corporate networks, general users, etc.

Trying stuff out, ceremony of building trust with what you’re running.

“I don’t know if I really trust everything I’m able to run.”

Threat assessment

Risk due to prompt injection

Sensitive data use and knowing if I can trust AI with it

What cues do you need to see from the environment to know that something is trustworthy

I want to be able to audit MCP interactions

Being able to trust that third-party tools won't steal data…

Two agents representing a hospital in different capacities: Scheduling and medical advice. These are different trust profiles.

Code auditing / compliance for AI systems

Auditing of both agents and MCP servers

Leif says: "Trust does not scale" - Trust is always local

Trust has to evolve from local bubbles of trust

App store review as a signal?

Curation / curated environment: Example: Entra marketplace badges

Average users don't trust any of this stuff (yet) (which is good) (we think) - Google did a user study

Consequentiality - increasing levels thereof (gaining trust over time) - What things do we have to show users? Auditability, transparency, constant feedback loops with the user.

Consumer Reports also found a lot of this stuff - but also reliability is a huge problem.

Trust is contextual - "I trust my bank with my money but not with my children." Vulnerability: "In what way am I becoming vulnerable? The $5 transaction level of initial trust."

What are users developing a relationship with? Product? Company?

Highly unlikely that there will be no bad actors in the ecosystem. Users typically place trust in brands, technology is there to ensure that trust isn't misplaced.

Reputation-based trust

"I trust you but only as far as I can throw you."

What is the signalling of trust in this context? We have "reputation bankruptcy with humans, why is it any different with AI?" I have a sense of singularity with Chris because I've known him for years, but we don't have that with AI.

Standards, certification and conformance go into trusting the system.

Systemic conveyance of trust

Trust is nuanced

Where/what are the gaps?

“It’s complicated”

Beyond Identity and Okta working on MCP proxies to be able to whitelist clients and do governance around what is allowed in to be used in the enterprise.

MCP proxies

Layered solutions / API key wrapper / Policy Enforcement Points

“Undo button” / getting your stuff back if something goes wrong. Human evaluation of risk.

None of us know how real human users evaluate risk.

Trust is an emergent property of an ecosystem, it has nothing to do with technology of the system (for regular users).

Most people don’t understand that the word “risk” even enters into it.

How do we achieve systemic trust? Human evaluation of risk. AI agent-based evaluation of risk, but someone is held responsible.

Not really a tractable problem to solve by engineers. Too much trauma bonding among engineers. Need local trust roots. I want to be able to decide who my trust roots are, and they have to be available in any jurisdiction that I might somehow be part of.

No single hierarchy PKI anywhere. DNS resolves names, but it doesn't resolve trust well. BGP is multiple-root (internetworking).

I want to reduce the amount I have to trust by giving least privilege inherent in the UI.

How do we deal with enforcement of rules - in lax jurisdictions? Reason the Russian mafia operates out of Indonesia (example).

Leif says, for his use cases, can pick own trust lists/trust roots, so I can exclude roots that I don't trust.

Trust is a process, not a thing.

Need to get away from the browser model for trust - custom clients due to things like vibe-coding.

Harms We Care About

Session Convener: Erica Connell, Joe Andrieu
Session Notes Taker(s): Erica Connell

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

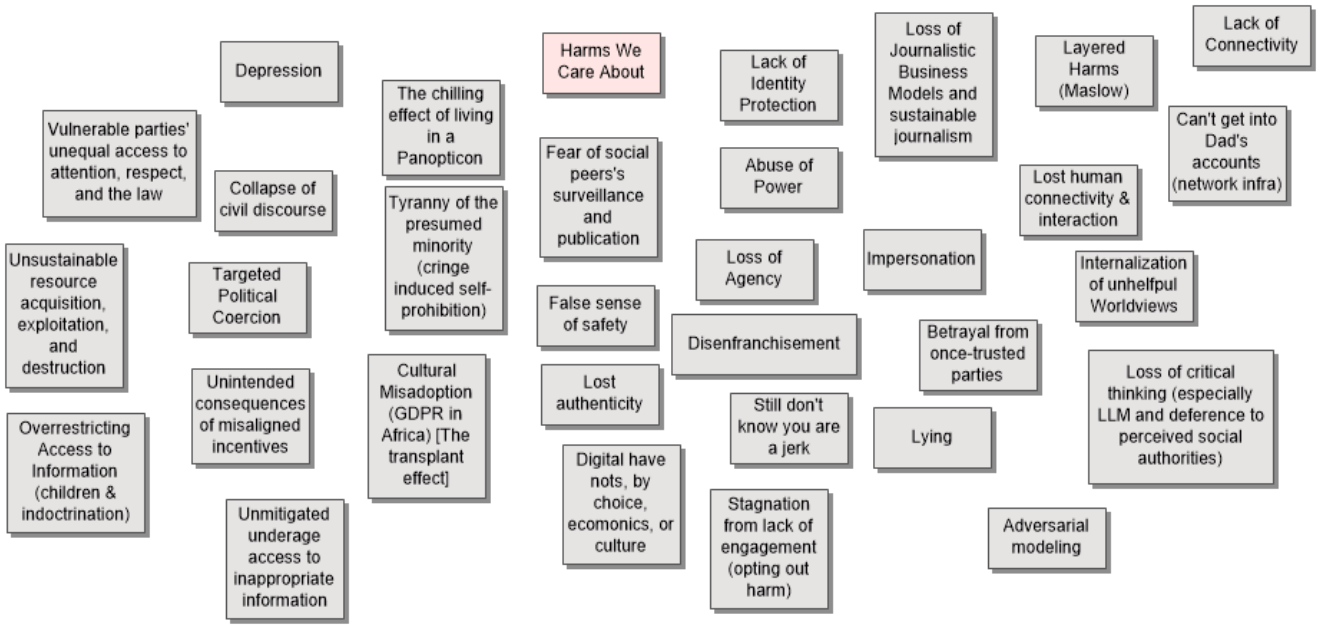
Identity harms

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

We discussed Harms philosophically, categorically, and practically.

2025.10.21 - IIW Harms We Care About Session

1. Brainstorming:
    a. Cloud cybersecurity
    b. Maslow hierarchy of needs - hierarchy of harms?
    c. Connectivity harm
        i. Inexcessibility due to AWS failure
    d. Truthtelling
    e. Financial
    f. Identity management
    g. Principles
        i. OICD made a statement of principles of statements of principles
    h. Level often left out
        i. Technical requirements
        ii. Is it a harm or a feature?
    i. Social harms
    j. Ramifications of living in a panopticon - constant surveillance
        i. Cringe culture - teens fearing violating the norms of the group
        ii. Authenticity is dangerous now, could result in bullying, etc
    k. Lying
    l. Digital submission
        i. What are the consequences of what we are doing?
    m. Role of critical thinking
    n. What do we do about the harms
    o. Where do the harms happen?
        i. When we build the tech?
        ii. When we use the tech?
        iii. When we educate about the tech?
    p. Categories of harms
        i. When there is a power imbalance that is abused to the detriment of the person(s) with less power
        ii. Risks are not harms
        iii. Harms coming at you externally
        iv. Self harms from tech choices you make
        v. Those around loss of free will
            1. Attention based to Intention based economy



OpenID4VC 101 & …..

Session Convener: Joseph Heenan / Kristina Yasuda / Paul Bastian
Session Notes Taker(s):

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

Slides presented are here:

https://docs.google.com/presentation/d/1VOWHrV_dBf4vHPCEtuXRYmxts9R5mjr2/edit?usp=sharing&ouid=107381980093922120275&rtpof=true&sd=true

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

Drivers License Demo

Session Convener: Francisco Corella
Joint work with: Suhni Chuhad, Pema Selden. Veronica Wognas
Session Notes Taker(s): Francisco Corella

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

A driver's license credential usable for website registration and traffic stops

An alternative driver's license presentation method

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

I presented slides describing a demonstration of a driver's license credential implemented as a JSON certificate, issued in full disclosure and selective disclosure formats, and usable for presentation at a traffic stop and for registration to a web site.

The audience was able to run the demo as I was going over the slides.

In a traffic stop, the QR code that the officer presents to the driver includes a challenge and must therefore be dynamic. Philip Quinlan pointed out that a dynamic QR code would be displayed on a small screen, and the driver would have to come close to it to scan it, which would be unsafe for the officer. After the session I found an alternative presentation method that uses a challenge for proof of possession, but where the challenge is not in the QR code. The QR code can thus be a large preprinted image that can be scanned by the driver from a safe distance. I presented this alternative at Day 2 / Session 10 / Room C.

Swiss e-ID "the least worst centralized government identity system?" & The Failure of Decentralized Identity (and what to do about it)

Session Convener: Christopher Allen
Session Notes Taker(s): Eric Scouten

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:

This is a recap of the blog post and slide deck posted by Christopher at Musings of a Trust Architect: Five Anchors to Preserve Autonomy & Sovereignty.

A few years ago, Swiss Post Office proposed a digital ID. Referendum voted it down.

Government went back and reworked to address system to address feedback. This passed by a very narrow margin in a recent referendum. Result is based on SSI technology, but is completely government-implemented (i.e. centralized). This system is open in the sense that other information _can_ be attached to government-issued digital identifiers; closed in the sense that only government can issue these credential.

Law *says* that digital identifiers are **not** required, but Chris is skeptical. The implementation will turn out to make physical identifiers into second-class citizens.

Swiss cultural concerns are largely about how the platform vendors (i.e. Android and iOS) will have an outsized ability to use data obtained through those credentials.

The TLS warning: Once you ship something, "good enough" becomes "stuck with it." TLS 1.0 was ratified in 1999 with some known problems. Problems weren't fixed until TLS 1.3 in 2019. (Gulp.)

Love this quote:

*If a system cannot hear you say no, it was never built for **us.** It was built for **them.***

Chris describes this as "the least worst implementation" of a government-backed digital ID system.

Swiss ID system doesn't have a well-established right to refuse participation.

What are Transaction Tokens?

Session Convener: Ashay R, AWS
Session Notes Taker(s): Mike Schwartz

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

Atul Tulshibagwale and George Fletcher, two of the authors of the spec, were co-presenting with Ashay.

DataTracker Page: https://datatracker.ietf.org/doc/draft-ietf-oauth-transaction-tokens/

See Identerati Office Hours Episode 116: https://github.com/GluuFederation/identerati-office-hours/wiki/Episode-116

Transaction tokens are obtained using token exchange flow, and are short-live and designed to be limited to one trust domain, for example, "retail-services.amazon.com".

Transaction Token Claims:

iss:
OPTIONAL The iss claim as defined in [RFC7519] is not required as Txn-Tokens are bound to a single Trust Domain as defined by the aud claim and often the signing keys are known. The iss claim MUST be used in cases where the signing keys are not predetermined or it is desired that the Txn-Token Service signs with unique keys.

iat:
REQUIRED The issued at time of the Txn-Token as defined in [RFC7519]

aud:
REQUIRED This claim, defined in [RFC7519], identifies the Trust Domain in which the Txn-Token is valid. This identifier MUST uniquely identify the Trust Domain to prevent the Txn-Token from being accepted outside it's current Trust Domain.

exp:
REQUIRED Expiry time of the Txn-Token as defined in [RFC7519]

txn:
REQUIRED A unique transaction identifier as defined in Section 2.2 of [RFC8417].

sub:
REQUIRED A unique identifier for the subject within the context of the aud Trust Domain. Unlike OpenID Connect, the sub claim is NOT associated with the iss claim.

purp:
REQUIRED A String defining the purpose or intent of this transaction.

tctx:
OPTIONAL A JSON object that contains values that remain immutable throughout the call chain.

rctx:
OPTIONAL A JSON object that describes the environmental context of the requested transaction.

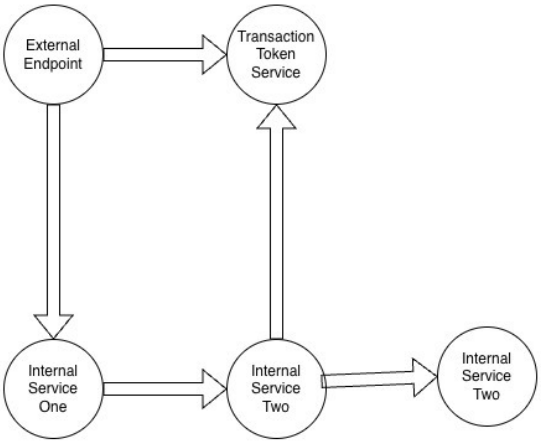
The JWT payload MAY contain other claims (although the spec doesn't explicitly say this at the moment).

The tctx claim contains a JSON value related to the transaction. For example a non-normative example from the spec:

```
"tctx": {
 "action": "BUY", // parameter of external call
 "ticker": "MSFT", // parameter of external call
 "quantity": "100", // parameter of external call
 "customer_type": { // computed value not present in external call
  "geo": "US",
  "level": "VIP"
 }
}
```

Any authorization system would need to know what the payload of the tctx means.

One of the main reasons for transaction tokens is to prevent internal APIs from ever accepting a token (or cookie) that is exposed to the browser. The token exchange part prevents many stolen token attacks, where an exfiltrated token is presented at different upstream APIs. If these API's only accept transaction tokens, then no stolen cookie can be presented, and the impact of the stolen token is minimized.



This diagram was used to work through a flow of how passing a tx_token to downstream service may involve additional token exchanges.

SESSION #3

Email Verification Protocol

Session Convener: Sam G & Dick Hart
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

Authorization 101

Session Convener: Steve Venema
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 101

Session Convener: Eric Scouten
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:

Discussion followed my slide deck (PDF).

Building a Multi-Agent Research Tool and Framework For Blockchain Governance and Standards using First Person Project

Session Convener: Mitchell Travers
Session Notes Taker(s): Haruki Oyama

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

bgin.ai

https://gamma.app/docs/Building-a-Multi-Agent-Research-Tool-and-Framework-for-Blockchain-32kkzbl0me7hg0s

https://bgin-global.org/events/20251015-block13

https://sync.soulbis.com/s/bgin-agentic-framework-archive-codex

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

https://docs.google.com/document/d/1HdYYbvddD78WNzPpT9lbl_rQYduYg8Y-acBtHBFnLJk/edit?usp=sharing

Presenter starts introduction about himself and bgin
Quick brief on bgin
- Better governance and standards around decentralized ecosystem like blockchain
- Build common ground and common language
- Tries to be this venue for multistakholder conversation

Last 6 months: building multiagent tool integrating first person project
Briefly describing the first person project
Starts talking about multiagent system
- Archive(RAG), codex(codebase), discourse agent

? Is Aira involved
- Yes, aira is the organization involved in managing the trust registries
- BGIN is one layer below that

? What makes this an agent as opposed to software
- We run the LLM within TEE and the three agents are communicating with each other

? Still do not understand what the word “agent” means here (as an agent you need to have it owned by someone)
- Separate from the 3 agents with its own right, people have their each agents

? Clarify the use case around blockchain
- Example: CS information sharing framework

? Chatham house rule needs to be said in a certain way so that information isn't accidentally revealed. There are challenges in automating this process.

Agents will be used to parse it
? LLMs take shortcuts, why not just software
Create better feedback loops for participation
"A lot of your work is being cited right now among the prompts"
Comment: Standards do not reflect intent
Starting point of agentic project: If there was a way without revealing who it was that contributed most, still attribute work to those that contributed

Segways into privacy pools
Should use the same cryptographic primitives as agentic framework
Talks about BGIN agent hack
System chat history and context refresh
Technical standards integration
VCs are the priority bc DIDs are hard to implement
This agentic framework can be applied to other governance bodies (just fork from BGIN)
Economics of framework (e.g. incentives and rewards)

Starts DEMO (on screen and on user devices)
Explains various features of the website and different WG rooms/chats

? What is the relevance of trust over IP in this?
Acts in layered ways to act in trust, if for instance BGIN contributes to Eth standard 8004 they would be contributing to one of the layers of the trust over IP protocol.
? Is this open source? Who is managing?
Managed by BGIN for the world (non-profit). It will become open source.
Currently funded by speaker
? Needs clarification of what is going on in the session currently
Enables standards development with added privacy and LLMs are there to add to the intelligence
? Are we building wikipedia
To an extent, decentralized, anonymized wikipedia
? What does the agent do
Explain the role of the three agents
Motivation: Memory and discussions are lost during WG discussions
? What do you anticipate as the end user, who is deploying the system
You can deploy as an individual or a foundation
Comment: When doing a standard you start off with the use cases so at first it is not necessarily technical, this would be wonderful to gather all the side knowledge especially regarding the technical specifications, saves work from having to copy paste and rewrite all the necessary information from one platform to another. The agent may capture the intentions.
Presenter explains additional use cases of the framework
Comment: By using the word "agent" in the presentation, the presenter is causing confusion at the start
Presenter should have said "shared research platform"

Why is there an agent? What is an agent doing?

You could theoretically replace the agents with your own consultant

Comment: Do not drop the agent bit, it makes money (laughter)

Comment: The use of homomorphic encryption implies a particular privacy architecture. It is hard to get a gist of the picture of how the features of the service fits together.

Comment: You can do agents that are internal, you are just assigning themselves their role

Comment: Homomorphic encryption would be taken out if I were to use it internally

Comment: But I would because even locally the data should be encrypted to prevent unauthorised access

? How did you integrate First Person Project

Not yet

? Why First Person Project

To presenter it is the most elegant and it has many alignments with people being able to create their own agent, can build credential interoperability, like people come to WG has their FPP connected to the Agent services.

? Who is in the IKP WG at BGIN

Mitchell and Nat Sakimura

? When will the first person agent go live?

A participant summarizes the project in their own words to clarify the talk so far.

? What's the choice of division of the 3 agents? Those choices will likely not cover all use cases

They have to start somewhere. Presenter will de-emphasize the word "agent" moving forward.

? How can codex interact with other systems

It would have knowledge and implementation know-how about external systems in the real world.

? Do you think the first person project will launch soon?

People do not know

Presenter wants for the bgin to be one of the first first person project adopter

FPP can be used to store credentials on their own and present that to somebody else

This project tries to harmonize the crypto world where people do not communicate with each other.

? How will you protect against buying votes and buying reputation? In the real world off-chain, how would you protect against plutocracy?

Having a granular contribution matrix means you get more composable credentials that make it harder to attack.

Create a positive financial attribution set that enables financial privacy within a group of people (merging of financial and data privacy via privacy pools)

? Is there a documentation

https://sync.soulbis.com/s/bgin-agentic-framework-archive-codex (details the values and philosophy to go back to when vibe coding the project) Started with philosophy and then into implementation, what are the right primitives (such as FPP and Trust over IP)

SEDI Guardianship & Delegation

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

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

Slides: SEDI Guardianship & Delegation.pptx

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

Type You Notes Here

Your words are your identity

Session Convener: Ben Curtis
Session Notes Taker(s): Ben Curtis

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 discussed how VCONs, the new IETF standard for storing conversations (email, text, WhatsApp, and voice) so they can be processed by standardized tools will impact everyday people, and the effect it can have on identification of individuals. Many positives were discussed for how VCONs can help individuals and business, but the following concerns or ideas were discussed:

- Recreation of identity via metadata or biometrics
- Reports and transparency around exposure
- Authorization/access to data

Platform-independent Identity Wallets

Session Convener: Stina Ehrensvard
Session Notes Taker(s): Nicole Roy

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:

Stina Ehrensvard
Nicole Roy
Bryce Fry
Johan Shellstrom
Mike Schwartz
John Bradley
Jim Fenton
Ryo Nakashima
Heather Flanagan
Chris Hubing
Ken Watanabe
Karen VanExel
Leif Johansson
Ananya Ravipati
Hideaki Fuyukawa
Steve Zoppi
Mike Jones
Nat Sakimura

SIROS Foundation (siros.org)
Powered by passkeys and open-source

wwWallet

wwwallet.org

Intent: platform-independent wallet for verifiable credentials

Intro: A new identity system for Europe

- Common digital identity for EU by 2026
- Hundreds of organizations engaged in pilots
- wwWallet has emerged as one of the leading solutions in the EU DI wallet pilots
- Part of the large-scale digital challenges in the EU for 2020-2030

SUNET, GUnet, yubico, SURF, ISRG, SIROS

Three-party architecture: Issuers, wallets, verifiers (relying parties)

“What if you could do a wallet just based on passkeys?”

Most people think of wallets as a mobile phone-based construct, but why does it have to just be that?

Stina Ehrensvard - founder of Yubico, stepped back as CEO and founded SIROS Foundation (non-profit) with Leif and Nat. Gather advisors from all over the world on what we need to do better.

EU vision of user controlled identity

- Credentials transferred to a mobile or web app
- User shares the data needed for the service
- Options include: Verified and pseudonymous
- Wallets not just for national eIDs / mDLs - starts there but also envision commercial uses for these wallets

Series of consortia to engage in “large-scale pilots” around wallet ecosystem. Testing different assumptions about how wallets would work in different scenarios. Looks chaotic because it is. EU regulation engagement is by its nature chaotic. More like a negotiation by member states than, say, US federal legislation.

“What if we tried to build a wallet in JavaScript, what could it do, what couldn’t it do?” Initial lab experiment, turned out that it could do quite a lot. Worked with colleagues in SURF, GUnet. Could even do things like in-person proximity flows. Where we need native API access is very small. The passkeys we have today could almost do everything we want/need.

Fully standards-compliant EUDI wallet based on FIDO passkeys, OpenID, ISO 18013-5, eIDAS

Zero-knowledge proof still needs standards

Primary security device for the wwWallet is a passkey or a webauthn token

Does the RP need to trust the wallet? Trust models are an open issue and evolving question. In real-world deployment there will be so many use cases where you have to do delegation, and things like document signing mean you’ll have multiple keysets controlling credentials/wallet, that you’ll have different constructs.

In the US, relying parties don’t trust the states. Therefore the issuer isn’t trusted. In Europe we have a very different model. The verifier’s trust is in the issuer. RP’s can’t understand every wallet. Trust the credentials issued by the trusted issuer.

Even disclosing what the wallet is, is a privacy violation.

American banks want attestations from the wallet.

In the German pilot, used the trust root that the German government wanted.

EU mandated that by 2026, (probably more like 2028) every EU member state must have a process for eID issuance into wallets. Rooted in the highest-level of trust, like a passport.

Passkeys are part of the trust model.

The wallet-secure cryptographic device/agent needs to be eAL level 4 certified.

At first, passkeys on their own weren't sufficient to do this. Worked on the browser PRF extension, which is now used by password managers.

Blob of your credentials is encrypted with a content encryption key, which is wrapped in each of your passkeys that you use to authenticate. Added a raw signing extension to webauthn to enable you to create derived keys off of a passkey and the private keys never leave the secure element.

Wallet follows you around, can be synced to other devices without worrying about the platform having access to the wallet's contents.

Zero successful phishing attacks against passkeys during a round of measurement involving 350,000 hijacking attempts (Google research)

Google saved 50m dollars using yubikeys - 0 account takeovers, 4x faster login, 92% support reduction.

Paper: "Security Keys: Practical Cryptographic Second Factors for the Modern Web"

Gartner found the same

Built-in and hardware working together:

- Syncable passkeys
    - No extra hardware needed
    - Easy for android, iphone ecosystems
    - medium-level security backup
- Hardware passkeys
    - Hardware delivery strengthens user verification
    - Works across all platforms and devices
    - Works for shared devices and legal identities
    - Affordable, robust …

Passkeys solves many challenges

- common id wallet:
    - built for mobile
    - cross-device access is hard
    - mobile device or cloud secure element

    - platform privacy issues
    - centralized data collection
    - ony natural persons
    - costly HSMs for data protection
- wwWallet - leveraging passkeys
    - built for the web
    - works across all platforms
    - any computing device, shared
    - both built-in and hardware passkeys
    - no vendor or platform lock-in
    - no central collection of data
    - both natural and legal persons
    - free, open-source components

Web is also good at experimenting with UX

We don't know, today, what the right UX is for telling users what's happening in these user flows, so with the web, we can rapidly improve that as we learn things. Will be highly-contextural, situation-dependent, not just a single UX flow.

Moves the critical security components from the cloud to the edge. The cost of deploying wallets at-scale is unsustainable with cloud-based HSMs. The number of transactions is immense. Today, the hyperscalers who have HSMs all build their own hardware.

We spent all this time to go from a two-party to three-party model, and then rely on a cloud-based issuer, verifier and credential management. That's not what we want or need. Makes no sense.

Security, privacy, cost, usability are the four pillars we need. Reliability is also a good one to add.

Initial pilot partners:

- German EUDI competition
- Success in first EU pilots (DC4EU, etc.)
- We Build consortium (legal person ID wallets)
- Interoperability CA (Canadian (Quebec)/French APTITUDE)
- Legal person ID wallets
- Sweden-Singapore pilots
- OCCRP 1,000 journalists - secure whistleblowing
- STM - international academic publishers/authors

Delegation is super easy to do - example: Legal power of attorney

UX model for oauth flows is underdeveloped

SIROS ID - "AWS for ID wallets'

- wwWallet as a service
- Native apps that can be connected to multiple wallet provider instances

- Facetec first to provide NFC passport + liveness
- Limited number of free YubiKeys for initial pilots
- Launch planned for late 2025

Can offer whitelabel wallets-as-a-service

SIROS ID - zkp projects

- Device-bound BBS for wwWallet and yubikeys
- Cleanroom implementation of longfellow-zk in rust for web assembly
- Striking a balance between issuer and wallet complexity

circuit proofs vs bilinear pairings

How do you engage?

Open source
https://github.com/wwWallet

Presenting CoralKM A user friendly protocol for decentralised Key Management and Recovery

Session Convener: David Gildeh
Session Notes Taker(s): David Gildeh

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

Slides: CoralKM Protocol
Repo: https://github.com/CoralStackCom/CoralKM

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

- **Overview:**
  - CoralKM is a DIDComm protocol for wallet recovery. It is designed for everyday users to easily onboard and manage Guardian's without having to have any technical knowledge of how it works behind the scenes. It also has a
- **Protocol feedback:**
  - Interesting approach, using namespaces to coordinate recovery without revealing guardians is unique
  - Have you thought about what happens if a Guardian revokes the Wallet after accepting Guardianship? (i.e. Bank decides they no longer want to be a Guardian for a user due to regulations/KYC issues)
    - No, but that is an example of where I need help fleshing out the protocol to a V1
- **Next Steps**:

Looking for more feedback and help. Please contact me (david@angelfish.app) if you want to work with me on fleshing out the protocol and getting the first version published

Four MCP Use Cases (with distinct identity considerations)

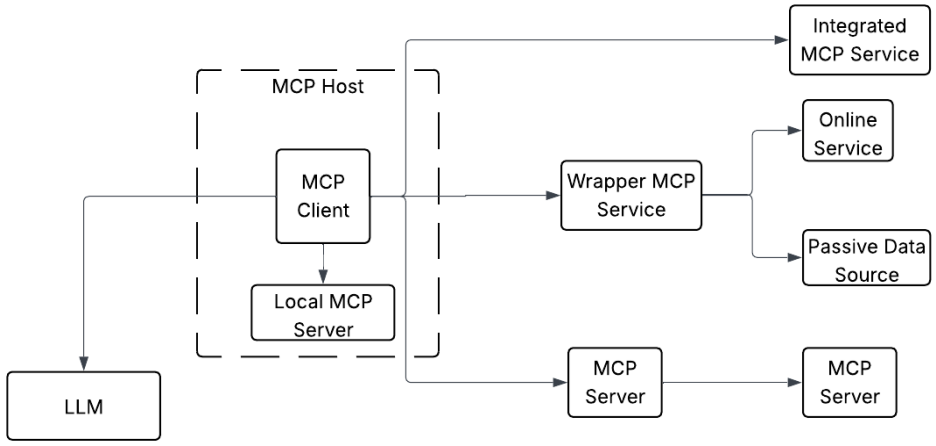
Session Convener: Atul Tulshibagwale
Session Notes Taker(s): Nick Dawson

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

- Agent Payment Protocol (AP2)
- Model Context Protocol

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

This is the general architecture of Model Context Protocol used for the purposes of this discussion.



We discussed four examples for agents using MCP, Human in the loop, no human in the loop, no human identity, and chained MCP services which could involve all or any of the above.

Tools for Traps - Managing Identity and Intention on Our Terms

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

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

Tools For Traps

Managing Identity and Intention On Our Terms

When we are connected to the digital landscape we are observed in some form(s) and fashion(s). It is fair to say that we have an identity of some sort applied to us. This identity is what could be thought of as a session identity. From the moment the device touches the connected realm, aspects of that device define that machine in those moments of connection. The device's own hardware, hardware drivers, software installations, the data associated with the account you logged in with, ip addresses, LAN MAC addresses, WiFi MAC,…create a specific session related to a specific device entity which is often operated by a person. An identity related to many things forms each time.

How can these spaces be occupied in a way that avoids system profiling funnels and the herding and nudging created by those forces? When we look at screens to operate on the other side of the glass, controlling intention while managing the degree of identity we wish to express, and how that is expressed, is a lot to think about. On the digital landscape that seems wildly complex to have to track, yet we do that all the time as we move through our lives in the Real World (RW). Spidey Senses work better here than there.

A simple mouse trap illustrates a want conveniently placed. As that want, let's call it bait, a signal releases potential energy and the hit is made…or not. With systems able to know what appeals to us and considering system designs built to move us, how can we avoid the allure of being baited. The tooling available is relative to the goal, the landscape related to that goal and the method(s) used while in pursuit of the goal.

Example: I want to hear a broadcast available which not only streams the show for internet connected devices, but also broadcasts on FM, AM or Shortwave radio, I have two very different approaches to getting that feed with or without being scoped by a system. Can you guess which is more residue free? What is the data cost of the differing paths to make the goal of listening to a broadcast.

Let's talk about the web and journeying there. Just like driving a car, the web is very similar in the sense that a browser (Brave, Firefox, Edge Safari, Chrome) used to surf the web is same as the idea of a car travelling the roads. Let's apply that thought framework to the digital realm.

To the car analogy: If I want to travel (browse) the web without having stickers (cookies and trackers) put on my vehicle (browser) it would be cool to have a car that rejects stickers being put

on it everywhere it goes. Some web browsers and add-ons are designed to help your web browser defend against your vehicle being stickered.

Not signing up for certain types of relationships like social media or purchasing is a tooling strategy. Choosing to sign up for relationships and adjusting the settings to match your preferences is a further example of engaging those system forces on your terms. Choosing not to sign up is another tooling choice for your larger relationship with IT systems which would be referred to as Your Real-IT in this space.

The cost of avoiding these systems and their forces may be being left out by community. In social media landscapes "The Tyranny of Convenience" (Tim Wu article) where the One-To-Many (one post to many eyes since it pops up in everyone's feed) allows for one to post news and info of their world, while missing the sense that those not in the space of that system will not see or hear of it except by second hand if at all.

Much more to say:

My Terms (IEEE 7012) terms granularity removes the default hook points favoring the house and that often are mandated in the All or None contracts of "take it or leave it".

Photographic Journalism: even framing a photo to not capture street signs helps defend against fraud; NorCal Fires 2017

NASA JPL Extraterrestrial Return Protocols related to concept of bringing other worldly things down to Earth; AI like bringing an alien back from space for people to lick or not so much…

_

Rashmi Siravara: Tools to traps was one of the best sessions in play with real time experience of the concept.

The use of

Goals
Landscape
Tools Sets
Persona to identify and categorize traps was phenomenal.

Human Behaviour interplay with the OS was in reach of accuracy. Manifestation techniques co-related to the traps was touched upon to explore this topic further in IIW-42.

SESSION #4

Threats + Mitigations Persistent State-Issued Citizen Entitlements (SEDI) Trade-offs (KERI-ACDC) Security

Session Convener: Sam Smith
Session Notes Taker(s): Kent Bull

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:

Attendees: 11

Sam: If you have unlinkability then you cannot have security because you cannot detect compromise.
Hart Montgomery: I see what you are saying, yet I disagree with you about the tradeoff.
Sam: It took me about three years of working through and thinking through this to realize and accept this. Provable linkability, beyond the means of zero knowledge proofs, means that what we call “unlinkability” is a weak form of unlinkability and is usually intellectually dishonest.

Persistent, widespread, high value, entitlement system:
Highest ROI to attackers = Highest susceptibility to attack.
Highest susceptibility means ALL vulnerabilities will be exploited eventually.

Survivable Security is a thing - this is a military term.
Survivability:

- Susceptibility - the likelihood of being attacked
- Vulnerability - likelihood of success and extent of harm given an attack
- Recoverability - likelihood and extent of recovery from a successful attack

Most targets on the internet are not compromised because of low vulnerability. Rather it is because of low susceptibility due to being not worth attacking. Most targets on the internet are highly vulnerable.
Susceptibility steps from ROI of an attack.

There is a trap of confusing low susceptibility with low vulnerability.

Design Spiral to Explore a Trade Space (diagram) - see the slides

Open Loop Models for Entitlement Verification
Issuer-Holder-Verifier Model with Verification using Verifiable Data Registry
There is no closed loop between the issuer and the verifier.

Best practice is to use secure signing hardware (TPM, HSM, Secure Enclave)
Asymmetric keypairs created/stored in secure hardware
Private key never leaves hardware
Weakest vulnerability is the AuthZ infra, not the signing hardware (typically OAuth/OIDC/SSO based)

Attack on Signing Authorization

- Compromise AuthZ infra to get fraudulent but perfectly verifiable entitlements
- Typically permissions are repudiable, as they are bearer tokens, thereby creating plausible deniability
- Plausible deniability = incentive to suborn employees

Statistics from Crowdstrike's 2025 report:

- Breakout time avg. fell to 48 minutes (this is the escalation, not the initial break in)
- Voice phishing up 442% between first and second half of 2024
    - Known as a "hands on keyboard" attack
- Initial access attacks 52% up in 2024. Access broker offerings increased 50% year over year. An access broker is someone who sells access controls on the black market, bearer tokens, usernames and passwords, etc.
- China-nexus activity surged 150%; targeted industries 200% to 300%

Passkeys 101

Session Convener: John Bradley
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

K-ARF Open Framework Digital Identity Infrastructure for 'South Korea

Session Convener: Jinyoung Jun from Hopae
Session Notes Taker(s): Bart van der Geest

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

Original Resource: K-ARF_Korean_Architecture_and_Reference_Framework.pdf

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

The Six Inversions

Session Convener: Christopher Allen
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

Digital Fiduciaries - What should they KNOW?

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

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

https://digitalfiduciary.org

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

We discussed the idea of a professional class, called digital fiduciaries, who are trained, certified, oath-bound professionals empowered to help with matters of identity, putting the interest of subject individuals above their own. In the same way that a doctor or lawyer is a trusted advocate in their domain, digital fiduciaries are trusted advocates in areas of identity.

Our intention was to discuss the knowledge that would be expected to be known by digital fiduciaries, the curriculum to train and test against.

However, most people aren't familiar with the notion of digital fiduciaries, so we spent the hour mostly discussing how DF might fit into a more robust, reliable, and respectful form of decentralized identity.

In particular, we talked about the role a DF might fulfil as the identity assurance agent who checks private, personal documents in a verifiable, auditable manner. By showing up in person, and

verifiable LEI (vLEI) Ecosystem Update

Session Convener: Karla McKenna
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:

Scroll down for Slides

Agenda

1. How do the LEI and vLEI deliver secure, certain and verifiable Organizational Identity?
2. Enabling identification, permissioning, authentication, and digital signing – application examples

GLEIF

GLEIF

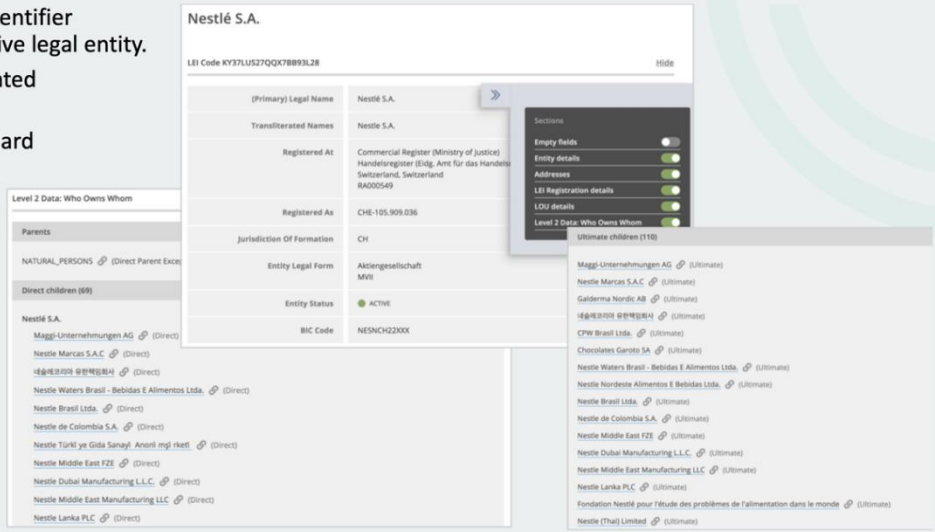
Enabling global identity
Protecting digital trust

How do the LEI and vLEI deliver secure, certain and verifiable Organizational Identity?

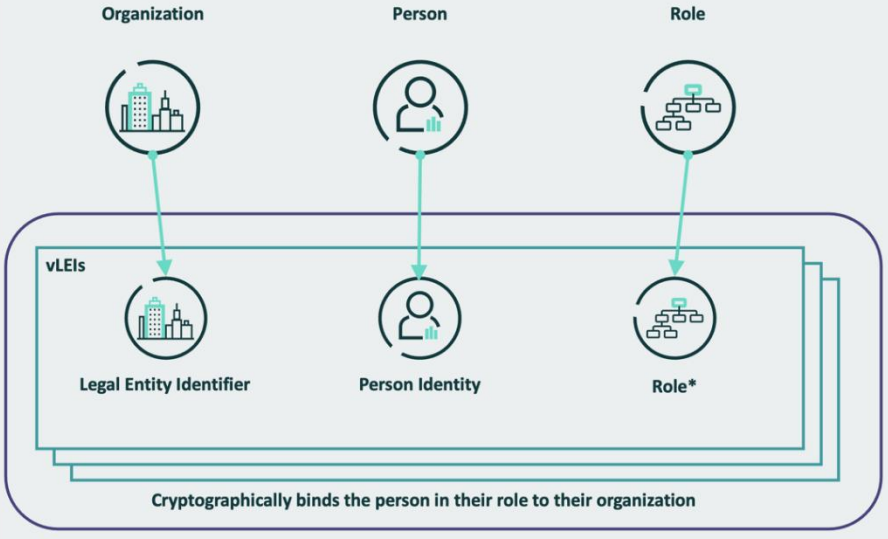
GLEIF

Identifying organizations with the LEI

- The LEI is a life-long identifier **owned** by the respective legal entity.
- It points to the associated reference data.
- The LEI is an ISO standard ISO 17442 – Part 1.



Identifying organizations and representing the connection among Organizations, Persons and Roles

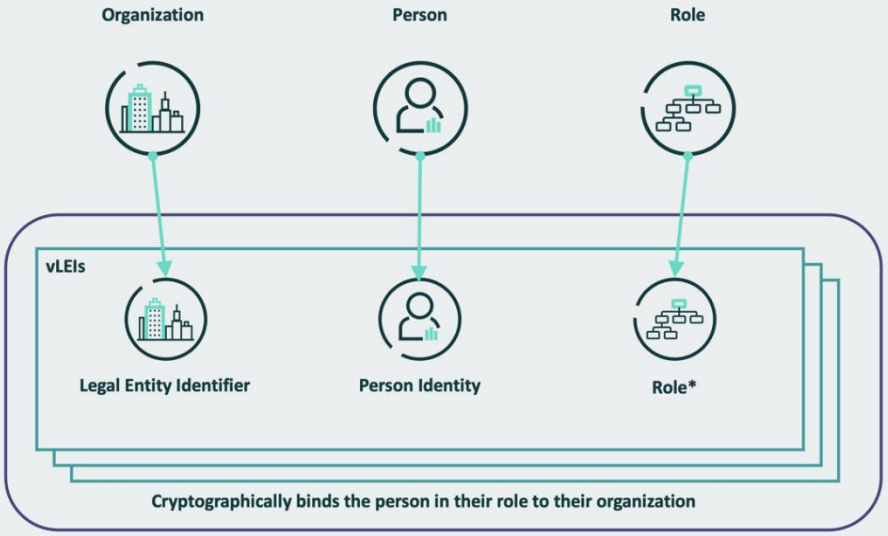


Real World

Digital Representation

- Two types of vLEI Role Credentials
  - For official roles- Official Organizational Role vLEI Credentials
  - For functional role – Engagement Context Role vLEI Credentials

Identifying organizations and representing the connection among Organizations, Persons and Roles



- Two types of vLEI Role Credentials
  - For official roles- Official Organizational Role vLEI Credentials
  - For functional role – Engagement Context Role vLEI Credentials

Digital Tools Features Analysis

Digital Tools Features Matrix: Signing

Features	vLEIs as Authentic Chained Data Containers	First generation Verifiable Credentials	eSeals	Digital Certificates
Digital Signatures	✓	✓	✓	✓
Persistent Digital Signatures	✓	✓ only those VCs on a blockchain	×	×
Single Level Issuance	✓	✓	✓	✓
Delegable Authority/Multi-level Issuance	✓	×	×	×
Non-repudiability	✓	✓	✓	×
Signing logging	✓	×	×	×
Signing in Full and in Part	✓	×	×	×
Horizontally-scalable Signing Infrastructure	✓	×	×	×

Digital Tools Features Matrix: Verification

Features	vLEIs as Authentic Chained Data Containers	First generation Verifiable Credentials	eSeals	Digital Certificates
Verifiable Provenance to a Global Root of Trust	✓	×	×	×
Instant Revocation State Verification	✓	✓	×	×
Decentralized Revocation	✓	✓	×	×
Privacy-respecting Revocation	✓	✓	×	×
Revocation by Any Party within the Chain of Authority	✓	×	×	×

Digital Tools Features Matrix: Security

Features	vLEIs as Authentic Chained Data Containers	First generation Verifiable Credentials	eSeals	Digital Certificates
Multi-signatures	✓	×	×	×
Secure Custodial Key Management	✓	×	×	×
Key Rotation	✓	×	×	×
No Reliance on Web Security	✓	×	×	×
Post-quantum proof	✓	×	×	×
Zero Trust Architecture	✓	×	×	×

Digital Tools Features Matrix: Global Applicability

Features	vLEIs as Authentic Chained Data Containers	First generation Verifiable Credentials	eSeals	Digital Certificates
Decentralized Authority	✓	✓	×	×
Globally Trusted Credentials	✓	×	×	×
Global Root of Trust	✓	×	×	×
Global Governance	✓	×	×	×
International Standardization	✓	✓	✓	✓
Multiple Roots of Trust in a Single Ecosystem	✓	×	×	×

Important points to take away from Digital Tool Features Analysis

- **Global applicability**
  - Identification of organizations with the LEI uses an internationally recognized global standard (ISO 17442 Part 1)
  - Digital signing with vLEIs uses anticipates the approval of an internationally recognized draft global standard developed by XBRL International D6 Working Group
  - Standard LEI XBRL taxonomy can be included as part of broader XBRL taxonomies
  - Authentication, Permissioning and Verification of organizations with vLEIs uses an internationally recognized global standard (ISO 17442 Part 3)
- **Unparalleled cryptographic security making vLEIs post-quantum proof leveraging**
  - Root of trust with Linked credentials requiring multiple layers of infrastructure to be compromised
  - Linked credentials with multi-signature feature and stronger identity authentication at issuance
  - No reliance on web 'security'
  - Key pre-rotation/rotation/ability to recover keys

- **Verification**
  - Automated decentralized verification of key state instantly indicated if a credential has been revoked
- **Plus . . .**
  - the ability to verify the connection among Organizations, Persons and Roles
  - only digital tool with the capability to bring verification down to persons
  - Enables organizations to leverage credentials with delegated authority both within and outside the organization

Qualified vLEI Issuers Update

- **8 QVIs currently**
  - 6 based in Asia
  - 1 based in EU
  - 1 based in US
- **vLEI Issuer Pipeline**
  - 17 organizations

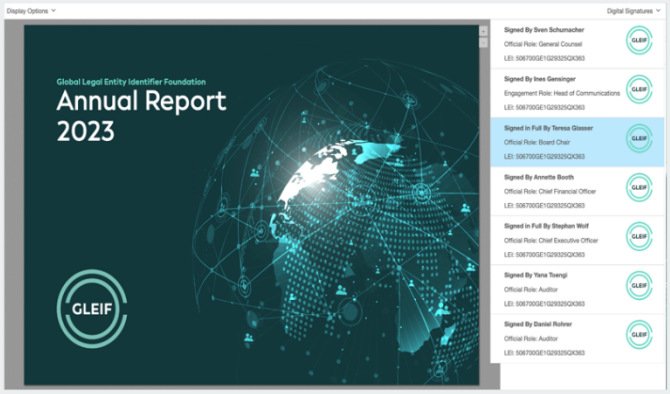
Enabling identification, permissioning, authentication, and digital signing - application examples

Using vLEIs: Private sector report submission to the public sector

Permissioning, authentication and signing with vLEIs

Demo of vLEIs signing Inline XBRL with vLEIs using draft standards developed by XBRL International D6 Working Group

- **vLEI credentials issued**
  - vLEI credentials are issued to certain officers and employees/managers of the organization.
- **Content 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.
- **Permissioned access and report submission**
  - Submitters present their vLEIs to access public sector portal
- **vLEI access and signing credentials presented and verified**
  - Status of the vLEI credentials (key state not revoked) and the cryptographic signatures are verified.



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

Why the LEI and vLEI in trade?

Secure and reliable legal entity identification helps:

	Cross-border payment	Fraud and risk mitigation	Financial inclusion	Supply chain Efficiency	ESG stewardship
Challenge	▪ AML Screening ▪ Realtime due diligence ▪ Cost	▪ Sanctions ▪ Information in silos ▪ Name matching ambiguity	▪ Access to trade and supply chain financing	▪ Lack of interoperability ▪ Fragmentation ▪ Manual work prone to error	▪ Regulation compliance ▪ Cost
How can the (v)LEI help?	▪ Minimize false positives	▪ **Cross-border Identification** of parties across the suply chain directly (e.g. buyer and seller) and indirectly (e.g. customs, insurance)	▪ Validated again local public registers	▪ Unambiguous identification ▪ Transparency and security ▪ Minimize fraud	▪ Machine readable, open data, and easily integrated ▪ API to LEI Repository
LEI	Unique, accurate (high data quality), scalable, consistent (parent relationship data), **users can challenge it.**				
vLEI	Digital and cryptographic advancement of the traditional Legal Entity Identifier (LEI). vLEI enables **decentralized and automated verification** of an organization's identity.				

LEI in Supply Chains

LEI in Trade and Trade Digitalization

Application of vLEIs - Digital Trade Documents Exchange Platforms

Problem:

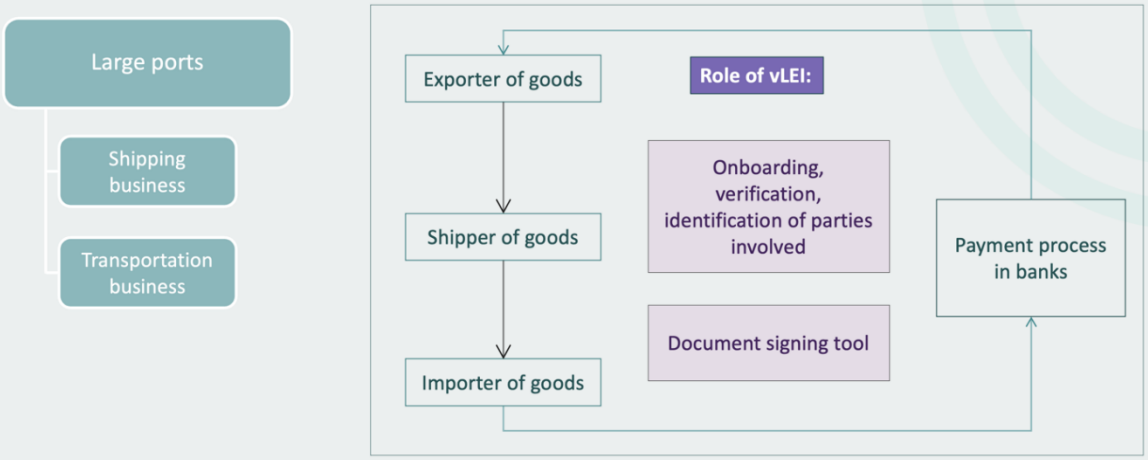
- Ensuring the authenticity and integrity of trade documents like e-bill of lading (eBL) and e-bunker delivery note (eBDN).
- Proprietary certificates are employed for user authentication, which may limit flexibility and interoperability.

Role of vLEI:

- vLEI verifies the identity of entities involved, ensuring trust in the accuracy and legitimacy of document exchanges.
- Supports secure document signing using standardized methods, improving reliability over proprietary certificates.
- vLEI offers flexible signing methods (PDF embedded and segregated hash signing), making document exchanges more secure and efficient.

Application of vLEIs - e-bills of Lading

e-bills of lading has information about the entire transaction



e-bill of Lading: Utilizes vLEI to identify enterprises and their employees on a digital trade platform, serving as both a unique identification and an online authentication and document signing tool.

Application of vLEIs - Product Traceability

Platform Function: Centralizes and tracks full life-cycle product data for financing and history verification.

Platform gathers data about:

- Producer
- Material
- Packager
- Quality
- Country of origin
- Exporter
- Importer

Collected data available through barcodes and QR codes

Role of vLEI:

- **Identifies Legal Entities**: Confirms the identity of producers, shippers, and other entities involved in the product's journey.
- **Verifies Data Size**: Ensures that the data package is accurate and complete.
- **Signs Data Package**: Digitally signs the data to confirm its authenticity.
- **Validates Trustworthiness**: Verifies the reliability and trustworthiness of the data package.

Application of vLEIs – ESG

The platform gathers ESG data from various sources, including IoT and other digital inputs.

The platform analyzes the collected data to evaluate the SMEs' environmental, social, and governance (ESG) performance.

Based on the analysis, service partners produce comprehensive ESG reports for SMEs.

SMEs with strong ESG credentials can access green financing from banks, improving their financial opportunities.

SMEs may undergo an ESG audit conducted by a professional institution to validate their ESG performance.

The ESG reports are converted into verifiable credentials, backed by implementer's blockchain for authenticity and integrity.

How vLEI Will Help:

- Each SME is issued a vLEI, which they use as a secure login credential to access the ESG platform.
- The vLEI extracts the SME's Legal Entity Identifier (LEI), identifying the SME and linking it to supply chain and ESG information.
- All ESG data for the SME is tagged under their LEI, ensuring that the data is accurately linked to the specific SME.
- The platform successfully verifies and tags the ESG data using vLEI, ensuring its authenticity and traceability throughout the process.

Application of vLEIs - Pharma Industry

Problem:	Role of vLEI:
Uncertainty over the authenticity of prescriptions, hospitals, doctors, and patients involved.	vLEI identifies hospitals, doctors, and patients to ensure authenticity.
Varying costs of medical procedures and consultations make it hard to verify which prescriptions are genuine.	vLEI digitally signs and verifies prescriptions, ensuring they are genuine and trustworthy.
Difficulty in securely sharing prescriptions across borders.	Encapsulates medical information in verifiable credentials, making cross-border exchanges secure and reliable.

LEI and vLEI in KYC: Simplifying Onboarding

KYC process	
Customer provides LEI	Bank uses LEI to identify the organization with certainty and with access to validated reference data about the organization.
Customer obtains vLEI	The customer can use the vLEI to sign and submit documentation required by the bank during the initial KYC process.
Subsequent business and onboarding	The customer can reuse the vLEI to apply for additional bank services.
Permissioning	The vLEI can be used to permission access by the customer to banking services replacing traditional username and password and other forms of multifactor authentication.

The vLEI also will:

- Speed up transaction processes by eliminating the need to repeat KYC verification, allowing faster access to financial services.
- Reduce information asymmetry, providing consistent and verified information across all transactions, which builds trust and accountability.
- Lower operational costs by reducing the need for manual verification, saving on human resources and minimizing administrative work.

Using vLEIs: Trust in voice calls and texts

Verification of corporate voice calls with vLEIs by the first QVI - Provenant

Companies and telco operators engaged in corporate voice calls will leverage the vLEI to instantly verify the authenticity of the caller

- Helping companies reach their customers
  - Customer service, Tech support
- Enables a call center to prove the right to use a local phone number although the origin of the call is international

GSMA Foundry launches Open Verifiable Calling project, building on proven live deployments to restore trust in Global Voice Communications

Richard Cockle, Head of the GSMA Foundry, said:

"Everyday consumers are increasingly confronted with the decision of whether to trust the calls or messages they receive. At the GSMA, we are dedicated to exploring and advocating for innovative solutions that empower mobile consumers to maintain trust in their communications."

- https://www.gsma.com/get-involved/gsma-foundry/content-type/news/gsma-foundry-launches-open-verifiable-calling-project-building-on-proven-live-deployments-to-restore-trust-in-global-voice-communications/

Music Industry Use Case: Songwriting, Publishing, Recording Agreements

Problem:	Solution:	Role of the LEI & vLEI:
Creators do not have an easy way to document information needed by publishers and labels, or a way to delegate this work to authorized representatives.	Verified writer identities – cryptographically secure publisher connections and identity verification.	The combination of identity verification and legal authority verification, encapsulated in a cryptographic credential that detects tampering, leads to verification across databases.
Music companies receive data about new music via texts and emails.	Verifiable compositions – machine readable writer and publisher data secured with digital signatures.	
Legal contracts are entered into catalog management systems manually.	Secure workspaces – collaborative deal rooms for writers and their teams.	
Fraud and poor data security run rampant throughout the music industry.		

vLEI Interoperability and Portability Engagement

Veridian
by Cardano Foundation

Chainlink
Cross-Chain Identity (CCID) and
Automated Compliance Engine (ACE)

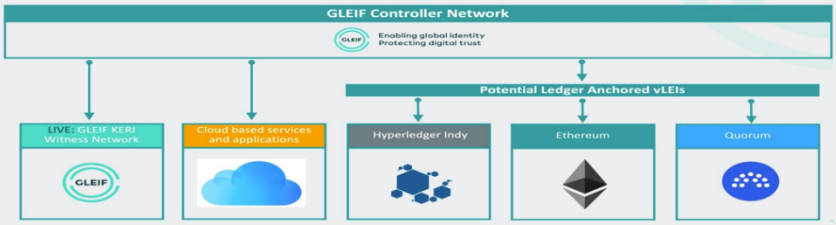
vLEI
Hackathon

IOTA Foundation
Trade Worldwide
Information Network
(TWIN)

Finternet Lab
open-source tools, including UNITS, DeDi
frameworks, and transaction protocols

GLEIF Partners
Program

esatus
SOWL vLEI Module



GLEIF

GLEIF Enabling global identity Protecting digital trust

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.

DIDComm 101

Session Convener: Sam Curren
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:

Went through the current state of DIDComm standard.

Played with demo.didcomm.org to show how DIDs work.

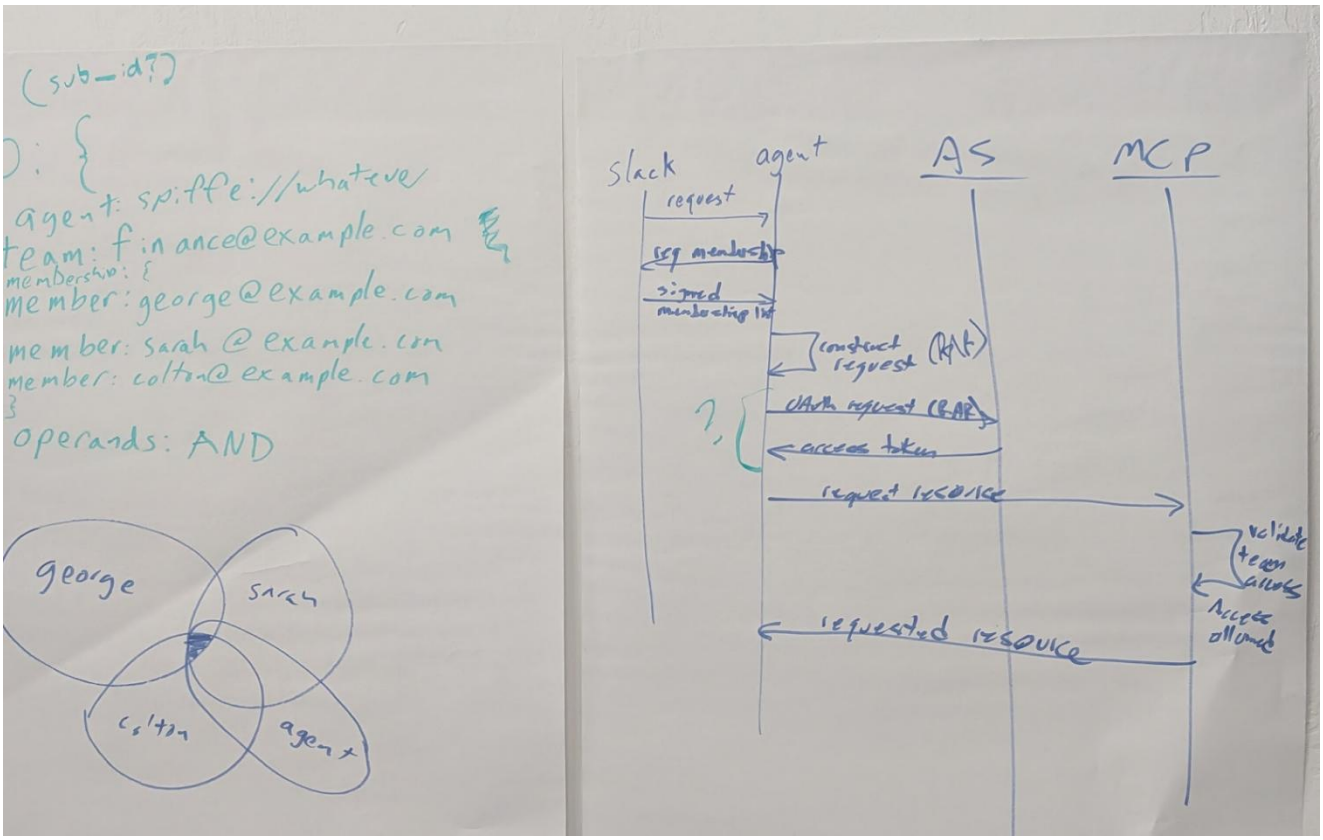
Slides Here: DIDComm v2 101 - October 2025 Update

Multi-Subject Access Tokens

Session Convener: Sarah Ciccetti
Session Notes Taker(s): Michael Krotscheck

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

https://openid.bitbucket.io/ekyc/openid-authority.html



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

Multi subject identity

Use case: An agent that is acting on behalf of a group.

An agent should have access to an intersection of permissions.

- Why does the group matter? Because access is transitive, and we want to see the intersection of what all of them can see.
- The issue is that if an agent is in a shared workspace, and can see more than the individuals in that workspace, they cannot expose that information to the rest of the users
- Assumption is that all users in the room have consented to the agent acting on their behalf.

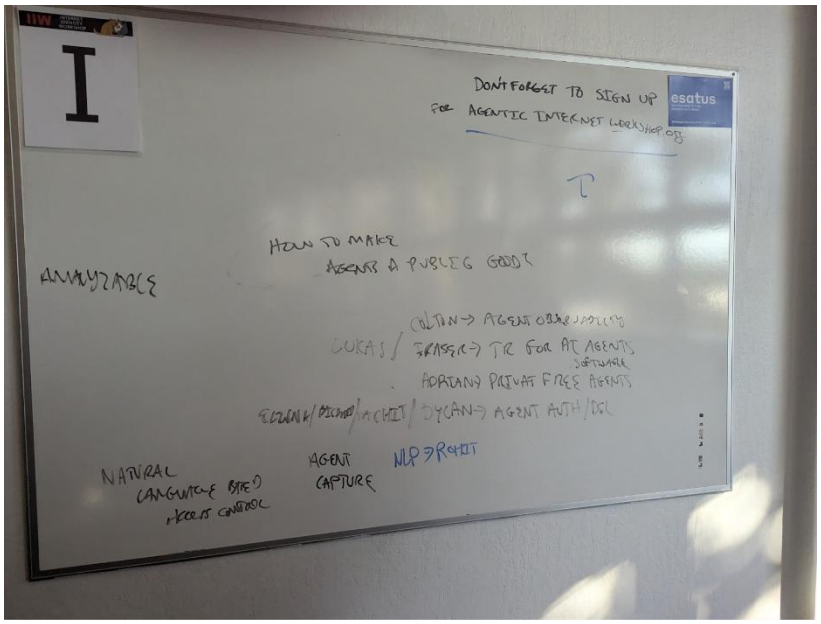
- If you have a collaboration style, either you give everyone everything, vs I am only sharing things with a consultant that has limited access.
- Maybe the agent has a special way to consume the collaborative material.
- You can give the agent access directly. That's easy. The question is: How do you derive that this entity can only act in ways that make sense.
- How do you construct an access token to access these resources, where does the membership live?
- You can make the subject the ID of the agent
- You can add some kind of scheme.
- You can say that the subject is the membership
- The more real time you want this use case to be, the more you want to move to a real-time architecture like AuthZen.
- This seems like an authorization thing, if the group expands or contracts the token will be stale
- The decision on whether you're granted access is not encoded in the token.
- There's a very early draft called OpenID for Authority.
- The weird set of access rights use case is handled well by RAR. And then you have the option of returning with the RAR blob in the token or not.
- security event tokens subject identifiers allows sub_id's, maybe as a list?
- Actor for the token is the agent, ergo the subject should be the agent. And it's acting with authorization against the team.
- RAR may permit logical operands: AND / OR
- Does the protected resource understand and/or know about the agent? That implies that the entity in the slack channel that is trying to access the documents is known to google. Does the agent have the rights to authorize as the user? i.e. does google know about the agent?
- How does the agent inspect whether the users have access to any given document?
- How do we limit what the agent can do above and beyond what is limited by the users.
- If everyone has delete capability, you need an additional constriction on the agent permissions to deny this.
- This doesn't have to be an agent. It could be a deterministic workload.
- Now we're talking about managing consent for new information to be pulled into the agent. And all members of the workspace must consent before they can access a new set of resources.
- So if a new person comes in, and hasn't gotten consent to access a resource type yet, then the agent suddenly becomes useless. That's going to add a whole new angle to peer pressure: Consent to the bot, dave!
- The agents are going to have to manage delegated identities for all users in the channel, for every channel in the slack server.
- Does the agent automatically get user access/context, or is it specifically assigned it and cannot modify it itself.

If the AS has some notion of what's in the channel it can make decisions on what the agent can do. But if it doesn't have access to the channel, then it needs to be told, and it shouldn't be told by the agent.

Scaling the Agentic Web

Session Convener: Andor Kesselman
Session Notes Taker(s): Eric Scouten

Tags / links to resources / technology discussed, related to this session:
SLIDES BELOW :
—--------
Scaling the Agentic Web: New Challenges and Areas of Innovation -- IIW Edition



Colton -> Working on Agent Observability
Lukas / Fraser -> TR For AI Agents
Adrian → Private Free Software Agents
Elina / Richard /Sachit/Dylan -> Agent Auth / Delegation

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

Started with a history of AI evolution.

Andor expects that thinking of agents as singular agents isn't likely to remain common. Pressures are likely to lead to orchestration of agents working with each other, but that comes with increased risk of attack surface and error propagation.

Identity for AI agents is far more complex than human identity. For example: Where is the agent running? What version? What host OS? What compute center? What context did it have? What goals was it given?

Some people are now working on Know Your Agent (KYA).

Interesting question: Does DNS scale up sufficiently for agents, especially given their potentially short lifetimes?

As of yet, MCP servers aren't really talking to each other. That will likely change soon and may substantially increase the attack surface vector.

Localhost client trust

Session Convener: Paul C
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:

- [:18] Mobile apps can say "I can be invoked using this URL"
- The OS checks with the website of the app to verify that the app has the appropriate URL
-

"Who's Responsible?" Authorization and Liability in AI Agents

Session Convener: Emu Iizuka
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

Beyond the Blue Check - from Social Verification to Verifiable Relationships

Session Convener: Brendan Miller and Alberto Leon, Applied Social Media Lab, Harvard University
Session Notes Taker(s): Brendan

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

Presentation: IIW - ASML Session 1 - Beyond the Blue Check

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

Summary:

The discussion focused on transitioning from social verification to verifiable relationships in social media, using the ASML wallet and open social media platforms like Blue Sky. Demonstrations included linking social media profiles and age verification using zero-knowledge proofs. Alberto Leon showed how to notarize transactions with X.com and generate credentials for Blue Sky profiles. The team also discussed the potential for using cloud agents to refresh credentials and the importance of privacy and safety. Future plans include person-to-person relationship credentials, content provenance, and single-use identity proofs. The session emphasized user control over digital identity and content, aiming to enhance trust and privacy in social media.

Proximity Presentation for SD-JWT using 18013-5

Session Convener: Lee, Kristina, and more
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 #5

How to use Keri/ACDC for SEDI Infrastructure Distributed Decentralized Signing Infrastructure

Session Convener: Sam Smith
Session Notes Taker(s): Kent Bull

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:

Design strategy: security first, always, no half measures.
Then use minimally sufficient means.

Recovery from Compromised Signing Infrastructure

- Recovery time depends on Architecture
- Rotate tokens/permissions/keys frequently
- Detect, revoke, and reissue entitlements as needed when fraud is discovered

Closed loop (not privacy preserving):

- Forced phone home to verify (this is not bearer tokens) - this is the centralized approach
- Persistent entitlements problematic with frequent rotation

Open Loop:

- no forced phone home to verify
- bare signatures on entitlements are unverifiable after rotation
- Unbounded fraud over time potential on persistent entitlements unless all entitlements are revoked with each rotation
- undetectable fraud potential on unlikable signatures (ZKPs)

How many of you rock climb?
Free climbing, without rocks and anchors, is only possible for people who are really, really good. Doing PKI only works for people who are really, really good at PKI, yet when you fall it still hurts very badly.

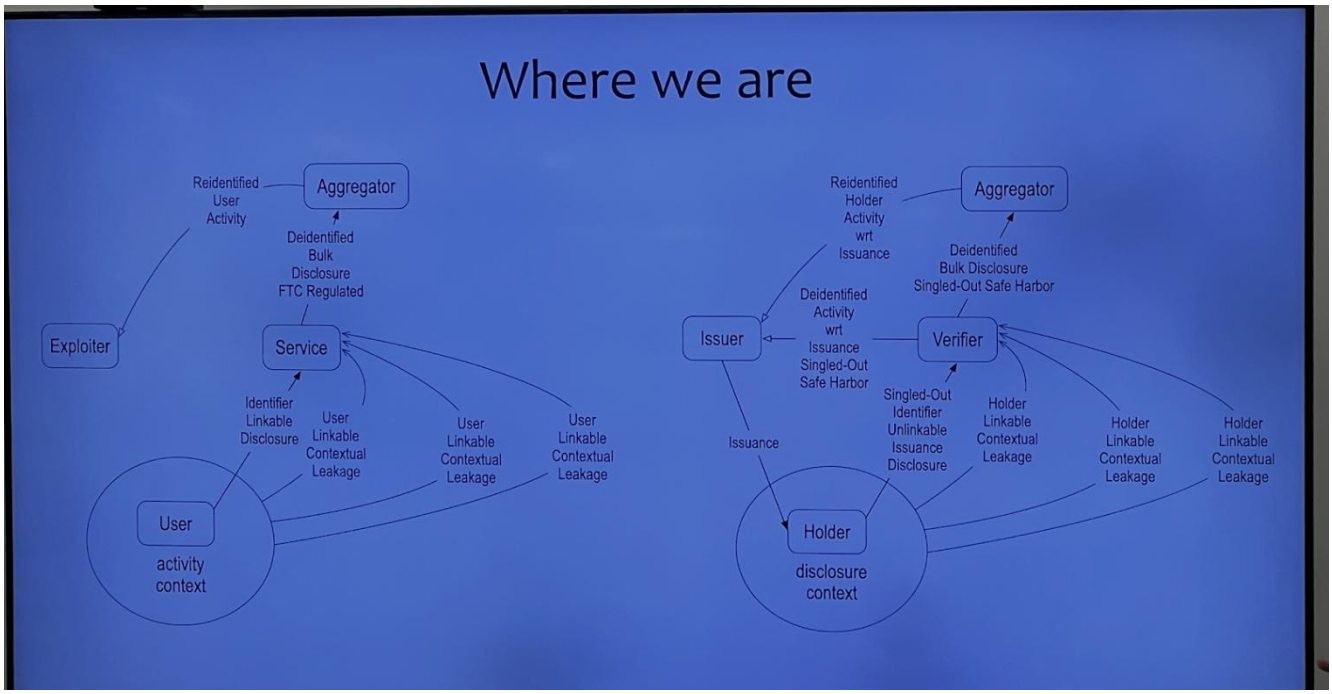
Climbers using anchors and ropes can recover from a fall. A fall doesn't hurt that much because the climber uses a close anchor.
No timely recoverability is the IT equivalent of free climbing.

You need recoverability. You need to build systems that are recoverable. When I built KERI I knew I had to build recoverability in as a first principle.

We cannot assume that key compromise is not going to happen.

Where we are from a privacy context globally

- Data aggregators re-identify people regularly, trivially. ZKPs do not stop data aggregators from performing re-identification.



Timothy Ruff: What do we say to those who feel ZKPs are an essential improvement?
Sam: We tell them that a ZKP based system is so much harder to detect fraudulent behavior on that the security tradeoff is not worth it. You have to go through the argument point by point by point.

ZKPs are a simplistic approach. Simplistic approaches are easy to sell and easy to believe in.

Comment from the audience: ZKP reduces disclosure at the expense of recoverability. ZKP key compromises cannot be detected. We are referring specifically to issuer key compromise, not holder key compromise.
The issuer is blind to the presentation. If a key has been compromised you can't tell.

NSA funded interaction graph technology after 9/11/2001. Every LLM has comparable interaction graph technology.

How to prevent subornment

- horizontally scalable distributed signing infra
- nonrepudiable accountability of each and every employee (actions bound to actors)
- detectability of all forged issuances without reliance on cooperation/collusion with verifiers via anchored issuances tied to each employee
- maker-checker-supervisor key management

All of security is in key management.

Question from the audience: you've given increased security. Can you get us back to as much privacy as possible?

Answer: ACDC State Registry using Transaction Event Log (TEL)
Start with a DAG of logs, KEL -> TEL

Certificate Transparency is a verifiable log backed map (using a sparse merkle tree). You can audit all the entries yet you have herd privacy for any change in state. KERI with ACDC State Registries is like this. A bulk update is what prevents a change in state from being correlatable to a given requestor.

This allows you to have a secure system, vendor to vendor. This means that no verifier vendor can link a given usage of a credential

No forced linkage from the observer (verifier infrastructure) back to the issuer. So you are preventing the issuer from being able to correlate usages of the credential since the issuer cannot know, due to bulk issuance, when a verifier is checking a specific credential because of herd privacy due to bulk issuance.

Decentralized Identity 101

Session Convener: Steve McCown
Session Notes Taker(s): Steve McCown

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

Here are the presentation slides we covered in this 101 session:

Decentralized Identity 101

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

See above…

Anastasia: Cinderella's Stepsister Turning Shabby X.509 Certificates into Elegant Anonymous Key Attestation

Session Convener: Dan Yamamoto
Session Notes Taker(s): Haruki Oyama, Ken Watanabe

Tags / links to resources / technology discussed, related to this session:
https://speakerdeck.com/yamdan/anastasia-cinderellas-stepsister-turning-shabby-x-dot-509-certificates-into-elegant-anonymous-key-attestations

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

Starts by talking about the basic workings of digital identity wallets
    VCs, selective disclosure
There is a requirement called non-transferability
    issuers do not want credentials to be cloned to other wallets
    they want the credentials to be bound to devices (device binding)
        the wallet has a secure storage and dsk and dpk are stored in these device wallets
        credential consists dpk as an attribute
        wallet provides PoP to verifier
? is the dpk available in non-apple phones too?
    Yes, you can generate using apple or android apis
    at this moment, however, verifiers cannot be convinced that the dpk actually comes from that device
        we need to verify that the dpk is actually from that said device
        -> we can use key attestation mechanisms
X.509 certificates enable this (used by apple and google)
    google in android acts as an attestation authority
    proceeds to show real example
        the chain of one Root Cert, 3 CA, 1 EA cert
        each cert has different sign algorithms.
        each cert has correlating factor.
Challenge of research project: creating an unlinkable key attestation with X.509
    traditional X.509 certs do not support selective disclosure etc..
Prior work
    Cinderella by MS Research
        Using zk-Snarks (Pinocchio) to anonymize RSA-based X.509 certificates
    Problem: proof generation takes minutes, huge parameters & non-universal trusted setup
        not suitable for practical mobile use
In recent ETSI report: Cinderella takes up to 9 minutes
    but zk-snark improvements can make this idea more practical
→ Proposal: Anastasia
    Psuedonymous Key Attestation
    Decrease computational cost of this attestation using latest ZKP techniques

UltraHonk (a PLONKish Schema)
Prevents overflow by concatenating per-certificate proofs
Uses Noir and Mopro
Performance: Generates two-level chain proof in about 20 seconds on an Android device
Proceeds to talk about example using anastasia
This zkp enables to hide CA subject
Limitation: prototype only supports ES256 anonymization
not compatible with root cert and CA1
DEMO
flow from issuance to verification
took 17 seconds to obtain a proof of about 24kb
cannot be encoded as a qr code or barcode but can still transmit this proof
On the verifier page, verifiers can verify this proof.
It took 21 sec
Proceeds to summary and future works
summarises the presentation
future works
to support ES384, RSA4096, Key Binding
Support privacy preserving revocation
use of google specific X.509 for finer-grained attestation
iOS support
provide formal security audit to assure actual security of proposal

https://github.com/yamdan/anastasia

? Does RSA produce acceptable performance for this
Yes (pretty subjective) and with future work it can improve even more
? Why do you name it anastasia
because there is a redemption arc for her in cinderella p2 and 3

Gen AI Phishing! Using AI for Bad Things!

Session Convener: Yuriy A
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

Passkeys PQC and Beyond

Session Convener: John Bradley
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

Gordian Autonomy Stack

Session Convener: Christopher Allen Blockchain Commons
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

Use cases in North American Real Estate

Session Convener: Michael Krotscheck
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

Identity 4 Groups

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

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

Slide Deck shared during the presentation
Sideways Verifiable Community .pdf

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

We are looking to build verifiable credential tooling and technology centered on groups and communities and their needs.

We invite folks who want to engage with us to find us at Sideways.earth

We have done extensive research on needs of groups and networks.
https://sideways.earth/neworkresearch/

You can also check out our github
https://github.com/SidewaysEarth/

Natural vs. Verified Person?

Session Convener: Luke Nispel
Session Notes Taker(s):

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

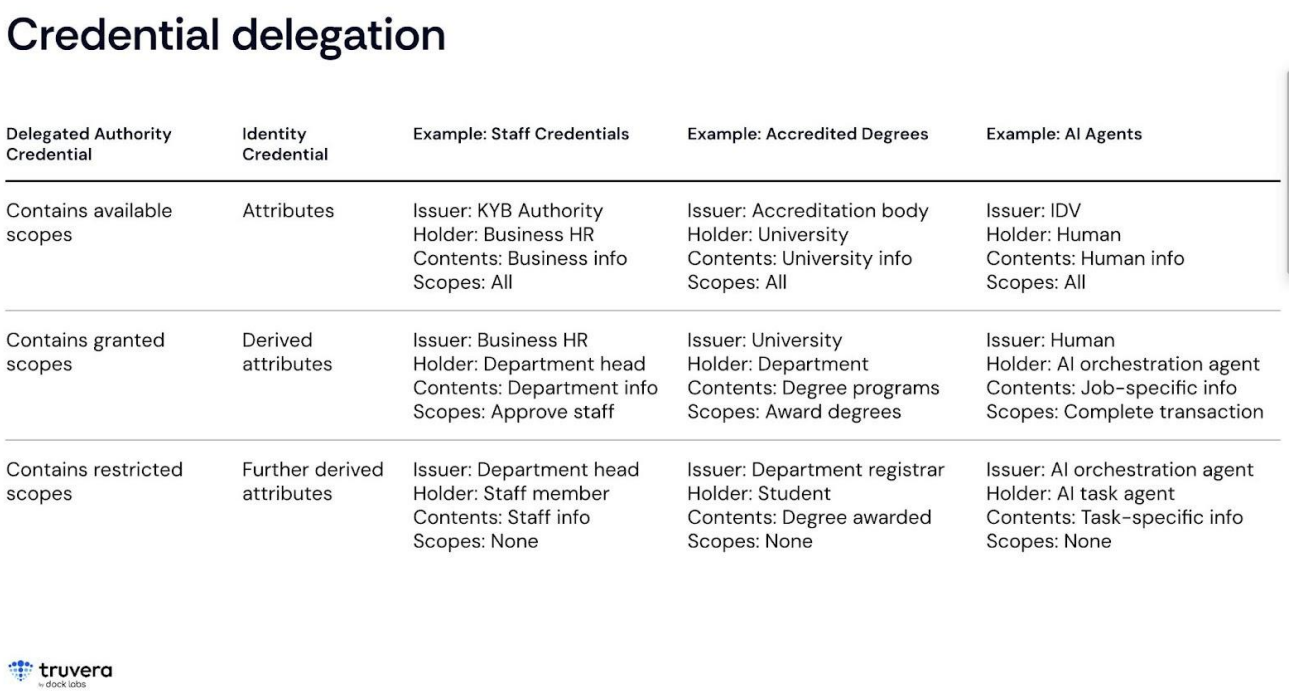
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

NO NOTES SUBMITTED

Technical: Delegation & Guardianship

Session Convener: Richard Esplin (Dock Labs)
Session Notes Taker(s): Elina Cadouri

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



Credential delegation

Delegated Authority Credential	Identity Credential	Example: Staff Credentials	Example: Accredited Degrees	Example: AI Agents
Contains available scopes	Attributes	Issuer: KYB Authority Holder: Business HR Contents: Business info Scopes: All	Issuer: Accreditation body Holder: University Contents: University info Scopes: All	Issuer: IDV Holder: Human Contents: Human info Scopes: All
Contains granted scopes	Derived attributes	Issuer: Business HR Holder: Department head Contents: Department info Scopes: Approve staff	Issuer: University Holder: Department Contents: Degree programs Scopes: Award degrees	Issuer: Human Holder: AI orchestration agent Contents: Job-specific info Scopes: Complete transaction
Contains restricted scopes	Further derived attributes	Issuer: Department head Holder: Staff member Contents: Staff info Scopes: None	Issuer: Department registrar Holder: Student Contents: Degree awarded Scopes: None	Issuer: AI orchestration agent Holder: AI task agent Contents: Task-specific info Scopes: None

truvera
by dock labs

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

Guardianship - legal authority
Delegation - technical authority

3 use cases we see regularly:

1. Healthcare - e.g. allow someone to pick up medication on my behalf, restrain scope
2. Enterprise - e.g delegating authority to employee to represent the company, exec can sign
3. AI agent delegation - e.g. agent can execute on behalf of an individual or company

Entity acting with authority needs to be auditable

Dock Labs approach:

- use two credentials: proof of delegated authority and delegated identity
- the verifier looks at both credentials and chain of credentials to the root of trust which can be a KYB credential

Digital bazaar approach (lower level, specific to certain use cases):

- focuses on cryptographic delegation - authorization capability using zcap that includes:
    - Agent (DID)
    - Target (resource)
    - Action (scope, GET/P)
    - Caveat (optional, given restrictions)

Cross-organization can require long dependency chains

UCAN spec on github
ZCAP: github.com/interop-alliance/zcap-developer-guide (in progress)

Benefit of credentials chain is you're only aware of the party providing the delegation

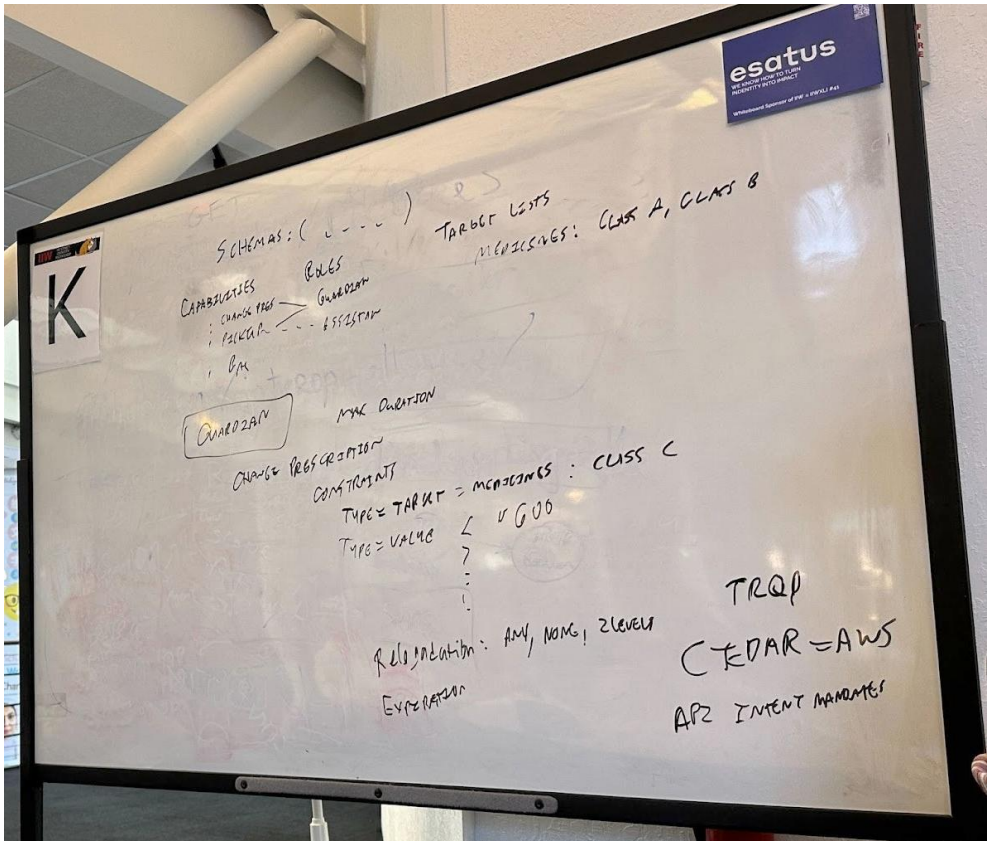
- Consider differentiating claims and permissions

How to make this easy to use?

3 key points for UX:

- solution designer
- wallet holder delegating
- verifier seeing the delegation chain

How to explain the rule set?



"Making User Policy Decisions Disappear " - paper by HP, Alan Karp

If Bitcoin had Identity Layer - first person network for retroactive UBI & solving $338T Global Debt Crisis

Session Convener: Nivas Sivaprakasam
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

Notes Day 2 / Wednesday October 22 / Sessions 6 - 10

SESSION #6

Is Compromising a SEDI Treasonous?

Session Convener: Rep. Chevrier
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

MyTerms for Dummies

Session Convener: Doc Searls, Joyce Searls, Nitin Badjatia, Kari McMullen
Session Notes Taker(s): Drummond Reed

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

https://customercommons.org/

The slide deck that Nitin presented is here:
https://docs.google.com/document/d/1TfrkpFFcmv8wElqYIffYqFO_jZG3GmXON_kzzM4SIb0/edit?tab=t.5flmnduk3wew

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

Nitin introduced the MyTerms project which has been a 8 year journey to create a standard for personal privacy terms that are based on the individual as the first party.

It was officially approved as an IEEE standard this morning.

Nitin walked us through the slide deck that explained the problems with the current state of cookies and unconsented data sharing and brokering today.

The Ideal state with MyTerms would be:

- No more privacy policies.
- Consent is eliminated! It is outdated. The new basis is contract.
- Cookies are restored with purpose. No more cookie banners.
- Rapid service delivery with 1, 2, 3rd level contracts are understandable.
- Frictionless. Grampa gets agency and can make proper choices.
- Safe data sharing. Donate to medical research, AI. World would be a better place.
- Intention Economy Alive. Rebalancing for the consumer, better safer info. Clear Safe Signaling.

Doc Searls explained the three basic elements of the new IEEE 7012 standard:

1. It is a contract.
2. The individual is the first party to the contract.
3. The contract uses a standard set of terms, maintained by a neutral nonprofit, from which the individual as the first party chooses.

Nitin explained that his goal is for the CRM company he works for to implement an API for companies to accept MyTerms ingestion.

Joyce explained MyTerms this way: “MyTerms is a way for ‘me to put my hand out first’, vs. our current situation of consumers being totally subject to the terms of the businesses they are dealing with on the Internet.” So the individual is part of the transaction rather than just the result of the transaction.

There was a long discussion about the fact that the standard does not specify the technical means by which MyTerms can be implemented. That’s a major task ahead.

There was discussion about adoption angles. One is to pursue an enhanced cookie banner that offers MyTerms as an option. That could be a streamlined route to installing a browser extension.

We discussed that there are two major steps ahead:

1. The development of a single agent-to-agent protocol to establish a MyTerms contract. Iain said that work will start here at IIW and the Agentic Internet Workshop.
2. The establishment of a MyTerms Alliance similar to what happened for Wifi (which was a separate alliance from the 802.11 standard).

The hosts shared a QR code for a Signal channel for discussing the go-to-market strategy and a place where you can see what is needed and help as you are able.

When Patients and Doctors write their own Software…

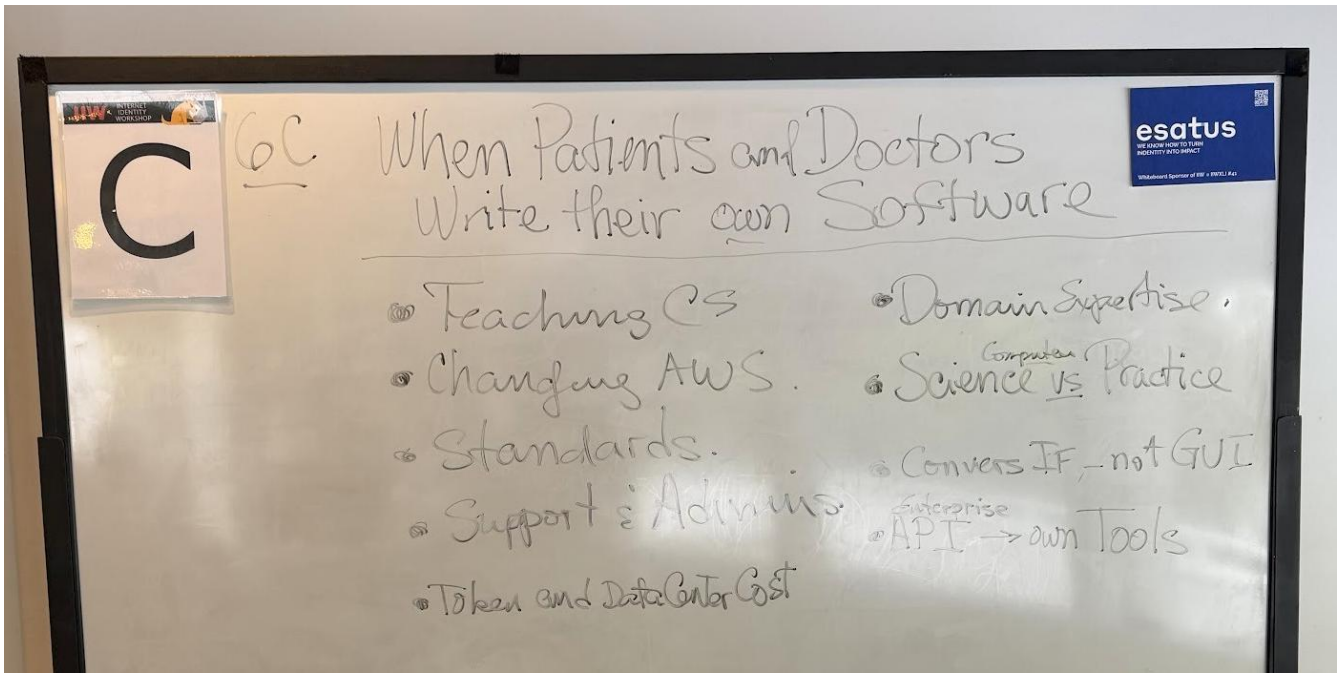
Session Convener: Adrian Gropper
Session Notes Taker(s): Adrian Gropper

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

IIW41_S2C_My Private AI Agent as an Authorisation Server

Demo Hour Table #13
https://www.google.com/url?q=https://docs.google.com/document/d/1PVS-VTpJLwKIwmzj5DxQZnyBPQ78pPXW4d5dhRxDSTM/edit?usp%3Dsharing&sa=D&source=editors&ust=1761180858559909&usg=AOvVaw0g8Ku035rkxUNqWWwYDhnT

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



Data Unions and Labor Law

Session Convener: Kaliya & James Felton Keith
Session Notes Taker(s): Margeigh took some notes

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

VoteJfk.org
JamesfeltonKeith.com

Here are some old articles on the topic.
A New Class of Stakeholdership
https://www.benzinga.com/fintech/19/10/14658429/a-new-class-of-stakeholdership-james-felton-keith-on-addressing-inequality-with-a-data-dividend

A bunch of articles on Data As Labor for Businesses Consideration
https://www.forbes.com/councils/forbesbusinesscouncil/people/jamesfeltonkeith/

DataIsLabor dot Com
dataislabor.com

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

You can hear the talk that James gave us here.
https://www.youtube.com/watch?v=fuCOoiV1l2I

Presenting VCs based on natural language instructions – Offline LLM for DCQL on Mobile–

Session Convener: Ken Watanabe
Session Notes Taker(s): Haruki Oyama

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

https://github.com/dorakemon

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

Speaker introduces himself and the outline of the presentation

Speaker starts with the background of presentation (basics of VC)
Explanation that everyone knows regarding the three party relationship of issuer, holder, and verifier
    selective disclosure
Nowadays holders have multiple VCs
Verifier can request VCs via DCQL query
    DCQL shows which VC and which attributes to request
Speaker explains a typical presentation scenario between holder and verifier
New scenario: as VC usage grows the holder may want to actively choose what to show because they will own much more VCs
Problem with new scenario: Troublesome to choose the right VCs from his wallet and right attributes to prove to the verifier
? Are you saying an LLM is going to be local and helping you put together VCs based on context? If so, how does it understand the context
    Will answer after demo

speaker starts his demo
    demonstrates the process of generating dcql from natural language (with selective disclosure) and then presenting the vc

? Can you create a new VC every time?
    yes
? Is this all running on a local llm?
    yes, no connection to openai and other servers, privacy enhancing
? does this llm also ensure it can deal with dictated wallets?
    yes
? is the llm integrated into the wallet or separated app
    integrated

speaker explains his system requirements

speaker dives into system architecture

steps involve: filtering, dcql generation, vp generation with vc storage linked to filtering

1. natural language instruction narrows down list of VCs
2. from user's instruction and related VCs, generate dcql to llm
3. execute the dcql to generate VP

? Are you signing all the VCs with one wallet entry?

Yes, I am assuming this is in one wallet entry

? When you combine the aggregated VCs do you not need to sign with all the keys of each VC?

Speaker did not assume multiple wallet storage

Integrated the system in one wallet but needs work to improve to multiple wallets

Speaker explains filtering process

uses text embedding techniques

? What do you use to convert the vectors

Uses text embedding outside of local llm

Many llms do not know dcql because it is a recent standardization

Speaker explains how finetuning was done

created dataset of fine tuning data

explanation of input prompt and expected output

fine tuned open source local llms

Picked multiple popular llms

qwen3-4b and gemma-2-2b-it performed the best

according to apple models under 3b parameters can run locally on apple silicon

explanation of execution environment

concluded presentation with summary and future implementation

? Digital credentials api picks

digital credential api needs dcql from verifier, holder can also create dcql query, it can also come from holder itself

? Shouldn't the natural language prompt come from the verifier? normally verifier will send the request

that is a different use case

participant: user will go through their own presenters and natural language will create the top 5 to send it back

? What happens if a verifier wants a specific credential type?

verifier can generate their own dcql, the application can also help verifiers by applying the automated workflow to verifiers on top of presenters

this applies to any other scenario including vcs in the real world

participant: likes the use case, can expand to spoken language

saving time at airport, bar, hospital

? How often do you get gibberish back?

Goes back to error rates slide

if you add more datasets the accuracy may decrease
? Have you considered using an MCP instead of llm to create the json
Should make the llm just pick up the attributes
Algorithmically making json using for loops will be faster and more accurate
comment: simple code > llm
? How was the f1 score
not calculated
? How about your training data? is that synthetic? how was it made?
used llm to generate these datasets
manually checked that each vc is correct
even the smallest of noise can make the accuracy of the llm very low
comment: natural language can be the one being sent at the end instead ultimately
comment: nobody wants to read json this is useful
? Can you generate proofs even before someone requests it
yes you can
comment: much better way then searching through your wallet
comment: very nice, will steal
[clapping]

? can you do on android also
can run on android, gemma is a google model
? can you make more complex prompts, for instance by specifying the specific vc the llm should look at
yes, likely, can implement this by editing UI also
? battery consumption
reasonable
? what do you think about the new apple foundation models, they handle pulling all the models for you (swift wrapper)
can apply the swift wrapper to this app
comment: no doubt you could do it
? what the llm speeds up is the generation of the dcql, is there any way to make the total vp generation more efficient, it's the wallet's job to answer the dcql
yes, and wallets can answer the dcql efficiently
[end session, clapping]

OpenID4VC Conformance Testing Deep Dive

Session Convener: Joseph Heenan
Session Notes Taker(s): Joseph Heenan

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

URL: https://openid.net/how-to-certify-your-implementation/

OIDF has tests that wallets, verifiers & issuers correctly and securely implement OpenID for Verifiable Credential Issuance / Verifiable Presentations specifications, with ISO mdocs or SD-JWT VC - we demo them, explain their limitations & how you can run tests yourself.

Instructions are here:

1. How to run conformance tests for OpenID for Verifiable Presentations
2. How to run conformance tests for OpenID for Verifiable Credential Issuance

Source code for test suite:

https://gitlab.com/openid/conformance-suite/

Slides (including the demo videos) are here:

https://docs.google.com/presentation/d/1b4RlSiBKyZdW9h4V9vCdb8FWHHvnNduB/edit?usp=sharing&ouid=107381980093922120275&rtpof=true&sd=true

Slides & videos separately:

https://drive.google.com/drive/folders/125AdoKFQHFQYErN04px1iC6T1fROAX15?usp=sharing

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

Any questions/problems email certification@oidf.org

On Behalf of use Authorization for AI agents (draft spec)

Session Convener: Hasintha Indrajee & Sachin Mamoru from WS02
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

Driving vLEI and KERI Adoption

Session Convener: Esteban García and Kent Bull
Session Notes Taker(s): Eric Scouten

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:

GLEIF goal: Identity system for organizations at global scale.

To drive adoption, you need a "perfect storm" of things going right. GLEIF sees this as a flywheel building on the following components:

- **Policy:** Policy makers in each jurisdiction that registers legal entities need to be on board.
- **Technology:** vLEI ecosystem depends and adoption/viability of KERI protocol.
- **Market drivers:** ROI or policy requirements that drive adoption.

On technology specifically, GLEIF understands that developers need access to easily-onboarded technology. Focusing on developer-oriented training materials.

Hosting a global vLEI Hackathon. Intent is to promote awareness of the ecosystem and to encourage adoption/integration into existing commercial systems. Hackathon projects address these topics: finance, KYB, and supply chain. Over 100 submissions for initial round. Final presentations in next few weeks.

Be aware of vLEI training materials published by GLEIF.

KeriCON coming up: First KERI-only conference. April 2026 in Salt Lake City, just before IIW. Conference web site not yet available.

I asked a question about the ordering of the layer stack. When I reviewed KERI a couple years ago, I had trouble figuring this out. Kent provided the following sequence (top to bottom):

- TSP from ToIP
- ACDC
- KERI
- CESR (serialization format)
- verifiable data structure (key event log) verifiable key and signing history
- cryptographic primitives (seeds, keys, signatures) and data structure primitives (text, labels, field maps)
- libsodium, crypto key generation, signing, and verification (currently written primarily at C)

Karla extends an open invitation to attend the marketing and outreach sessions hosted by KERI Foundation.

See https://ericscouten.dev/2025/iiw41/#session-6k-driving-vlei-and-keri-adoption for photo from session.

KYAPAY - A protocol for Agent & Principal identity & Payments

Session Convener: Ankit Agarwal @ Skyfire (ankit@skyfire.xyz | ankit@tryskyfire.com)
Session Notes Taker(s): -

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

2.2 KYAPay - A Protocol for Agentic Commerce - IIW/AIW - Oct 2025

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

OPAQUE Passwords

Session Convener:
Session Notes Taker(s): Bryce Frey (brycefrey@google.com)

Tags / links to resources / technology discussed, related to this session:
https://datatracker.ietf.org/doc/rfc9807/

https://pqshield.github.io/nist-sigs-zoo/
https://blog.cloudflare.com/another-look-at-pq-signatures/#the-algorithms

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

SESSION #7

Attestation-based Client Auth & Native Client Attestation Grant Key Binding (merged sessions)

Session Convener: Christian Bormann & Frederik Krogsdal Jacobsen
Session Notes Taker(s): Frederik Krogsdal Jacobsen

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

OAuth 2.0 Attestation-Based Client Authentication draft:
https://datatracker.ietf.org/doc/draft-ietf-oauth-attestation-based-client-auth/

OpenID Connect Key Binding draft:
https://openid.github.io/connect-key-binding/main.html

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

This session merged two related session

Presented the client attestation spec and some use cases: wallets (Christian, Paul & Tobias), customer IAM in highly regulated environments (Frederik) , and enterprise IDP (Kosuke).

Good reception to the basic idea of the spec.

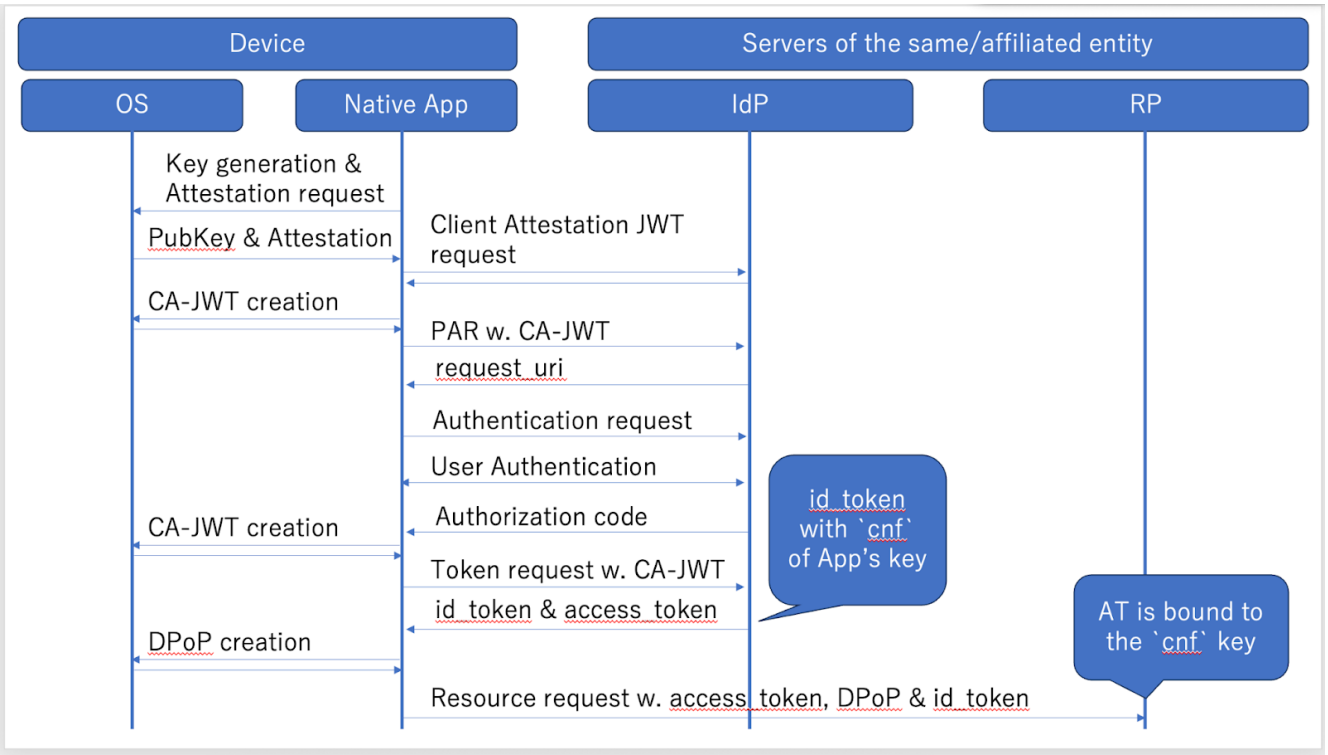
Feedback: This is not really necessarily a client authentication method. Since you are only allowed to use one auth method at a time, it should be optional for this to be an auth method so it can be combined with e.g. mTLS.

Kosuke's key binding enterprise use case was more controversial because of the use of OIDC key binding, which brings questions about how to interpret audiences in JWTs (aud claim).

Suggestions:
We should write up our use cases. People want guidance on how to use the spec in various use cases with different security and privacy assumptions.

The spec should maybe be renamed to indicate that it is not necessarily a client authentication method. It should also be optional in the spec whether you want to use it as client authentication.

Adding an optional optimization that makes it possible to reuse DPoP header for the key binding in this spec would be useful. It should be an explicit opt-in, e.g. by adding a "magic" keyword that means "look in the DPoP header instead".



Why

- It may be easily introduced to existing systems
  - No additional (huge number of) Client IDs
  - No extra implementation for RPs who doesn't need DPoP
  - access_token may be limited-length (can't contain cnf)
  - no need to create token introspection endpoint

Verifiable Relationship Credentials (VRCs) and R-Cards: A Design Session

Session Convener: Brendan Miller, Alberto Leon
Session Notes Taker(s): Rob Aaron+others

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

Session slide deck:
https://docs.google.com/presentation/d/1dfgZ4ZyI4zdolN2d0yVOGYqGzye5BjofZg5d5oDzXkg/edit?usp=sharing

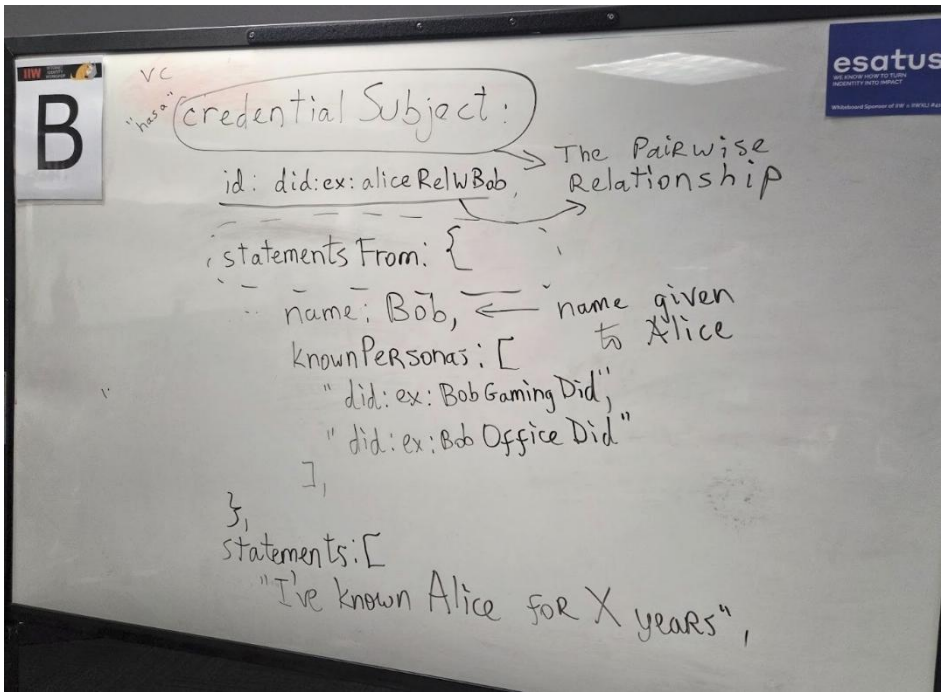
Decentralized Trust Graph Working Group (includes signup info): https://lf-toip.atlassian.net/wiki/spaces/HOME/pages/257785857/Decentralized+Trust+Graph+Working+Group

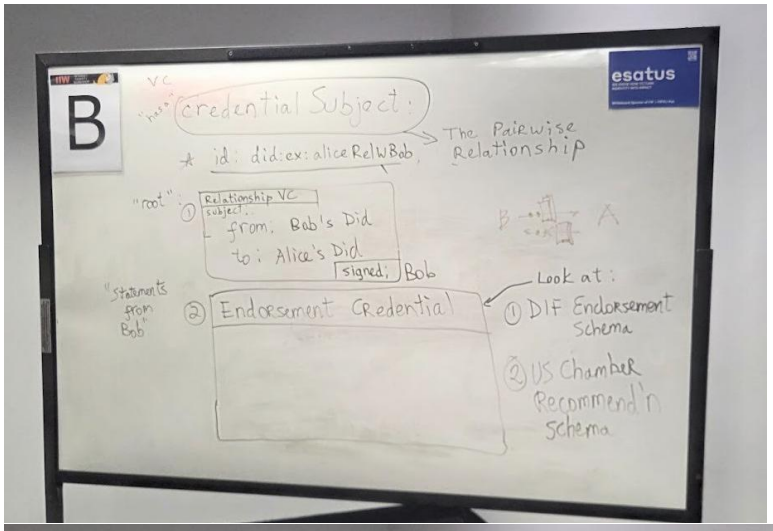
FPP White Paper: https://www.firstperson.network/white-paper

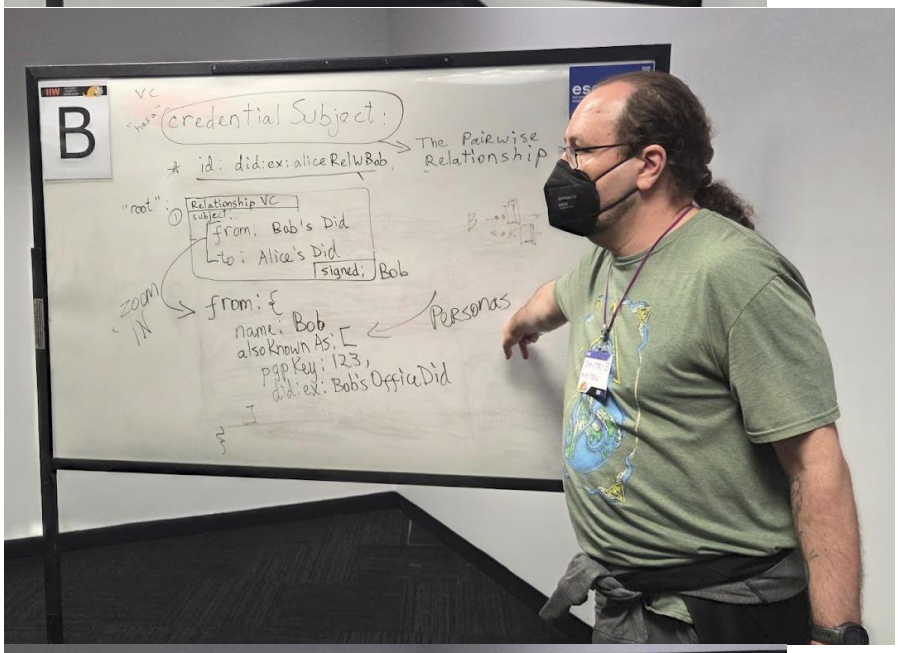
Draft specification produced based on this conversation can be found here:
https://github.com/trustoverip/dtgwg-cred-tf/commit/95ecb368a73ec8e466d46820e8d04690b6f61102

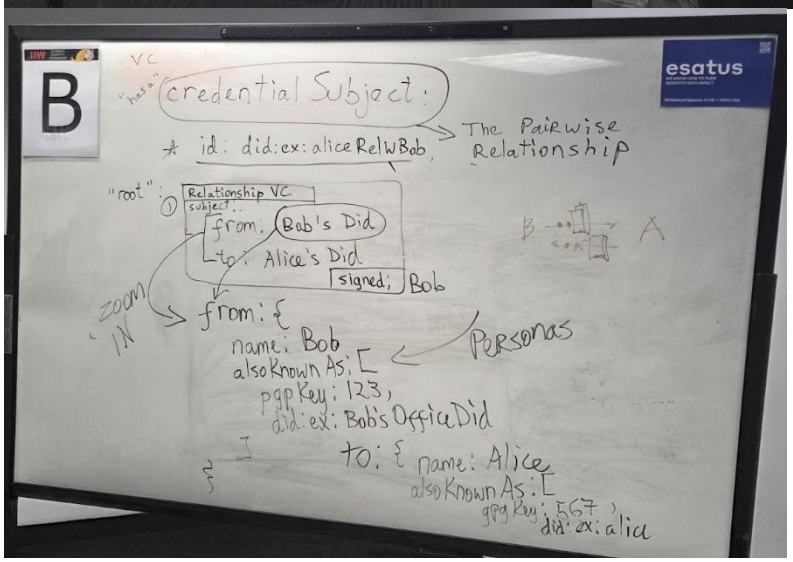
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

CURRENTLY IN DRAFT MODE!!




B
esatus
VC
"has"
credential Subject:
The Pairwise Relationship
id: did:ex:aliceRelWBob,
"root":
Relationship VC
subject:
from: Bob's Did
to: Alice's Did
signed; Bob
"statements from Bob"
Endorsement Credential
Look at:
① DIF Endorsement Schema
② US Chamber Recommend'n Schema


B
VC
"has"
credential Subject:
The Pairwise Relationship
id: did:ex:aliceRelWBob,
"root":
Relationship VC
subject:
from: Bob's Did
to: Alice's Did
signed; Bob
zoom IN
from: {
name: Bob
alsoKnownAs: [
pgpKey: 123,
did:ex: BobsOfficialDid
Personas


B
esatus
VC
"has"
credential Subject:
The Pairwise Relationship
id: did:ex:aliceRelWBob,
"root":
Relationship VC
subject:
from: Bob's Did
to: Alice's Did
signed; Bob
zoom IN
from: {
name: Bob
alsoKnownAs: [
pgpKey: 123,
did:ex: BobsOfficialDid
Personas
to: { name: Alice
alsoKnownAs: [
pgpKey: 567,
did:ex: alic

TASK: To be finished by Brendan

Session2 - IIW

The discussion focused on the concept of verifiable relationship credentials (VRCs), which allow individuals to share specific aspects of their identity with others. Key points included the importance of personas, the need for machine-readable terms, and the potential for multiple relationships. The W3C specification for verifiable credentials was referenced, highlighting standard elements like ID, type, issuer, and proof. The conversation also explored the idea of pairwise relationships, where both parties share a unique identifier, and the potential for separating vouching statements from relationship statements. The goal is to create a standardized model for VRCs that balances privacy, verifiability, and usability.

Work in conjunction with the First Person Project, by Applied Social Media Lab at Harvard University's Berkman Klein Center for Internet and Society

VRCs form connections between two people

Major use case: Linux Foundation using for Kernel management

Clarifying question asked: one VRC, how many R-cards? A: dozens

Personas - unlinkable to other personas/identity.

VRCs relevant in contexts: one for work, one for school, one for sports

PHC is different. Proof of person in each eco system / trust network (not the focus of this session)

Should purpose be required for machine readability?

- How will the vocabulary be developed?

Other top-level properties? Required or optional?

- termsOfUse
- refreshService
- status

Other nested properties?

- credentialSubject.nonces (to validate live exchange/session?)
- proof.attestationObject (hardware attestation linked to biometric key?)

Additional: validFrom would be an interesting addition

Q: Machine-readable, yes but also human and "vibe"

Q: pubic or private?

Darrell - if VRC for connection of someone you play volleyball with, private; if to a business, public

TASK: Add Dmitri comments/screenshot here

Comment: Personas are going to be extremely important! -Drummond

Per Drummond: Bob is staying statements about himself (not the other way around)

Doc brings up CustomerCommons and MyTerms ceremony as being a

Q: Do we want to separate out vouches?
vLEI model: One company VRC, multiple statements follows

Paul: persona name should be optional
Dmitri: Yes, ID required but nothing else
Drummond: R-cards should contain much of this information

Endorsement credential was brought up - public or private

TASK: Dmitri screen shots

Pivot: Instead of one pairwise ID, have array of participants
TASK: Dmitri screen shots

Relationship VC *and* endorsement credential
TASK: wasn't clear on the endorsement cred thing (someone with the name R-something brought it up?)

Q: What is a trust community?
Drummond: Any formation, family to nation state, of humans

Brendan asks: Do we want one schema for r-cards?
TASK: didn't get the answer to this

TASK: Add as needed. Did my best! -Rob

Alberto's AI Notes & Transcripts

AI Summary
The discussion focused on the concept of verifiable relationship credentials (VRCs), which allow individuals to share specific aspects of their identity with others. Key points included the importance of personas, the need for machine-readable terms, and the potential for multiple relationships. The W3C specification for verifiable credentials was referenced, highlighting

standard elements like ID, type, issuer, and proof. The conversation also explored the idea of pairwise relationships, where both parties share a unique identifier, and the potential for separating vouching statements from relationship statements. The goal is to create a standardized model for VRCs that balances privacy, verifiability, and usability.

AI Action Items

- [ ] Explore how the VRC specification can align with existing standards like vCard.
- [ ] Determine if there should be standard property names for certain VRC fields, or if it should be more open-ended.
- [ ] Provide links to related documents and projects mentioned in the discussion.

Recording
https://otter.ai/u/--tL6v6SPS8mKs6EebfPtPwJ1pY?utm_source=copy_url

Transcript IIW ASML session 2_otter_ai.pdf

Raw Notes:
Topics Covered

- Introduction to VRC (Verifiable Relationship Credential) and what FPP (First Person Project) is.
- How to explain VRCs to newer participants.
- Overview of Personas and R-Cards.
- Multiple questions raised around R-Cards and VRCs.
- Context and purpose of VRCs — why they exist.
- VRCs help create the trust graph.
- VRCs act as anchors within ecosystems.
- Relation to W3C specifications.

Technical and Conceptual Discussion

CredentialSubject

- Question: Does a VRC require a URL or web server?
- Discussion around DID method requirements.
- Mentioned SCIDs as possible formats, with webvh being one.
- webvh supports peer-to-peer communication, possibly used for personas.

Public Issuance

- Should be human-readable, machine-readable, and “vibe-readable.”

Dmitri’s Input

- Each property should be understood conceptually (like a UML diagram).

- Entities include: `knownPersonas`, etc.
- Emphasis: Personas are very important.

Personas

- Personas are facets of relationship generation.
- They represent who is sharing what with whom (e.g., *Bob shares personas with Alice*).
- Mentioned directionality in `credentialSubject`.
- Each side of a credential has personas associated with it.

Relationship & Endorsement

- Discussion on Endorsement Credentials.
- Question: Should endorsements be a separate data model or credential type?
- Talked about "vouches" and "statements."
- Human-readable elements should appear in R-Cards.
- Negative ("bad") statements don't need to be public.

Key takeaway:
Relationships and Endorsements are different.

Cryptographic Considerations

- Question: How do IDs connect statements and relationships?
- Concept: Two IDs (representing two parties) connect to one shared ID through cryptographic proof.
- The credential includes both issuer ID and subject ID.
- The issuer signs the credential, while the other party signs the presentation.
- After issuance, both sides confirm via mutual presentation.

References & Standards

- Mentioned DIF Endorsement Credential Schema.
- Also referenced LinkCreds, U.S. Chamber of Commerce, and related trust frameworks.
- Discussion: What defines a Trust Community?

R-Card Structure

- Personas appear on both sides of the credential.
- R-Card design should be scalable with a skeleton JSON-LD context for flexibility.
- Could resemble JSON-based vCards

Recommended Fields:

- `did`
- `name`
- **(and other persona attributes)**

Question raised: Should relationships be unidirectional or bidirectional?

KERI Plus W3C VC Interoperability

Session Convener: Kent Bull
Session Notes Taker(s): Eric Scouten

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

https://ericscouten.dev/2025/iiw41/#session-7c-keri-plus-w3c-vc-interoperability

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

Working update on GLEIF-supported work to turn an ACDC into a W3C VC DM 1.1 or 2.0.

Fundamentally trying to solve the problem of making an ACDC credential resolvable by a client using W3C VC technology who doesn't actually understand any of the KERI stack.

Is it possible to go the other way? tl;dr: No. IOW can a W3C VC be turned into a valid ACDC? No, because KERI has tighter security requirements than W3C. One example is the use of JSON LD contexts, which are vulnerable to schema malleability attacks. KERI doesn't rely on any web infrastructure as part of its security posture.

Problem: A lot of the security libraries want access to private key material in order to sign.

Utah mentions that there is also work to make ACDCs available as mDLs as well. Proof of concept demonstration at the SEDI summit last week.

ACDC has introduced a new "cargo" field in the ACDC which represents a signed commitment to a particular serialization of (for example) a W3C VC credential, which then gets placed in the ACDC chain.

FIGHT CLUB: The Kids Are Online

Session Convener: Swan Black
Session Notes Taker(s): Swan Black, When Leggett

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

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

Session Brief:
Scope
This is a plain-language discussion about the lives of children on the internet, and the role everyone else in global society plays in that. If a point can't be plainly stated and directly connected to something a kid on the internet actually experiences, it's out of scope.

Base Rules
The first rule of fight club is no one talks about fight club, but what I really mean is that this discussion should be filtered out of this room through a similar lens as say, an AA meeting where the point is the content and not specifically who said what. There will be moderation by Swan, aka Swanocracy. After 20-30 seconds of drift Swan will verbally/audibly draw focus back to the scope of plain language on the experience of kids on the internet either from their or the rest of our points of view.

The Audience will Audit Swan by raising their hand if they oppose the re-direct to cancel it, majority rules.

Keep this Lively: How we'll fight Fair
Key Ideal: Seven sentences should be the top; three sentences is perfect. Stop tucking your metaphorical thumb: your point should not test mental endurance or require sophisticated expertise. As you talk, imagine you're giving a sound bite to your cool cousin.. someone skeptical but curious, and NOT like you're delivering a proposal to a committee or manager.

CONVERSATIONAL DEFINITIONS
On the internet: In contact with systems or people through a networked device
Internet: The mesh of servers, companies, code, and people that moves information and money.
Child: A person still learning judgment; an individual human not yet able to give meaningful consent.
Adult: Anyone building, governing, profiting from, or choosing to use what children are passing through and/or trying to reach.
Governing body: Whoever writes or enforces the rules: state, company, or community.

BOUNDARIES
This is not a space for theory or invention. We're talking about **the living problem the tech is supposed to solve**, not the tech itself.

- No hypothetical architectures (“what if we built…”).
- No abstract “trust frameworks.”
- No deep moralizing about parents or governments/understand the spectrum.

Everything said here must tie back to what kids are actually encountering, and what we’re enabling, preventing, or considering in a DIRECT, one to one way.

Fight Club: The Kids Are Online
Session notes

- Format: circle. Introductions: each person said "My name is ___ and I am here to fight." Guest from Japan introduced herself in her language. Set tone: honest conflict, plain speech.
- Opening claim: kids are already on the internet. This is not optional. The question is what environment we are building around them.
- Surveillance and shrinkage of private space
    - Multiple people: constant surveillance (tech and social norms) has removed spaces where kids can be messy, test boundaries, and grow.
    - Comparison to older childhoods (woods, neighborhood play). Those spaces allowed experimentation. The internet functions now as the wild space kids enter.
- Attraction to subversion
    - Internet as the modern "forest." Kids are drawn to transgressive, subversive content because exploration is part of development.
    - That attraction is not pathology. It is part of growing.
- Control versus autonomy
    - Strong pushback on adult hubris. Adults should not assume full control over kids' online lives.
    - Tension remains: real safety risks exist and cannot be ignored.
- Testimony of harm
    - One attendee described being groomed online as a teen and later trafficked.
    - Frustration with responses that treat this as only individual crimes instead of systemic failure.
    - It was discussed that a culture of tolerance around grooming children has grown because companies and celebrity figures groom children to make decisions that put them at higher risk of exploitation, i.e. “Don’t get your degree and just come work for me” but also in the sense of marketing.
- Young people in the room
    - Teen and young adult speakers described alienation from adults and feeling unseen or invalidated.
    - They reported a pervasive issue with adults in trust roles who lack the empathy or knowledge to meaningfully help.
- Cultural harms
    - Cringe culture, public shaming, and exposure make kids afraid to be themselves.
    - Being visible is not the same as being safe.
- Emotional throughline
    - Recurrent themes: watched but not believed; exposed but not protected; lack of realistic hope.
- Final reflection on agency and inclusion
    - Children are a unique minority everyone passes through and the most vulnerable historically.
    - Solutions cannot just center kids. Kids must be involved personally and directly in design and policy.

    - We need to understand different perspectives, needs, and generational trauma that shape children's trajectories as well as adult responses.
- Practical implications discussed
    - Shift from blame of individuals to fixing systemic factors that enable harm.
    - Build ways for kids to be heard safely in design processes.
    - Rethink "safety" beyond surveillance and moderation to include trust, privacy, and routes to real help.
- Meta note about format
    - The Fight Club format forced plain speech and direct accountability.
    - Conflict produced contact. People stopped theorizing and started reckoning with concrete experiences.
- Suggested next steps (from the room)
    - Create channels to include young people in authentic ways in design conversations.
    - Document survivor testimony and perspectives as system evidence, not only anecdote or in pursuit of justice or restoration.
    - Prototype interventions that prioritize guardrails that child agency and measurable safety outcomes.

State-Endorsed Decentralized Identity (SEDI) for Dummies

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

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

Slides: SEDI for Dummies 10-22-25)

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

Type Your Notes Here

SD-JWT entry level

Session Convener: Lukas Han
Session Notes Taker(s): Lukas Han

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:

slide: SD-JWT Entry Level

State of the State: Tracking and coordinating Public Policy

Session Convener: Ethan Veneklassen
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

Biometric bound verifiable credentials

Session Convener: Richard Esplin
Session Notes Taker(s): Haruki Oyama

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

Slides
https://docs.google.com/presentation/d/17Bsd2eVqyjNkHkxM70nOFZmB94JjHl98Wl9HbR2nUjM/edit?usp=drivesdk

Recording of talk from EIC
https://m.youtube.com/watch?v=ih_W38GlRMI

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

Starts with self-introduction of speaker and participants
Traditional approach is to trust the wallet biometric, but
    People hand their phones to others around them
    Wallets can't be trusted, so we need a trustless architecture
Verifiable credentials help us trust information taken from the holder. If you ask a person for their information directly you can trust that information whereas online you could have someone else with the same name
What speaker is trying to do: only holder gets to use the vc, in a privacy preserving way.

? Is the biometric compiled through the source? Security tradeoff
    Depends on the integrated biometric
    API in wallet sdk spins up the biometric plugin
? Issuers do have biometric data already
    The proposal is an improvement around that
    Different legal regimes see this issue differently

Key architecture question 1: How do you store your biometric? (database, decentralized storage, user-stored)

- Benefit of using credentials to manage the biometric tools is enabling user-stored

? Would the user-stored be proprietary or is there a standard

Key architecture question 2 and 3: where is the biometric collection and comparison
    sensor at issuer/wallet, sensor in wallet (tradeoff)
    speaker's ecosystem can support multiple biometric schemas
? biometric distills to a number, 1. how are you protecting that number 2. difference between android and ios sensor
    the difference between the two the speaker does not know

participant: android (many different price points leads to many different sensors of different quality) apple (high price point with homogenous sensors)
? What if I have an android phone but I also have an ipad. How can I share my credential between the two

speaker's solution: third party services that the product is connected to allows for interoperability

tradeoff between on-device and cloud comparison

on device: data does not leave device but device must be trusted
tradeoff preferences depends on use case and client
on-device comparison and sensor at issuer/verifier - does not work
cloud and issuer - biometric data must be stored by 3rd party
on-device sensor in wallet - biometric data never leaves the device
cloud and wallet - optionally can store biometric data locally

? Does not make sense to trust a device for collection but not for comparison, can always send to the comparison server

the iProov team says in cloud environment there are ways to detect compromised devices

Truvera's approach

1. do enrollment
    a. the ecosystem determines the biometric for the user
2. local biometric check
3. credential verification

Presenter explains the credentials which consist of

1. enrollment
2. biometric check
3. biometric bound
    a. only technical challenge is integrating biometric into the devices

? the biometric ids aren't private, from a privacy perspective would the biometric id be different

zkp via bbs

linking attribute is correlatable so need to decide in use case if that is detrimental

summary

what other biometric ideas are in the space

? is offline presentation possible

possible with tradeoffs: need to cache issuer keys, recognizes that revocation may be stale, and need on-device biometric comparison

participant summarizes core idea of presentation for clarification: you guarantee that the data can only be shared in the context of the biometric?

if biometric fails, that is detected by the verifier who can reject the data (but the data was technically shared)

? if I have a driver's license, nobody tells me what kind of wallet I can keep it in. Using your technology, what needs to happen for the credential to be a VC that can be used anywhere? Do I have to pay to get an ankle bracelet to use the service?

the biometric is moving around the ecosystem, so the ecosystem has to agree on the biometric that will be used

but multiple biometrics providers can be used simultaneously

? but my driver's licence can be used with any verifier

but the drivers license discloses your photo to every verifier; this is an improvement in ensuring the biometric isn't shared

? is there a way to move from service to service without sharing biometric data with every verifier

speaker would like an approach that can do that, but doesn't know of a way to do so

? how is the check done by the verifier

gives the verifier 2 credentials: credential + biometric who checks the compound proof

? do users see the biometric check

users do not see their biometric checks

? how do you ensure the biometric check comes from the same wallet as the main credential

credentials can be linked to wallets so the verifiers can check they come from the same wallet

some theoretical use cases might benefit from the biometric being done from a different wallet than the main credential

biometric check has a short expiration

? how to pragmatically be implemented on user device, a wallet cannot read off of the fingerprint sensor

iOs and Android don't give access to the fingerprint data

uses third party biometrics (generally use the camera)

? 1-to-many biometrics may have collisions; is this secure

1-to-many work in small use cases

some vendors believe they can be used in large use cases

1-to-many matching can allow smooth UX where the user doesn't need a wallet or to remember any type of identifier

for large use cases, we generally ask the user to provide an identifier to store the biometric template so we can do 1-to-1 matching

comment: you have to trust the verifier anyways with the biometric ID

Password Auth w/ PQC in the Quantum Era

Session Convener: Bryce Frey (brycefrey@google.com)
Session Notes Taker(s):

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

https://pqshield.github.io/nist-sigs-zoo/

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

First went over a TL;DR of the threat of quantum computers to classical/traditional cryptography.

Then:
The risk to passwords is for any site that has been sending their user's passwords in plaintext with only TLS encryption protecting them. As pre-PQC TLS can be (and should be assumed to be) stored now by an adversary to be decrypted later when they have access to quantum computers. (why do some sites *still* send the plaintext password instead of hashing? Old infra/wanting to do password strength checking server side instead of client side/etc.; I'm not here to make judgements or chastise, only to inform on ways to improve while preparing for quantum computers).

Any site that sends over some derived hash of the password over TLS, that password hash should also be assumed in scope for store-now-decrypt-later. But, hashing the password with a different salt can result in a new, safe hash.

I went over two options for password auth w/ PQC, explicitly acknowledging that their threat models do not match every site's threat model, and some sites will need to choose a different option, such as a PQC OPAQUE or PQC PAKE once one becomes available.

Model 1: encapsulating the plaintext password using a PQC KEM, such as ML-KEM (or, even better, a hybrid PQC/traditional crypto KEM, like X-Wing, which combines ML-KEM-768 & X25519; just incase lattice math is broken on classical computers). This allows the smallest change to existing password auth infra for many sites. May be the easy way out. Also allows continuing to do password strength checks on the server.

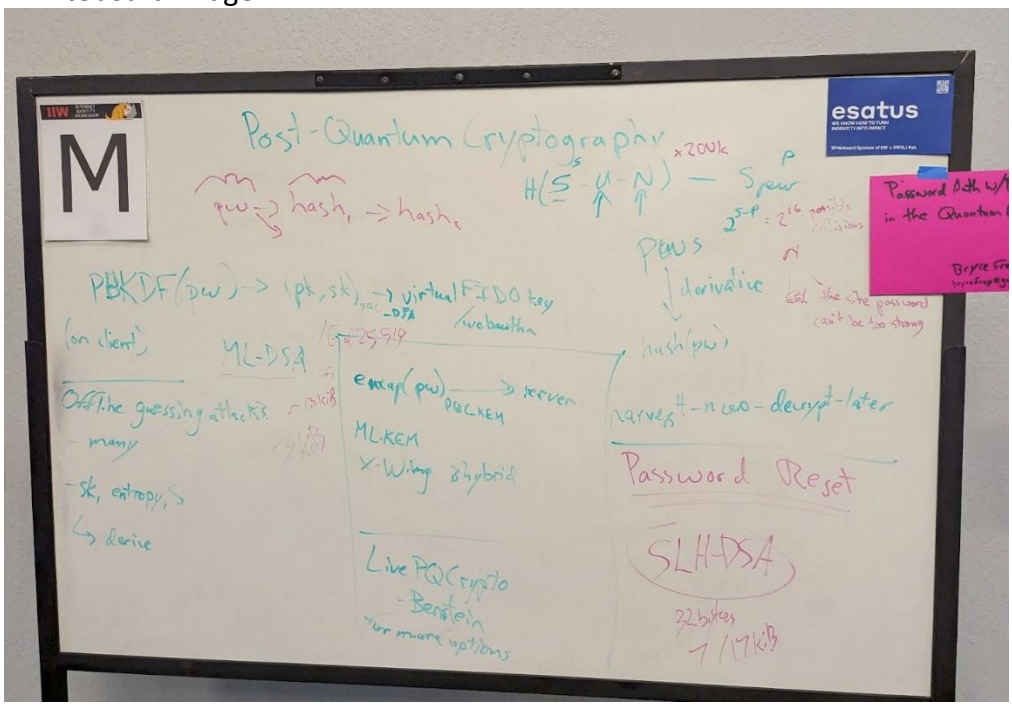
Model 2: deriving an asymmetric keypair using a PQC algorithm from the password using a PBKDF, and then using a challenge-response protocol with that keypair. FIDO, while having a more complicated spec, is probably the best choice for most since sites should be adding a FIDO server for passkeys, and then they can just use the same backend. To do this, a site can't depend on the browser or the OS for their webauthn/fido APIs, but rather need to reimplement/mock (since not all parts are needed) the FIDO/webauthn spec in the frontend code to make the keypair a 'virtual FIDO key' (my terminology).

One case when Model 2 doesn't have the right threat model for everyone, is that it may still allow for spearphishing: an attacker can trivially get the site salt and the user salt (since it must be available on the client side to derive the keypair on the client side); and then keypairs can be generated for a common passwords. This would not work at scale, since there are still site-specific and user-specific salts, but it may be effective against individuals. This threat model has not been fully fleshed out.

What PQC algorithms to use? ML-DSA will be the default for most (it was one of the first NIST approved; while its physical parameters are not as good as EC, they are generally *OK*; implementations will be widespread for the aforementioned reasons). ML-DSA has the risk that it may be broken on classical computers with the additional scrutiny that it will now get. A better solution is to combine ML-DSA with a traditional algorithm (such as Ed25519) to protect against that possibility. Another option (Bryce's preferred) is to instead use SLH-DSA. SLH-DSA unfortunately has very large signatures (7-17 KiB), VERY large signing & verification times (up to 14,000x ML-DSA; see signature zoo for more details), but very small public keys. The large signature situation is great, but 17KiB is manageable. The very large signing times shouldn't be an issue on modern desktops/laptops/phones. But most importantly (and why Bryce likes SLH-DSA specifically for virtual FIDO keys), the only mathematical basis that SLH-DSA is based on for cryptographic security is the cryptographic hash function; i.e., as long as we can't break cryptographic hashes, we can't break SLH-DSA; and all signature algorithms depend on the strength of cryptographic hashes in addition to their trap-door function (thus, if you break SLH-DSA, you've broken every current signature algorithm).

Had some discussion about comparing the different PQC algorithms (approved and proposed). See signature Zoo linked above.

Whiteboard image:



SESSION #8

Digital Credential API for openid4vci

Session Convener: Kristina Yasuda, Paul, Lee
Session Notes Taker(s): Lukas

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 do we need to solve to integrate DC API with Openid4VCI

Last time: issuer metadata can't be fetched so we put it in credential offer
—
Most of the case, auth on the website and send a credential to wallet (pre-auth flow)

Security attack:
browser and phone is good state, user installed malicious wallet

DC api => malicious wallet said "I can do it" => it can't talk to issuer (wallet attestation needed)
So instead, it redirects the offer to a good wallet and processes it.

1. auth flow?

solutions from PR (Wallet selection Binding during issuance)
1. dc api return which wallet is selected
2. allow-list of the wallets
3. issuer could provide binding key when making the create call, platform would pass the wallet hmac (binding key, selected wallet identifier)
4. issuer could provide allow list of wallet attestations to be standardized PKI

- **Wallet attestation relay problem**

Harms -> Story (Turning a harm into a story using Story "Mad-libs")

Session Convener: Erica Connell
Session Notes Taker(s): Erica Connell

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

Stories, Harms.

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

We collaborated to create the following story:
Susie's Story

14-year-old Susie has the perfect gift idea for Aubry, a popular girl in her friend group, whose birthday party is coming up: a rare Labubu. Susie is confident with computers, and quickly runs a search for retailers. Her problem isn't finding one, it's that she has a prepaid gift card with $50 on it, while rare Labubus can cost hundreds.

In the search results, Susie sees her salvation: LabubuFinder.ai. She opens the site and chats with the AI assistant to find the rare Labubu. Happily, the website has a few available. Sadly, none are within her budget. The closest she finds is $75. She updates her search prompt to include her budget limitation. The AI Assistant is very understanding and supportive of her situation, it cannot find one that fits. What it does next is offer what it explicitly tells her is a reasonable alternative solution- to use her card and pay the difference on another one. Susie didn't think of that!- and proceeds to purchase the desired Labubu using her mom Betty's credit card information. After all, mom has always supported her social engagements. Susie even makes sure she receives the confirmation email. She makes a mental note to negotiate repayment terms with her mom. Proud of her independence and problem solving skills, Susie feels accomplished.

After a week, there's still no Labubu. Susie gets anxious. There's only a week until the party! The confirmation email promised shipping in 24 hours, and now the tracking link only returns a 404. Something is definitely wrong, and Susie turns to her mom for help. Coincidentally - or is it?- Betty is also looking for her for an explanation about the unknown credit card charge on her statement. Susie quickly explains, and Betty pieces everything together.

Using the moment as a teaching opportunity, Betty explains how to spot fraudulent websites, practice safer online habits, and understand financial responsibility. Susie learns that independence also means knowing when to ask for help. Betty contacts the credit card company to dispute the charge and report the scam. Susie even gets her $50 back, but more importantly gains valuable lessons about verifying online sellers and protecting herself online.

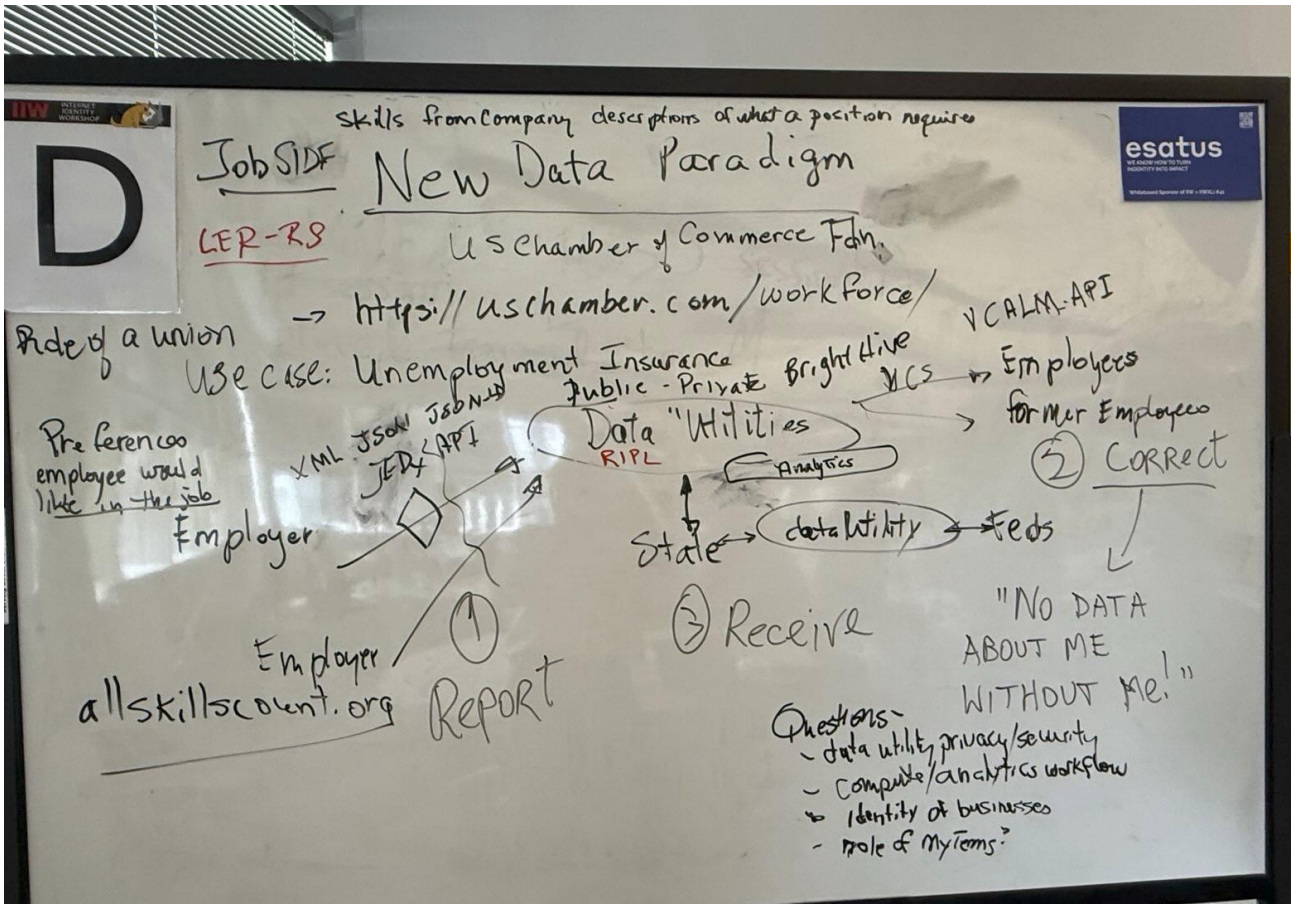
As moms do, Betty comes to the rescue by helping Susie find a legitimate retailer with overnight shipping. Susie goes to the party, gives Aubry the gift to her great delight, and then prepares to work off her incurred expenses - by babysitting for the next 6 months.

The New Data Paradigm

Session Convener: Phillip Long
Session Notes Taker(s): Phillip Long

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

Resources: New Data Paradigm - presentation (Oct.2025)
New Data Paradigm - Paper
Whiteboard Pic —
JEDx API |
VCDM v2.0 |



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

Current employer administrative data and education/training records of employees are reported to states in 50 different ways.The New Data Paradigm involves a structured coding of data employers submit to states wherein they operate about their employees. The Job and Employment Data Exchange (JEDx) has implemented an API (JEDx API), in collaboration with the

HR Open Standards organization and 1Edtech, to securely transport administrative records and Learning and Employment Records (LERSs) about employees from the employers to a new public-private data utility. The JEDX API is payload agnostic in that it can carry flat files, spreadsheets, XML, JSON, and JSON-LD data structures, and wrap them in an outer credential,cryptographically signed, to guarantee tamper evidence in the transmitted data. The API also features autocoding to add missing information in transit.

The new shared data facility serves as a collection, aggregation and reporting CAR) resource for the state and its employers. The state draws data from this utility for its reporting and analytics work, some of which must be presented to different federal government agencies. The states reporting to different federal agencies is proposed to model the a similar architecture, where the state places the data it must send to the federal government in a data utility from which the different federal agencies pull it

The new data facility opens opportunities for additional services. The data employers report about their workers could be transformed into LERs and signed by the the data utility itself and offered directly to the employees themselves.

Non-Binary Approaches Human Verification - from 0/1 to 0.0/1.0 /Discussion Session

Session Convener: When Leggett
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:

This was an open discussion session centered around two related topics: human verification and non-binary scoring. In other words, rather than a simple Yes/No, what could an alternative look like? Would it look like a reputation score or a credit score?

The conversation ranged, talking about the dangers like:

- Who gets the keys?
- How is it governed?
- How do you avoid abuses like what happened with Credit Scores?
- Is this public infrastructure or tech feudalism?

Here were some conclusions with general consensus:

- A range based score that had a kind of transparent rubric for scoring, was a useful kind of yardstick that could be used for contextual threshold based gating, rather than using a binary.
- If there are trust authorities involved in the scoring, it should be a system that allows multiple, or even many authorities
- The needs of actors using the scoring would be varied and contextual. For different contexts, different thresholds would be sufficient, as well as which kinds of evidence are contributing to the score: i.e. which claims can be made

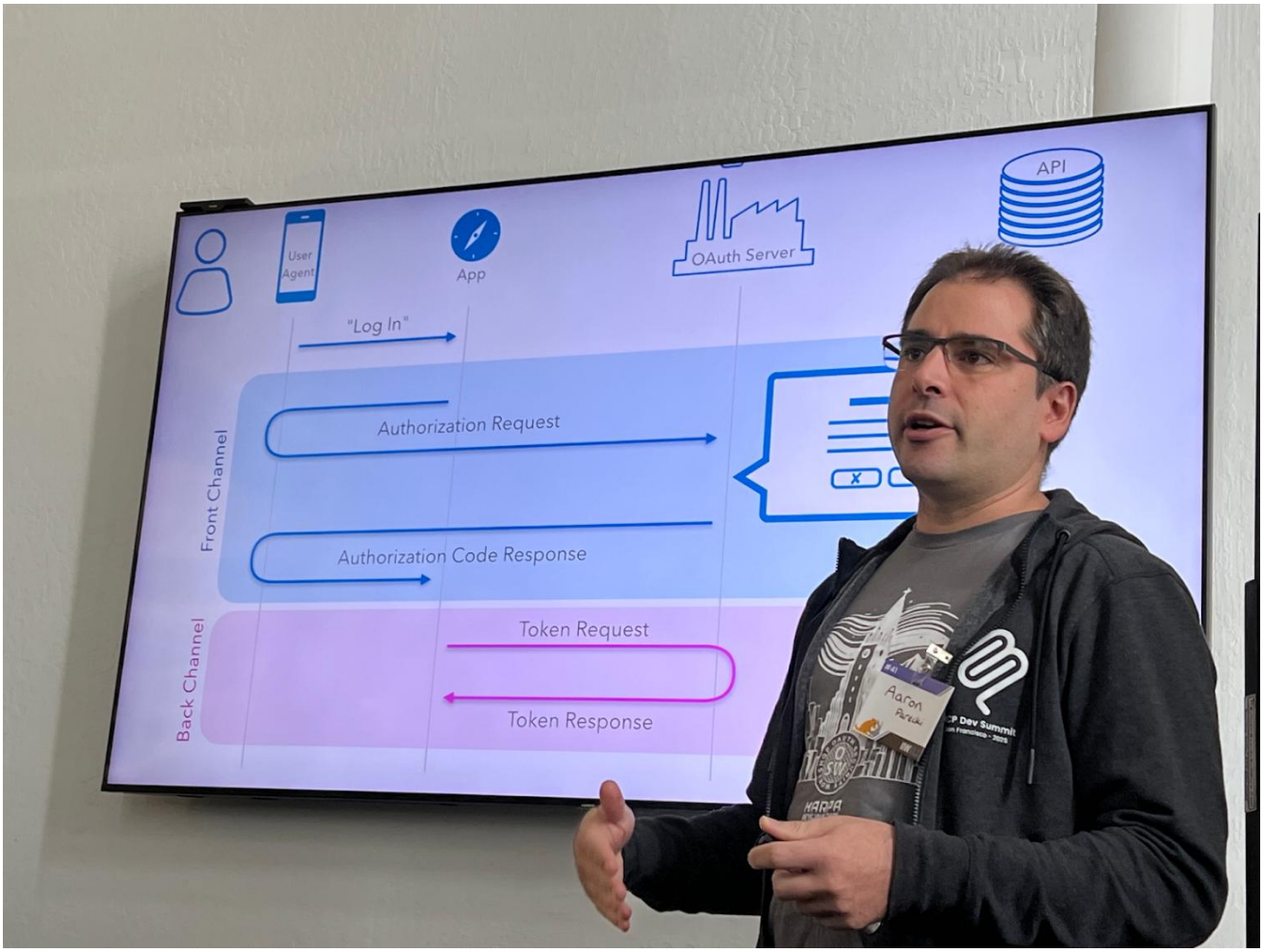
Scores should come from, and provide different options, for positive contribution. For example, mobile drivers license or passport, but also options like the First Person Project.

OAuth for MCP

Session Convener: Aaron Parecki
Session Notes Taker(s): Kent Bull

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:

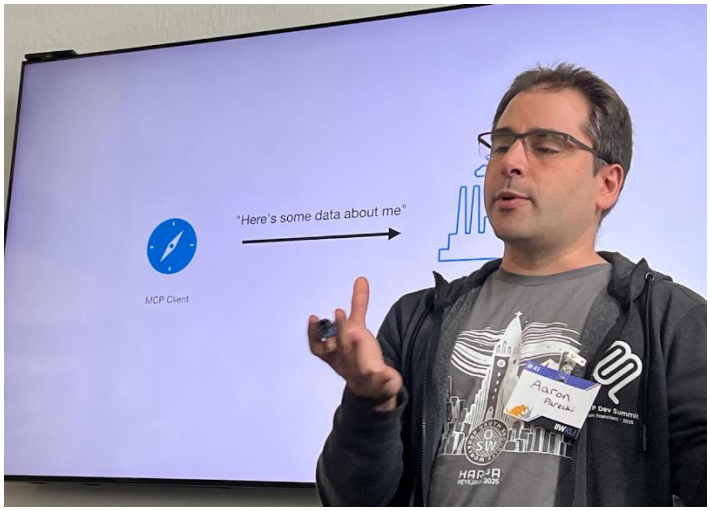


Existing model that is being used in the past worked for a long time, yet this does not work for MCP.

Why doesn't it work for MCP?

The problem is that one of the goals for the user experience of MCP is that a chat bot can give a server a new endpoint that the MCP server has not seen before. This has driven a lot of things that MCP has had to introduce to OAuth.

The user will connect their agent to an MCP server they have never seen before. That client must introduce itself to the OAuth server.

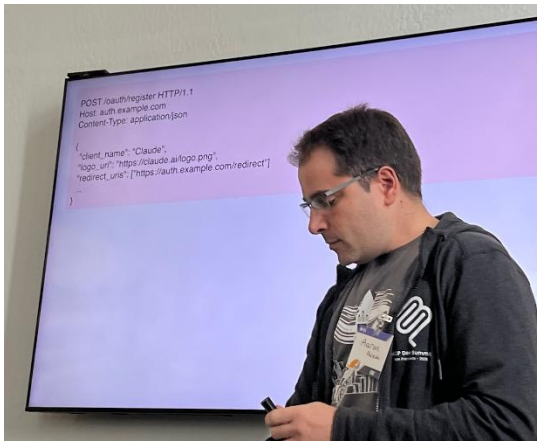


Dynamic client registration is one potential solution to this.

A bunch of JSON is submitted from your AI agent, like Claude, to the OAuth server. There is currently no way to establish the authority of that self-attested registration request to the OAuth server.

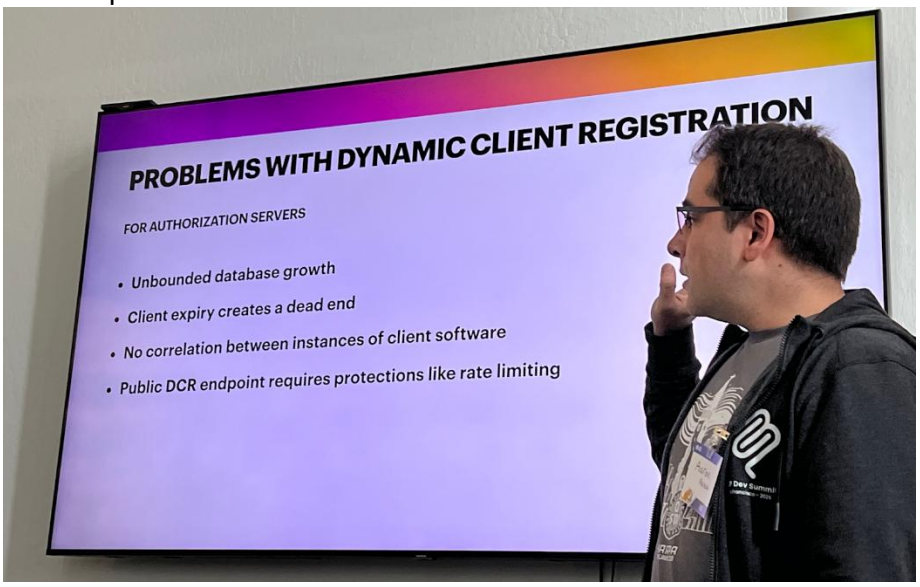
There are hand-wavey key management problems.

Different types of clients have different types of problems and solutions. Server side apps are effectively permanent instances of a piece of software, mobile apps are mostly persistent, and single page web apps are a new app every time the page is refreshed. This causes **unbounded database growth**.



Solution in the spec is to use “Software ID” yet very few people do this. Public DCR (Dynamic Client Registration) endpoints require protections like rate limiting.

Clients can't tell if their client ID is still valid so they end up reregistering frequently, sometimes on each request.



Solution: Client ID Metadata Document

Problem: authority for the DCR request is interesting only to a subset of the apps that implement OAuth servers. Some OAuth clients have no interest in establishing authority (via a signature) of a registration request, other clients do care about it.

Instead of posting every time a user logs in it hosts metadata about the app at a URL.

Question: Is the host of the metadata the same as the client host?
Answer: not necessarily. They can be separate.

Question: Then how do you establish authority of this registry request?
Answer: …

Moving on,
If you host the metadata

Security angle is answered by redirect_uris section of the metadata document.

Making this better for webserver based apps you can use "jwks_uri" showing a list of keys that are allowed to sign a request.

Question: is this like a DID Doc?

Answer from Justin: software statements in DID Docs help address this question
If you want client authentication then you would not be able to use traditional client secrets at all with this.

Discoverability and being self-evident is important.

Question: How does this work for an instance of a client?

Answer: let's go back to mobile apps. Each download of a mobile app is a separate instance. The intention is that each mobile app would use the same URL.

Regular OAuth, developer of mobile app would go to the web portal of the service they are going to, like Google calendar, and would have gotten a client ID, put it in the source code, compiled the app, and then put the app in the app store for download.

What about Agents or MCP Servers? Does an MCP Server know a client is a client? No, not yet. And it mostly doesn't matter today, depending on your risk tolerance.

New idea: Attestation based client authentication
App Backend (AB) - app, once submitted to the app store, gets platform attestation, sends it to a backend, and then the app can know whether a given app instance is legitimate. You use an app attestation for this. For example, for global high scores for a game leaderboard.

The AB can give a well defined JWT back to the app signed by the AB private keys. This JWT is then forwarded to the Authorization Server (AS) of the MCP server. The MCP server's AS would then look up example.com/clientid.json to get the public keys.

Yet this only matters for Auth Servers that cares about signed DCR requests. There will be a fragmented ecosystem of some Auth Servers that care and some that do not care about signed DCR requests.

Even the platform identifier is not a guarantee, it is a sign of an authentic client, not a guarantee.

The trust model this relies on is the domain name. The security of the request and signing is based on the security of the domain name. DNS + CA Certificates (PKI) security.

vLEI Authentication Organizational Login (vLEI) with ecr credentials

Session Convener: Christoph S, Vincent V, Stefan I
Session Notes Taker(s):

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

NO NOTES SUBMITTED

Trust Registry Query Protocol

Session Convener: Andor, Darrell, Drummond, Phil
Session Notes Taker(s):

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

https://trustoverip.github.io/tswg-trust-registry-protocol/#introduction

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

Trust Registry Query Protocol (TRQP) allows cross network queries of ecosystem information about PARC

- Principal: Who are we talking about?
- Action: What can they do?
- Resource: What can they do it with?
- Context: Where can they do it?

Same policy language as CEDAR and AuthZen

Two key endpoints

- Authorization: test for current action
- Recognition: registry of registries

A - recognizes -> B - authorizes -> B'

Term "authorization" is confusing because it's a bit different from OpenID authorization, but there isn't a better term.

OpenID Federation Draft 43 introduces similar policy language.

TRQP is important for discovery, but is especially useful for corroborating information across trust registries.

Registry shouldn't report on people, but on issuer / verifier organizations.
Context is provided by optional fields for adding information specific to an ecosystem.

Death and the Digital Estate / OPEN ID Foundation Community Group

Session Convener: George Fletcher
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

Women in Identity? - What should an organization focused on inclusion be doing with and for the community of ID Professionals?

Session Convener: Elizabeth Garber
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 #9

OpenID 4VC1/V8 - HPKE -> how to proceed?

Session Convener: Kristina, Gareth, Christian
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

OpenID AuthZEN: The "OIDC" for Authorization

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

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

Slides:
https://drive.google.com/file/d/1Su6WonsbCmsiphQtP73XeeM6B9LKH8k1/view?usp=sharing

OpenID AuthZEN WG: https://openid.net/wg/authzen/

Current (Final) Spec: https://openid.net/specs/authorization-api-1_0-04.html

Interop site: https://authzen-interop.net/

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

Q: Partial evaluation - is it part of the remit? A: Yes, but post-v1.
Q: What shared signal events would AuthZEN consume? A: Any data that relates to authz.
Q: What shared signal events could AuthZEN produce? A: AuthZ decision logs?
Q: Paging styles supported? A: cursor-based. Deferred offset/limit out of v1, but open to adding it as optional.

Abstraction for decoupling Verifiable Credential Formats and Zero Knowledge Proof libraries - Now with concrete product group demos!

Session Convener: Mark Moir, Adrian Ross, Mike Kaufman
Session Notes Taker(s): Mark Moir

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

Session slides:
https://www.dropbox.com/scl/fi/s3fkf6pauitcrnpbofi31/2025-10-IIW-slides.pdf?rlkey=b4piuwdjb5lrhew0q92lthpso&st=y8qpxw90&dl=0

More detailed presentation about the implementation of AnonCreds over our abstraction are here: https://www.dropbox.com/scl/fi/rzac0hd3zw8boq50vignw/IIW-Apr-2025-VC-and-ZPK-abstraction-final.pdf?rlkey=1i4vzm8rzm7ssu4eqt1w3qbda&st=vxilkqxo&dl=0

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

This session provided an update on work presented at previous IIWs, in a new context.

As reported at previous IIWs, research work done in Oracle Labs has established an abstraction for decoupling verifiable credential formats (above the abstraction) from the cryptographic/zero knowledge proof libraries that support them (below), enabling a range of benefits, including the ability to easily adopt new or updated libraries for reasons such as performance, security, features, project health etc.

Mark and Harold, who did this work (along with various interns), have recently joined a product group with whom they had already been collaborating; this session reported for the first time on this collaboration. The group is building a solution for integrating Decentralized Identity features including support for DIDs and verifiable credentials into the Oracle Blockchain Platform ecosystem.

The session began with an introduction by Adrian Ross on the product group's work integrating Decentralized Identity features, and included demos showing the use of AnonCreds. Various data such as schemas, credential definitions, and revocation information are stored in the Verifiable Data Registry based on the permissioned Oracle Blockchain Platform.

Next, Adrian Ross and Mike Kaufman presented two demos. The first demo showed the setting up an Issuer, issuing a credential, and presenting and verifying a presentation, with the Holder/Prover role on a mobile device. The second demo demonstrated revocation of a credential.

Next, Mark Moir gave an update on work done in Oracle Labs since the last IIW, which included completing support for all features of the abstraction using two underlying cryptography/ZPK libraries (except for one feature that is not yet supported by one of them). Then, he described

new work supporting AnonCreds over the abstraction, reporting that they have successfully made changes to the anoncreds-rs and anoncreds-clsignatures-rs repos, enabling building an anoncreds-rs library with the same interface, but using the cryptography of any underlying library that implements the abstraction.

Then, a third (prerecorded) demo was shown, repeating the first one, but using the cryptographic library (AC2C) of AnonCreds v2, via the abstraction. This demo showed proof generation and verification noticeably faster than in the first demo, due to replacing the Camenisch-Lysyanska (CL) signature baked into AnonCreds with the more modern and lighter-weight BBS signature scheme, as well ZKPs for other features, with AC2C's implementations, via the abstraction.

Mark also explained that, although the anoncreds-rs interface is unchanged, for revocation, the usage has to be modified, for reasons explained below. Therefore, the demo using the abstraction does not yet include revocation, and there is more work to do to make it work.

The reason usage for revocation has to change is related to using cryptographic accumulators via the abstraction---rather than the Tails file approach that is intimately tied to the CL signatures implementation used by AnonCreds. This has the significant advantage of not requiring all devices to download a Tails file, whose size imposes a practical limit on the number of credentials that can ever be signed by a traditional AnonCreds Issuer. The disadvantage is that we lose the ability to create a "witness" for proving nonrevocation directly from the Tails file, and instead must apply every "update" to the original witness to acquire a current witness.

The session was well attended (maybe 20 people?), with lively engagement via questions and discussion and positive feedback from the audience.

The slides presented in the session here:
https://www.dropbox.com/scl/fi/s3fkf6pauitcrnpbofi31/2025-10-IIW-slides.pdf?rlkey=b4piuwdjb5lrhew0q92lthpso&st=6ks516ea&dl=0

A more detailed presentation about the implementation of AnonCreds over our abstraction are here: https://www.dropbox.com/scl/fi/rzac0hd3zw8boq50vignw/IIW-Apr-2025-VC-and-ZPK-abstraction-final.pdf?rlkey=1i4vzm8rzm7ssu4eqt1w3qbda&st=vxilkqxo&dl=0

What is going on with Age Assurance around the globe

Session Convener: Shoma Tanaka
Session Notes Taker(s):

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

https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements

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

We began the session discussing how self-service checkouts verify age for alcohol purchases, comparing traditional employee ID checks with emerging technologies like facial age estimation. The group reviewed international approaches including parental permissions, digital age assurance wallets, and recent EU research outlining ten ways to confirm ages. Concerns remain about online markets and the importance of privacy-respecting but reliable age verification for both youth safety and regulatory compliance.

First Person Project and Ayra Cards

Session Convener: Darrell O'Donnell & Drummond Reed
Session Notes Taker(s): Darrell O'Donnell & Drummond Reed

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

First Person Project slides:
https://docs.google.com/presentation/d/1wz_nVjrHzth_QyYAuDWIf4w5Clg_olXvS-jMiv8GR4c/edit?usp=drive_link

First Person Project White Paper: https://www.firstperson.network/white-paper

The Special Network Effects of Ayra Network Credentials white paper: https://ayra.forum/ayra-network-effects-whitepaper/

Ayra Cards slides:

- Ayra Cards Whitepaper: https://ayra.forum/ayra-cards-and-fpp/
- Slides used: https://docs.google.com/presentation/d/12Ct-UuawEJ_-Vosda4HtUA0Ye4Z6FYw2H1vKkgFNFg8/edit?usp=sharing

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

Drummond began by providing a high-level overview of the First Person Project, with an emphasis on how it is enabled by Ayra as a decentralized trust registry infrastructure. This infrastructure makes possible what is called (in the The Special Network Effects of Ayra Network Credentials white paper) an "Ayra network credential". This is a digital credential that can be issued and verified across many different digital trust ecosystems provided they are members of the same decentralized trust registry network (which is the role of the Ayra Trust Network).

Drummond explained how First Person credentials, as a standardized methodology for privacy-preserving proof of personhood, are one example of an Ayra network credential. He then turned it over to Darrell to explain how Ayra cards are another example.

Darrell explained that Ayra cards are designed to standardize how businesses can issue employees a business card credential, a staff pass credential, or any other corporate role credential in a way that is widely interoperable and verifiable—and also easily extensible to more specific behaviors by carrying a "payload" of additional identifiers or claims. Ayra cards standardize the "dance" two parties need to do when they first meet and need to discover more about each other.

Because they are issued by a business to its employees, contractors, or others in its ecosystem, many Ayra cards can also effectively function as First Person personhood credentials (PHCs), thus killing two birds with one stone and increasing the value of the credential to all parties.

CONNECT TO Global eIDs (Live Demo) Web API & Wallet access

Session Convener: Lucas Han & Bart von der Geest
Session Notes Taker(s):

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

NO NOTES SUBMITTED

Tools For Traps - Managing Identity and Intention On Our Terms

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:

When we are connected to the digital landscape we are observed in some form(s) and fashion(s). It is fair to say that we have an identity of some sort applied to us. This identity is what could be thought of as a session identity. From the moment the device touches the connected realm, aspects of that device define that machine in those moments of connection. The device's own hardware, hardware drivers, software installations, the data associated with the account you logged in with, ip addresses, LAN MAC addresses, WiFi MAC,…create a specific session related to a specific device entity which is often operated by a person. An identity related to many things forms each time.

How can these spaces be occupied in a way that avoids system profiling funnels and the herding and nudging created by those forces? When we look at screens to operate on the other side of the glass, controlling intention while managing the degree of identity we wish to express, and how that is expressed, is a lot to think about. On the digital landscape that seems wildly complex to have to track, yet we do that all the time as we move through our lives in the Real World (RW). Spidey Senses work better here than there.

A simple mouse trap illustrates a want conveniently placed. As that want, let's call it bait, a signal releases potential energy and the hit is made…or not. With systems able to know what appeals to us and considering system designs built to move us, how can we avoid the allure of being baited. The tooling available is relative to the goal, the landscape related to that goal and the method(s) usd while in pursuit of the goal.

Example: I want to hear a broadcast available which not only streams the show for internet connected devices, but also broadcasts on FM, AM or Shortwave radio, I have two very different approaches to getting that feed with or without being scoped by a system. Can you guess which is

more residue free? What is the data cost of the differing paths to make the goal of listening to a broadcast.

Let's talk about the web and journeying there. Just like driving a car, the web is very similar in the sense that a browser (Brave, Firefox, Edge Safari, Chrome) used to surf the web is same as the idea of a car travelling the roads. Let's apply that thought framework to the digital realm.

To the car analogy: If I want to travel (browse) the web without having stickers (cookies and trackers) put on my vehicle (browser) it would be cool to have a car that rejects stickers being put on it everywhere it goes. Some web browsers and add-ons are designed to help your web browser defend against your vehicle being stickered.

Not signing up for certain types of relationships like social media or purchasing is a tooling strategy. Choosing to sign up for relationships and adjusting the settings to match your preferences is a further example of engaging those system forces on your terms. Choosing not to sign up is another tooling choice for your larger relationship with IT systems which would be referred to as Your Real-IT in this space.

The cost of avoiding these systems and their forces may be being left out by community. In social media landscapes "The Tyranny of Convenience" (Tim Wu article) where the One-To-Many (one post to many eyes since it pops up in everyone's feed) allows for one to post news and info of their world, while missing the sense that those not in the space of that system will not see or hear of it except by second hand if at all.

Much more to say:

My Terms (IEEE 7012) terms granularity removes the default hook points favoring the house and that often are mandated in the All or None contracts of "take it or leave it".

Photographic Journalism: even framing a photo to not capture street signs helps defend against fraud; NorCal Fires 2017

NASA JPL Extraterrestrial Return Protocols related to concept of bringing other worldly things down to Earth; AI like bringing an alien back from space for people to lick or not so much…

_ Rashmi Siravara: Tools to traps was one of the best sessions in play with real time experience of the concept.

The use of
Goals
Landscape
Tools Sets
Persona to identify and categorize traps was phenomenal.

Human Behaviour interplay with the OS was in reach of accuracy. Manifestation techniques co-related to the traps was touched upon to explore this topic further in IIW-42.

Trust Governance

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

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

MEDIUM ARTICLES

Trust Governance Overview
https://gluufederation.medium.com/trust-governance-6eeded59eaab

Trust Governance Architecture
https://gluufederation.medium.com/trust-governance-architecture-c8248faf5043

WIKI PAGE
https://github.com/JanssenProject/jans/wiki/Trust-Governance-Architecture

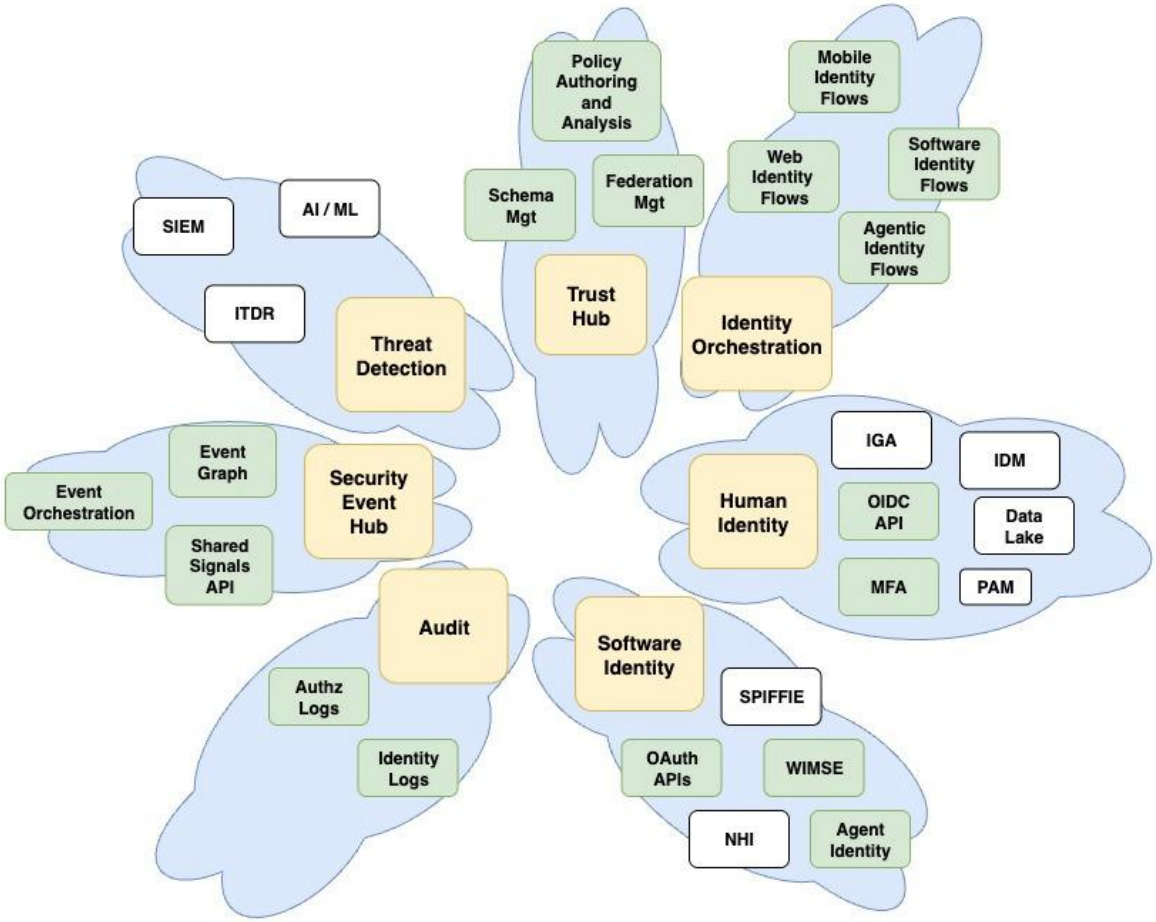
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Design principals:

1. **Governed by Design** Every policy, schema, and federation change follows the same rigor as modern DevOps. Code reviews, audit trails, and automated gates make governance continuous, not periodic.
2. **Provable by Design** Policies are verified using formal methods and theorem provers — checking for logical errors, conflicts, and unintended overlaps. Authorization decisions move from “assumed safe” to mathematically guaranteed.
3. **Declarative by Design** Access is defined in terms of *capabilities* — the combination of an Action and a Resource. This aligns governance with business operations, not just identity data.

4. **Interoperable by Design** Built on open standards like OAuth, OpenID Connect, and federation protocols, Trust Governance unifies policies and tokens across cloud, SaaS, and on-prem systems.
5. **Observable by Design** Every decision, event, and token is logged and analyzable. Built-in observability enables continuous assurance and rapid detection of anomalies.

Trust Government Components



Several enterprises and integration firms have expressed interest to collaborate on Trust Governance. Mike suggested moving this work to an OWASP Project, OpenID Community Group.

First Person C2PA Registrar

Session Convener: Luke Nispel
Session Notes Taker(s): Eric Scouten

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

See https://ericscouten.dev/2025/iiw41/#session-9j-first-person-c2pa-registrar for photos of Luke's slides.

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

Goal: Create an endorsement network of artists that recognize each other.

Looking into how to use [First Person](https://firstperson.network) credential, which has verified person infrastructure, to build an identity claims aggregator. Their ICA implementation allows Facebook, GitHub, Adobe, many other verified IDs. Then you can anchor things on the blockchain.

Have implemented their own C2PA verifier and signing infrastructure. Content uploaded to their service gets registered on blockchain. Registrar for verified persons on the Cheqd. Each Cheqd DID has a linked resources field which allows linkage to small information. Could point to URLs with additional information or C2PA Manifests hosted outside.

Purpose: Peer-to-peer artist network empowered with C2PA and Cheqd.

Interesting business model experiment: Artist can choose to charge the verifier to verify identity through this framework.

EOL of VC's Issuers & Wallets (policy/technical)

Session Convener: Ryo Nakashima
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

B.Y.O.E. (Bring Your Own Everything) App Development

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

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

Slides: https://docs.google.com/presentation/d/1MLAGQmR-J5Uq42qS5g2georPB3PpKnZhVAlSA_SZOlE

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

Assume all this IIW tech succeeds…

- Identifiers for humans and software agents
- Delegatable Permission (capabilities)
- Verifiable Credentials
- Issuer Registries
- Permissioned Storage (encrypted, replicated, offline-first-capable)

This enables: New App Dev Paradigm (the "Anti-Platform" approach)

All that tech enables BYOE App Development
Bring Your Own:

- User IDs
  - also signing keys and encrypting keys
- User Storage
- User's Contacts / Social Graph
- User Preferences and Settings
- Compute
- and even b.y.o.:
  - LLM / SLM AI model
  - Analytics
  - Comms/messaging
  - …

What does "LOGIN" look like?

1. QR Code scan or a "Login with Wallet" button (that invokes a Web Wallet)
2. App asks for:
   a. DIDAuth Request
   b. Preferenes
   c. Storage access

How much of this stack exists?

- User IDs -- use DIDs or equivalent
- User Storage - Wallet Attached Storage spec
- User's Contacts / Social Graph - use jCard + mobile contacts
- User Preferences and Settings - in progress
- Compute (we're all used to this)
- and even b.y.o.:
    - LLM / SLM AI model
    - Analytics
    - Comms/messaging

The Ask:

- Think about this.
- Consider playing around (or shipping to prod) a BOYE style
- Check out the zCap and WAS specs

Quantum Resistance - Passwordless Authentication using Existing Primitives

Session Convener: Ravi Ramaraju, Mike Jones, Andy Swett
Session Notes Taker(s):

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

https://www.hawcx.com/

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

Participants included:

- Andy Swett (Hawcx)
- Mike Jones
- Ravi Ramaraju (Hawcx)
- Riya Shanmugam (Hawcx)
- Jim Fenton
- Bryce Frey (Google)

We discussed how the Hawcx protocol defends against attacks by future quantum computers.

At the end of the session, we had a discussion about the role that Device Bound Session Credentials https://www.w3.org/TR/dbsc-1/ could play. We also discussed how the W3C standardization roles require multiple independent interoperable implementations of each feature in a final specification.

Risk of public notarization of accountability

Session Convener: Kigen Fukuda
Session Notes Taker(s): Haruki Oyama

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:

Speaker starts by explaining association sets and privacy pools
    Where does information come from? We want to trust that the information came from a source that is part of a trusted ecosystem
    trusted third party that conducts screening towards deposits
    There should be a social accumulation of trust or reputation before going into the association sets
        most researched way: decentralized association system(?)
        people can artificially increase wallet reputation
? difference between trust and reputation
    reputation is the trust within the ecosystem

sanction list and non-membership proof
    receiver needs to specify its compliance policy
explanation about VDR, best effort
    VDR is public and immutable
There could be another KYC provider issuing a verifiable credential
This model can be used to BGIN to increase accountability and unlinkability

? What does that mean
    you can ensure accountability and unlinkability within an AS to an extent

Explanation about tornado cash
    mixing service that allows for mixing of funds
    sanctioned by US government
Trying to build a system that has trust established (AS, like a trust graph almost), but with anonymity

? what is VDR
verification data record, on-chain record

storing VDR is controversial
    it is storing hashed data on the blockchain

? Can the auditor cheat
    people can keep them accountable by comparing it against the vdr

in most cases the auditor will be the court

AS: confidential intelligence

? Is the compliance policy also on chain
Yes, compliance policy can be in natural language but with no room for interpretation
? Give a scenario where this would not be money laundering
any use case where cash is used, now put that onchain
confidential information being put into AI
the mixing process protects again prompt attack (second case is not compliance policy)

Concern by presenter is that VDR leaks information
? What is the VDR leaking
at least the location they are located at
? who do you want to protect, the person giving or receiving
giving
comment: should cover all the compliance policies available
? entities like Russia could dirty up the contribution list

need to figure out how many people are needed to make the system actually private
? how many users is this
an open question

another use case is threats and harms
you want to be able to share potential harms to the general public but not be found out that you shared certain information

? is there a tradeoff between number of people in AS and trust vs privacy
AS could have compliance policy themselves
VDR may not care about certain attributes within the AS

VDR could store the scoring information about counter-party
calculate the score of a wallet based on transactions including valid VDR
core of system: social accumulation of compliance score
giving economic intelligence for conducting due diligence
accountable economy vs existing economy
difference in incentives

? Are association sets in the diagram separate from each other
yes, different AS has different compliance policies

privacy concerns will get much more complicated because of PII disclosure

? If you ask people to follow PII disclosure then are you not defeating the purpose of paying in cash

moved away from embedding offchain information

? why can you already not make crypto transactions like you do in cash offline
you can send but then people would not want to receive

in traditional finance systems like this are done through complex builds of control
comment: privacy of the recipient
not private to court

? vdr needs to be signed right
yes there is signing for it

Slides:
https://drive.google.com/file/d/1b2ryv7GRNAn0DZoMHjJSANjKYLBscsKN/view?usp=sharing

SESSION #10

OpenID4VC "server-to-server' mode

Session Convener: Kristina, Joseph, Paul, Lee Christian, +
Session Notes Taker(s):

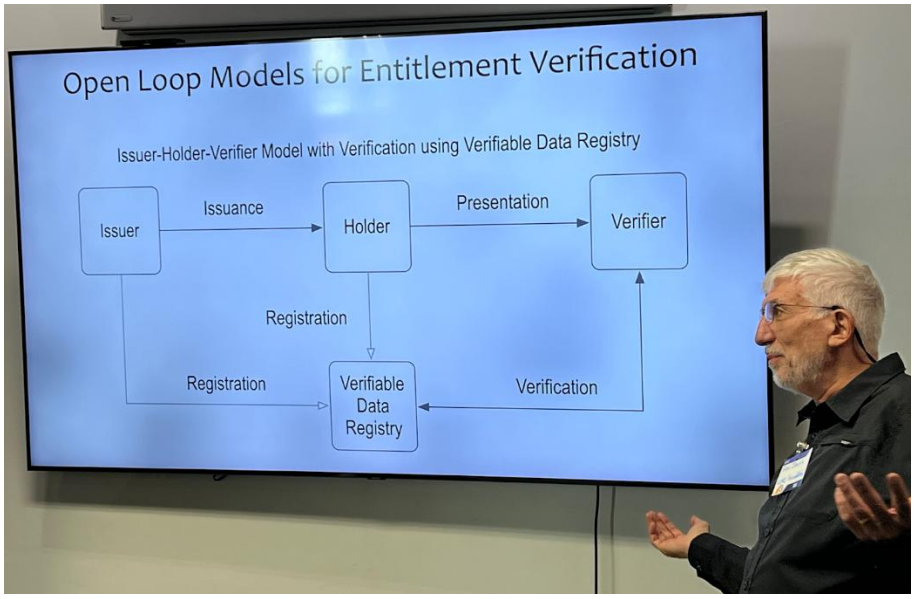
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

NO NOTES SUBMITTED

ACDC Blindable State TELs

Session Convener: Sam Smith
Session Notes Taker(s): Kent Bull

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



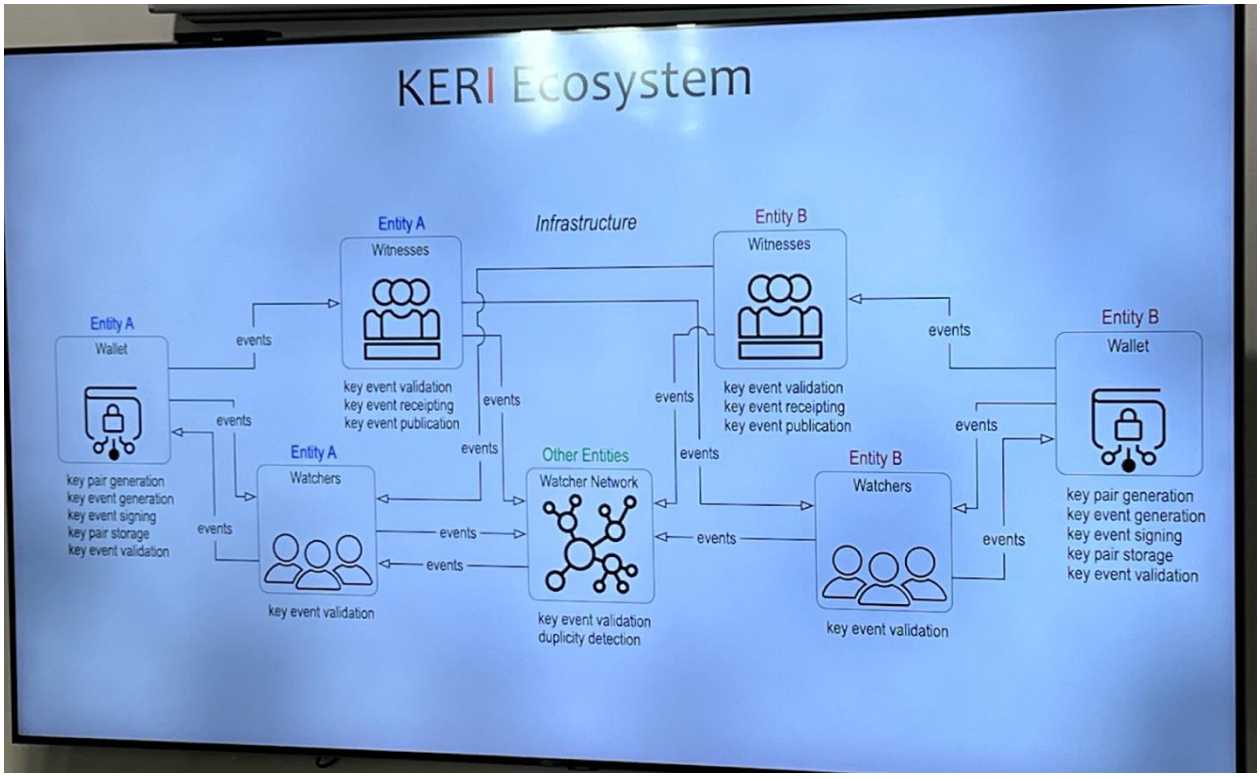
Breaking the correlating link between verifier and issuer during a specific ACDC verification using a blindable state TEL.

ZKPs defeat detectability of key compromise. We want to have detectability so that recovery is possible.

ACDC State Registry using Transaction Event Log (TEL)

- Each Transaction Event is bound to the issuer's key state via an anchoring seal in the issuer's KEL
- Example: Driver License
    - want to be able to dynamically revoke a driver license rather than have it expire on a given date.
- Watchers watch KELs
- Observers watch TELs (registry TELs and ACDC TELs)
- Registrar is a service that publishes TELs (Registry TELs, ACDC TELs)
- Witness publishes KELs
- Publisher is controlled by the issuer, Consumer is controlled by the verifier

In KERI we say promulgators of information control their own nodes, governance of publication and observation nodes can be different meaning this data can properly be portable and fully decentralized.



All of these five boxes would be one blockchain. Blockchains centralize governance. Promulgation and confirmation are centralized. Then it is total ordered against what everyone else publishes.

Blockchain does not allow you to recover. Losing keys is catastrophic. You lose your money or your data.

If I can choose magic crypto x yet “magic crypto x” does not allow detectability or recoverability then I will always choose not to use “magic crypto x” because I want detectability and recoverability. KERI gives you detectability and recoverability.

What we’re trying to do is balance several different objectives and we are deciding fraud is the worst problem in the ecosystem and that everything else is secondary.

How do we not have forced correlation?
Separating observers from registrars allows at point of verification (PoV) technical protection from unwanted correlation. Beyond the verifier’s observer, regulatory and legal mechanisms must be employed to disincentivize verifiers from selling data to data aggregators, preventing further unwanted correlation.

Fraud = impersonation fraud or identity theft.

What you want is a bulk update mechanism so you have herd privacy.

New thing: Presentation Registries.

Holders have a presentation and they sign that presentation so the verifier knows they signed that presentation at the time of presentation. What if the presenter’s keys are compromised? How does the presenter protect themselves?

They use the same TEL registry mechanism. Instead of an issuance registry the holder uses a presentation registry. So, if an impostor compromises their keys and prematurely adds a presentation to the presentation registry then the true controller can detect that their keys have been compromised since the true holder has their own local copy of their presentation registry that would have at least one less event when compared to the attacker’s/impostor’s registry.

Question from the audience: Why issue and not holder?
Answer: it is a terminology difference between W3C and ACDC.

Blinded State Registry

Sparse Merkle Tree predicate proof is an alternative to a ZKP Circuit (ZKP Predicate Proof)

- store the values in the leaves, not in the branches or the root.

How do I do this?

- if I have a ZKP I don’t need a lot of storage, I just need a relatively large computation, defeats detectability of issuer key compromise
- For sparse merkle tree (SMT) I have relatively large storage yet a relatively small computation, enables detectability of issuer key compromise
- Example: age check with a current date inclusion proof. This takes about 1MB of space. Store a predicate for all possible current dates.

Alternative traffic stop authentication safer for the officer

Session Convener: Francisco Corella
Session Notes Taker(s): Francisco Corella

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

A driver's license credential usable for website registration and traffic stops

An alternative driver's license presentation method

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

I called this session in response to feedback I received in Day 1 / Session 2 / Room L when I presented a demonstration of a driver's license credential usable for website registration and traffic stops. In a traffic stop, the QR code that the officer presents to the driver includes a challenge and must therefore be dynamic. Philip Quinlan pointed out that a dynamic QR code would be displayed on a small screen, and the driver would have to come close to it to scan it, which would be unsafe for the officer. In this session we discussed an alternative presentation method that uses a challenge for proof of possession, but where the challenge is not in the QR code. The QR code can thus be a large preprinted image that can be scanned by the driver from a safe distance.

MyTerms Practical Experience

Session Convener: Iain Henderson
Session Notes Taker(s): Kari McMullen etc.

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

customercommons.org

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

Iain Henderson presented a more technical version of the MyTerms deployment.

He shared examples online of cookie banners and privacy policies that come up when people go to web sites. He then brought up practical MyTerms deployment options, demonstrating a spectrum from the lowest level of Customer Commons involvement where the standard is published and let be by the non-profit.

The opposite end of the spectrum is a single MyTerms specific mobile app and deploy it globally.

The Customer Commons team believes the reality lies somewhere in between, but is calling for help to ensure it is a planned deployment that does not toss the approved standard (Jan 2026) onto the floor for anyone to pickup.

The demonstration by JLINC of a protocol then commenced by Ben of JLINC

Ben discussed different layers including one with a cryptographic signature, one with a notary signature, and so on.

He demonstrated the person signing with a cryptographic sig option.

First he logged into the JLINC portal.

You see a list of Available Agreements. In theory, the 13 agreements listed could be used. There is a raw text based version as well.

A hash of the content is referencing a URL in JSON LD.

Scan a QR code to sign. It has a select box to allow two of the agreements.

Real demo, does work. The agreement was in standard JSON format, included where to submit the agreement to. It was in machine readable terms, taking the place of what you have to click a checkbox for today, as well as machine readable bullets for what the company is allowed to do.

The machine readable standard is not defined in the standard.

The options for how technically is not in the standard.

Technical implementation has to be black and white

Going to be tough to spec out the consequences in each contract.

Opportunities for deployment include

- Brave Browser
- Linux Foundation for a rapid start up – set up a task force and work in an open and

If bitcoin had an identity layer 2.0

Session Convener: Nivas Sivaprakasam
Session Notes Taker(s):

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

NO NOTES SUBMITTED

What are DIF Recommended DID Methods

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

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

SLIDES

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

Do It Yourself Agent Expert - Building an agent to talk to a Spec

Session Convener: Chris Phillips
Session Notes Taker(s): Chris P after report

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:

Light attendance which allowed for deeper conversations with Attendees' was had.
Each attendee had a very diverse use of AI ranging in off the shelf use of CLI interface, AI access via web UI / interfaces to prominent AI vendors, and out of the box clients for coding.

The intent of the session was to offer insight on techniques to amplify the value AI offered when performing a task. In this case it was around improving how to handle larger specification documents and 'talk' with them and interact with the concepts

Cross-border interoperability of VCs

Session Convener: Hideaki Furukawa
Session Notes Taker(s): Kosuke Koiwai

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

How to translate Japanese name to English - this year Japan gov started registering how to pronounce your name. Until middle of this year only Chinese characters were registered so no way to directly translate from Kanji to Hiragana

Even more problematic is converting foreigners names to Japanese phonetics, then converting that back to English
Korean mDL - also has written name in Korean

eID gateway service to access such as Korean, Japanese, UAE etc. some times just need to check authenticity of the credentials, not names but

Name is just an attribute of an identity. All types of names can be in a credential,
Facebook charges 500 dollars for verified accounts

Drivers licenses - what type of vechicles you can drive is different between countries. Treaty of international driving permits will hopefully solve

It is interesting how people sees IDs and trust them even if they have never seen them
COVID days - VC certificate - just showing QR code was accepted

Name Matching - address verification for fraud prevention - there are some places in land boarders there are cities with different names, there are roads across countries and called diflerently. How to tell if the address written in German and Danish are the same or not

Denmark has a governmental list of GPS coordinate with addresses.
US has master street name guide
US has overrapping jurisdictions
Japan has many address systems - land address, house address, postal address, house address not lead to street address
LEI also has problems of address
If a jurisdiction needs to read VC from another jurisdiction, they need to understand the underlying rules
If you take the date and store to another database, the data is no longer attached to credential.
EULSP one of the big use case was identity matching, citizen of one country and another country is the same or not, Germany, full name, place of birth, name of birth.
If you go to India you have to leave your passport to them for a month, so you need another passport.

Agent Identity Gateway

Session Convener: Teng Wu, Emu Iizuka
Session Notes Taker(s): Richard Esplin

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:

Teng and Emu wanted to both discuss agent identity, so combined the session.

Teng's proposal
—----------
Existing infrastructure isn't agent friendly. Since agents don't have their own identity, they have to shadow humans.

- Need to track the relationship between the agent and the human
- Need to track that the agent is accountable—agent reputation
- Then the gateway relays to the service whether it was a trusted agent or a human

Comment: The agent identity is often not important. Analogy to a car accident where the car's VIN is like the agent's identity, but you actually ask for the human's information. But what you really want is the insurance provider's identity.

Unified Identity: Human Identity + Agent Identity + Human Authorization

- Human identity can include both the "online identity" and the "real-world identity" (who will go to jail for the action)

Comment: is this similar to a notary who checks the responsible parties and issues an endorsement?
Yes, the gateway tracks who is the responsible party.

Gateway tracks the contract between the human and the agent in the authorization.

- Proof of humanity is an important attribute of the authorization check.

Comment: Might be proof of legal personhood–represents an organization

Comment: Requiring a proof of humanity prevents people from using their own agents which compromises their human rights

Comment: It isn't always true that the human is delegating restricted permissions to an AI Agent. In some cases, the agent might exist to enforce corporate policy and restrict the human's scope.

Emu's discussion
—----------

How does the resource server define the scope of authorization?

Comment: OAuth access tokens and capability certificates already exist and can be used for this use case.

Comment: Policy languages like CEDAR exist and would work well, but VC's and trust frameworks are a better model for cross-domain AI agent interactions then OAuth style non-human-identity (NHI).

Comment: Introducing a non-human readable policy language can make it harder to understand what an agent should be allowed to do. Something like "My Terms" face similar problems to be understood by a user. Too legal and it isn't understandable. But human readable icons aren't clear enough.

Comment: Organizations should consider that identity that originates from another identity domain may not be trustworthy. People share logins, organizations refuse to revoke, etc. It is important to consider in the risk profile that organizations.

Comments: AI agents may behave in unexpected ways, such as exploiting a vulernability to complete a task.

Might need to delegate authorizations among multiple AI Agents.

- Limit the number of hops of AI agents (levels of delegation)
- Limit the amount of money that can be spent

Comment: is this just scopes?
Yes
Comment: why would it be useful to limit the number of hops?
Comment: with people, it can be useful to say "you or a friend can pick up my prescription, but no one else
Comment: but this doesn't map well to AI Agents

Where does liability lie in AI agent interactions?
Comment: There is a contractual relationship between service providers that should define where liability lies. But your visibility may only be with the next hop.

Teng
—----
Authentication might be at the edge or with an IdP.
Comment: The same agent will respond differently to the same request.
Comment: That's why we don't trust the agent, we trust the credentials that the agent shares from their wallet.
Comment: Any actor can go rogue, whether a human or an AI Agent. They can opt for reputational bankruptcy.
Comment: How do you prevent an agent from sharing its wallet key with another agent?
Comment: Definitely a problem that we need to work on.

Comment: Reputation and accountability are equivalent.

Accountability needs to consider the agent and the human behind the agent.

Comment: How can you prevent an agent from sharing its private key?
You have a wallet that does not allow the private key to be exported, and the agent can only interact via MCP. It doesn't solve everything.

Hologram Messaging Verifiable Chatbots P2P + Ai

Session Convener: Fabrice Rochette
Session Notes Taker(s): Ariel Gentile

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

Presentation available at https://gamma.app/docs/Hologram-Verifiable-AI-Decentralized-Identity-6id4p8o57sh75bq?mode=doc

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

Hologram app is the first "self sovereign" messaging app, intended to connect users with businesses and other users in a verifiable and privacy preserving way.

It uses technologies well known in the community, such as DIDs, Verifiable Credentials and DIDComm.

In the session we demonstrated different open source components developed by 2060.io (see GitHub page https://github.com/2060-io) to create feature-rich Verifiable Services that can exchange text, images, videos, request machine travel document data and even coordinate video calls to for example perform biometric verification. All running in a self-hosted manner, no need to third-party services.

Links to Gov ID Issuer demo: https://github.com/2060-io/hologram-gov-id-issuer-vs

And Generic Verifier app: https://github.com/2060-io/hologram-generic-verifier-vs (demo deployment QR code at https://dm.gov-id-issuer.demos.dev.2060.io/qr)

The End of the Global Internet

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

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

https://sphericalcowconsulting.com/2025/10/07/the-end-of-the-global-internet/
https://sphericalcowconsulting.com/2025/10/14/tech-supply-chains/
https://sphericalcowconsulting.com/2025/10/21/demographics/
https://ericscouten.dev/2025/iiw41/#session-10n-the-end-of-the-global-internet

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

Assumptions on how the internet should apply is not applicable anymore
- due to national sovereignty, sanctions
- Does AI affect this?
  - Data centers in america (in the 4000s)
  - how many data centers in africa (100s)
  - very skewed

There are many mitigating factors to preserve the global internet as we know it
For instance, we need computers across the world and we need a bunch of players around the world
- geology

you have to work with other companies in other countries
- e.g. company in netherlands

demographic
- demographic of people in the world
  - western and japan: old
  - nigeria's avg age: 18
- what happens when population goes old
  - south korea
  - birth rate replacement of .6
  - do not have time to innovate in sectors besides sectors that they need emergently

what are african kids growing up with (what sort of values)
- tribal
- do they think of privacy, community, consensus the same way?
  - they kind of do not
  - what will the internet look like next

trust frameworks in countries across the world are not the same
- interoperability between these regions are extremely difficult
- mutually exclusive requirements
- even in the united states, states are for and against big tech
- eu dislikes big tech, so much work in digital identity being put in

this is where the posts are up to now until this week
in 15 years in time, people in the room will not share the same values as now
    how are we going to adapt to this
    need time to prepare
    you cannot have a baby in 1 month with 9 women
this is not a bad change but it is a change -> what do we do?

? is there enough pressure for certain things to stay global, the economic drive for things to work
    speaker thinks no because for instance in 65% of payment systems in India are india only
        comment: it was like this in poland and japan like this until recently also
    comment: similar thing was the case for routing also
? we have an evolved system that is the result of circumstances, is your thesis "we do not understand circumstances"

    we will be like britain
    things broken up (though they still exist)
comment: global order by the united states, current trade wars are not sustainable
    will go into period of extreme nationalism but at least in the US economy is so dependent on immigration
    other countries will also not be able to sustain anti-globalism similar to the us
situation in the us have broken various assumption in businesses nowadays
without efficiency what is there to aim for?
    efficiency is not an achievable goal in the long term as a business

? how long will you not have to declare data as an import from a foreign country
    probably not for long
    safe harbor act

comment: "global standards body" is it really true that these bodies are diverse, how much of what we developed is truly a global consensus, there are countries and regions out there that are working to create a similar global concept based on their own ideals
    global standards vs world series
"open standards" what is the consensus on what an open standard organization is
    ISO: not that easy to participate in, have to buy standards
    claim to be an extremely global standardization organization but people from "minor" countries do not effectively participate
NSA couple months ago had a standards meeting
    brought in 200 experts, "China is eating our lunch because they are funded and organized, can you guys do something about that?"
comment: why not educate the NGO sector, they should send the engineer to actually useful government projects and not governance conferences
international data summit(?): did not care about digital identity, countries that sponsored the most were those that were trying to buy reputation
    gap that is left in the change in us global policy

comment: many mentions of “do not be influenced” in a trust framework (standard?)
political ideology based on age
african romance frauds
    revenge for colonialism towards the UK, trying to shift capital back to africa
the international realm is interested in attacking the us
    russia, china, nk, iran, nigeria
    drug cartel -> cyber crime cartels that are set up which operates on efficiency
        tens of thousand people from such countries
        cannot be dealt with a small task force
comment: we as a society needs to curtail internet traffic from international places
comment: numbers of these cyber cartels went down but the size went up
    you do not actually know where the traffic comes from
comment: there are forces counteracting these crimes
    e.g. IETF: bunch of hippies, self-healing
        this however does not scale
the internet society tracks where the internet keeps being turned off
    countries are controlling access to the internet
    concern is that you are getting to a point where you cannot combat this
need to learn about the culture of places that are going to grow
    there is a bunch of work that there needs to be done for these post-colonial regimes to be broken down towards the direction of globalization
the internet was never global
    internet itself has never been a single network -> this is an illusion
    efficiency and resiliency do not get along very well
    e.g. bureaucracy is meant to be resilience not efficient
china runs a different internet than other countries do
    there are trends that are acting against the globalization that we are building right now
tradeoff between resilience and efficiency

(Second note taker)
The internet is breaking apart!

National standards bodies are creeping into grounds that were once part of the global standards space. Demanding that standards begin meeting their needs.

Premise: if you think about the internet today, it’s built on shared protocols.

It’s built on shared assumptions.

Governance - a lot of open governance forums.

Especially early on, innovation was happening way faster than regulation

Some of the shared assumptions no longer apply:

1. National Security
2. Digital Sovereignty - trade wars, sanctions, data centers weirdly distributed, power and control
3. Media feeding a certain amount of distrust in any global solution

Mitigating factors:

1. Tech based society needs computers - the stuff you need is not equitably distributed due to geographical differences. The skills you need. → too many interdependencies
2. Demographics – african average age is in 20s while US/UK is 40+. Populations are aging and centers of innovation will shift

Centers of innovation are shifting to places with different value systems around things like privacy, consensus, etc. The future nature of the internet will align to different value systems.

Trust Framework in Europe is not the same as TF in China, Africa, India. And these policy stacks are not interoperable with one another. Mutually exclusive requirements for buying software.

What does this mean for standards development?

- People getting older, not a strong pipeline
- Focus on process
- Different value systems

Is there enough pressure for certain things to stay global? Where economics drive necessity to work. E.g. payments

- No. It's happening in payments
- Alternate DNS

Routing was never neutral; never has been, never will be.

We have an evolved system that evolved based on circumstances and it's going to keep evolving. Are you saying we don't understand the circumstances?

We're seeing the dissolution of the post-ww2 global order. Assumption of a unipolar world will how it will always be. Natural evolution of standards world is going to become more parochial. Some of these dynamics are going to have to change/are not sustainable.

US situation has undermined a lot of the underlying assumptions that businesses and governments have operated with.

Resiliency over efficiency

How long before we have to declare imported data? Eg data that crosses borders.
Max Schrems talks about safe harbor rules and why they are terrible and unachievable

What is a “global standard” anyway when there is so little representation from e.g., Africa etc. The lack of truly global representation means you could argue that this is not an appropriate term – was it EVER a global internet?

Heather called back to her post reviewing what “open” really means in standards (is it the availability, the FREE, etc.)

I missed Kaliya’s question

Gov’t insists China is “eating our lunch” because they’re organized and funding… but unwilling to engage and put finger on the scale of what’s happening in standards and cybersecurity.

FBI - be careful about your HSM but we can’t tell you which ones not to buy.

NGO universe is being organized via ITU, WSIS, IGF – but do WSIS and IGF actually govern anything? How do we get this sector more involved in practice on the ground

WSIS didn’t engage with Digital Identity as a topic

Countries sponsoring the most were trying to buy reputation. They are trying to influence emerging countries.

African Union Interoperability framework is all about resisting undue influence.

Revenge shifting of capital to global south reportedly underpins a lot of cybercrime

A lot of countries have political reasons to attack the United States → this takes the shape of cybercrime cartels. Fully funded, institutional. States themselves cannot take out these cartels. Society may have to consider curtailing some web traffic from nations that are attacking us.

When the Russia-Ukraine war started, attacks from Russia declined, although the size went up. It went down because many of the contractors were from Ukraine.

There are forces counteracting some of these trends. IETF is a bunch of hippies practicing internet voodoo. I don’t mind where the work is happening

What do you mean by the end of the global internet? Companies don’t deal with global regulatory frameworks

USPS - packages still arrive, though they travel through different systems

ISOC tracks where the internet keeps getting turned off. It’s going up.

Is it worth fighting for?

Need to learn more about the cultures where the innovation is going to happen

West african countries have so much to give that we aren't getting today in our global conversations today. Post-colonial regimes

We need to realize that the internet was never really global. Internet is switched off, routing, data centers. It was never built with certain geographies and people in mind so fighting for it depends on accepting this and finding ways to ensure that the next phase of evolution really does work for them. Find better ways of working together

The internet itself has never been a single network – it's a collection of lots of little island.

AWS outage shouldn't take out the global internet. This amount of consolidation

When the wrong cable gets cut, even one country is splintered. the backup cable shouldn't be next to it: efficiency DNE resiliency

Biological comparison – we see efficiency and resiliency tensions all over nature. Bananas.

Notes Day 3 / Thursday October 23 / Sessions 11 - 15

SESSION #11

MALNETS: Understanding malware networks

Session Convener: Jacob Siebach
Session Notes Taker(s): Jacob Siebach

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 simplest example of a malware network is a single, central malware server (malserver) that delivers a malicious payload to a target (usually a person using a browser). There are several "redirect servers" that, when reached, will redirect the browser to the malserver. Many compromised, legitimate domains send the user to the redirect servers. In this way, the unsuspecting user is (through various means) led to a legitimate domain, but sent through the malnet until they hit the payload.

We discussed various attack vectors that malicious actors utilize, discussed the trade-offs of security vs. privacy with using phone vs. web apps for companies, and offered suggestions on possible future research in the field.

And I sang the opening line of "Hello, my Baby". ;)

OIDF AI Identity Management Community Group Call

Session Convener:
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

Storytelling - The Art of the "Lie" Utah's Biggest Liar

Session Convener: George McEwan
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

How should we do SEDI

Session Convener: Alan Fuller
Session Notes Taker(s): Kent Bull

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

Utah SEDI bill SB0260 - https://le.utah.gov/~2025/bills/static/SB0260.html

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

Policy discussion on how to pull off SEDI properly.

Where will SEDI be issued? Default is public safety, driver license division. It might be in the department of government operations to start. It doesn't belong there, though it might start there.

Comment from Judith: There is governance and then there are procedures. Policies need to be created to fill the missing gap when often procedures are thought of as policy. Procedures are how I am implementing the policy.

Comment from Phil W.: We often talk about things that are SEDI. A driver license is not SEDI, it is just one example of a certificate that will be represented in SEDI. There are things like addresses that are transient that I would like the state to endorse. Yet a birth certificate is not transient. The state would endorse that also.

…many comments from the audience…

Jeremy Firster: We have digitization and digitalization. What documents are we speaking of? Driver license is only one document. We have to make sure what you digitally does not replace what you can do physically. Anything digitally you can do physically.

Alan Fuller: I agree, that is in the (SEDI) bill, to support the physical.

Topic: adoption

Regarding our mDL program, what we are 5 years into, has some failures. We only have 4% of the population, can't use it anywhere, and the verifiers we had initially are going away. We're stuck in a bespoke app on a phone. Their business model is to charge holders of the credential and verifiers of the credential. They are trying to charge verifiers too much so no businesses jumped on board to pay to license verification software.

Comment from Kent Bull: could the verifier software be open source?

…many comments on the topic…

Sam Curren: the verifier policy needs to not be a weapon. Open source and free market takes care of the problem of ineffective or bad verifiers.

Mats-Joonas Kulla from Estonia: on adoption, how do you get businesses to accept digital identity? How do you make people want to have digital identity?

Judith Fleenor: on adoption you need parallel tracks of attention for verifiers and businesses

Alan F.: One of the challenges here is for online credentials. Online market is massive and they are not based in Utah. Gaming, social media, adult media, and so forth. And it becomes more complicated with guardianship.

Alan F: A couple of key take-aways–

- Need to have parallel strategies for adoption, one path for verifiers and one path for credential holders
- Need to focus on procedure of the deployment, as well as policy, governance, and technology
- Need to think about what information to put in the state SEDI credential. Should address be there? Or should it be a separate license?
- Focus on serving the needs of the people more than serving the needs of the state government itself.
- Don't get locked in to a single technology stack. Maintain flexibility where possible.

Future of Work meets Identity and Data Portability

Session Convener: Brad Topliff
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

Perspectives from the United States: From Refugee Registration to Self-Sovereign Identity

Session Convener: Besem Obenson
Session Notes Taker(s): Eric Scouten

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:

Besem working for UN for 18 years mostly in the Americas. UN has lost significant funding in 2025. How to prioritize services for displaced populations? Displaced = refugees, displaced migrants, internally-displaced, etc.

100MM+ people are forcibly displaced, including refugees, stateless people, asylum seekers, IDPs, and victims of human trafficking.

Many lack access to legally-backed identity, which means they may lose access to protection, justice, food, health care, and freedom of movement.

UNHCR manages 25MM+ records for verification, but system is not built for user control. Data misuse can endanger lives or expose people to further exploitation.

What does trust mean when the state or traffickers may both pose threats?

Besem has spoken with thousands of displaced people and also traffickers to understand what identity could look like for them.

How do you restore identity when you don't have a toehold of identity? Quite possible they are young enough that they don't know their own names, birthplace, birthdate (even country of birth), parents, etc.

The Decentralized Promise

- SSI = user-owned, portable, cryptographically verifiable
- Promises privacy, interop, and consent
- Assumes digital literacy, connectivity, and safety *(big assumptions)*
- Risk of exclusion for undocumented or exploited populations

Can SSI frameworks include those who lack legal status, documentation, or digital safety?

What information can even be shared amongst UN agencies? UN agencies have a lot of power to assign and/or determine identity and thus decide what services are available.

Many people (e.g. refugees) lack legal status in the country where they are physically located. Some countries (Venezuela, Nicaragua) make it very difficult to obtain documentation.

Where the Models Clash (and Converge)

- Humanitarian ID | Decentralized ID
- Centralized trust (UN/NGO/government) | Distributed trust (blockchain, verifiable credentials)
- Identity as protection and verification | Identity as autonomy and self-determination
- Limited user consent | Explicit user consent
- High operational control | High individual responsibility

Where is the ethical middle ground between protection, autonomy, and safety from exploitation?

Open Questions and Next Steps

1. What ethical principles could guide inclusive decentralized identity that protects refugees, asylum seekers, and victims of trafficking?
2. Could humanitarian registries issue or verify decentralized credentials without risk?
3. How can we prevent exclusion, misuse, or harm from digital proof systems?
4. What collaboration might emerge from IIW to test these ideas?

Goal: Identify 2-3 actionable principles or prototype ideas to explore post-IIW.

Discussion

What is the access to technology among displaced persons? Many adults have access to phones. Refugee welcome centers often offer fast charging and free wi-fi. This is helpful in regaining access to medical, educational history, etc.

Participants examined whether humanitarian registries could issue or verify decentralized credentials without compromising data protection or neutrality. The group discussed the risk of digital exclusion, misuse, and harm, especially for refugees and trafficking survivors-the notion of those folks who want to be “deindentified” to save their lives. Proposals included sandbox testing with NGOs, data minimization protocols, and layered consent systems. Collaboration ideas centered on pilots linking IIW technologists with humanitarian agencies to co-design verifiable credential models.

Anonymous Credentials / ZKP - Overview & how do we get things into deployment?

Session Convener: Christian, Leif
Session Notes Taker(s): Christian

Tags / links to resources / technology discussed, related to this session:
https://docs.google.com/presentation/d/1DU70hAcb7OgTIAtMOHAwKfgzpEnk33QraPvm2R1rovs/edit?usp=sharing

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

Human Alignment in Agent to Agent Authorization

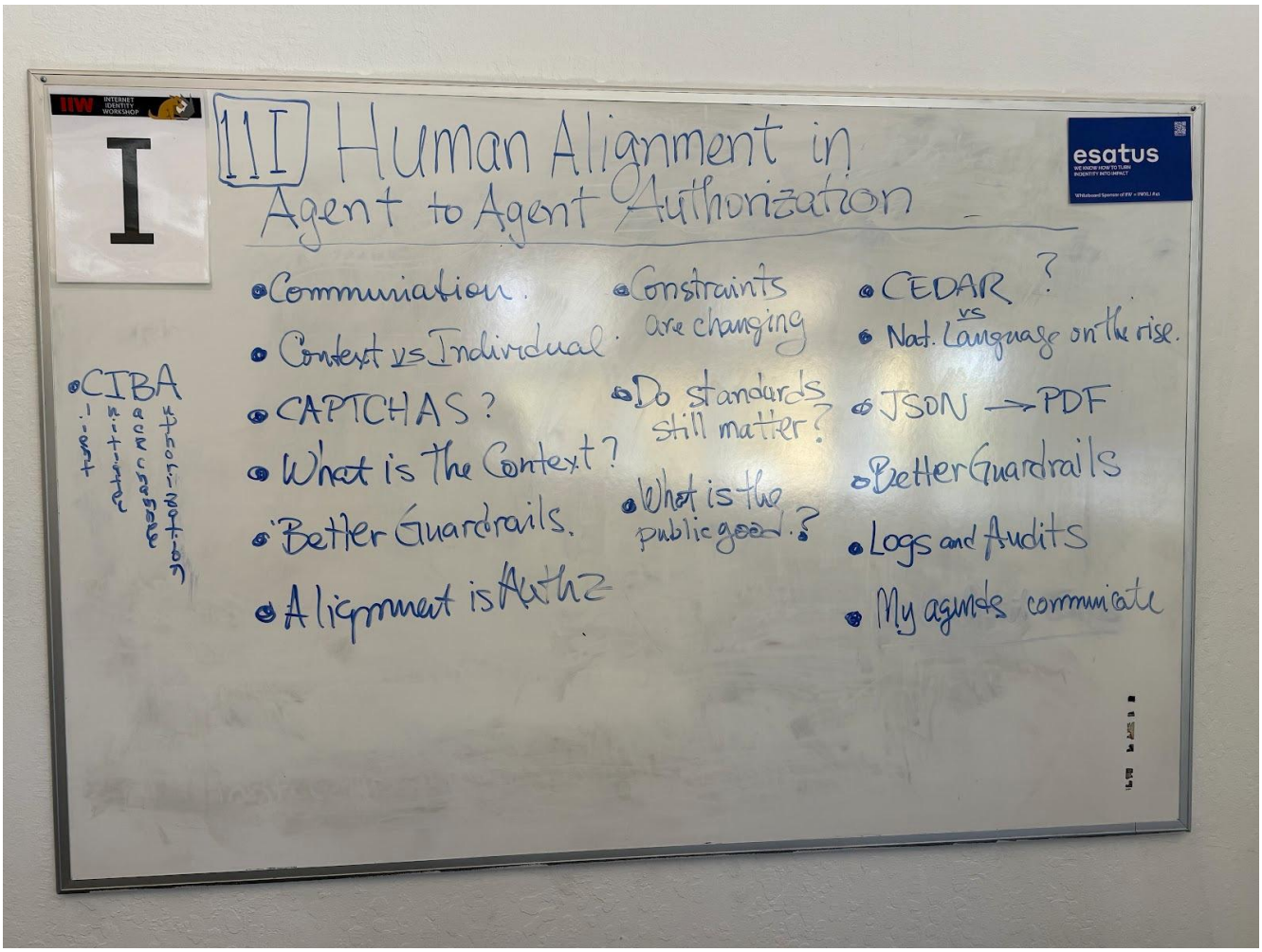
Session Convener: Adrian Gropper
Session Notes Taker(s): Adrian Gropper

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

IIW41_S2C_My Private AI Agent as an Authorisation Server

Demo Hour Table #13
https://www.google.com/url?q=https://docs.google.com/document/d/1PVS-VTpJLwKIwmzj5DxQZnyBPQ78pPXW4d5dhRxDSTM/edit?usp%3Dsharing&sa=D&source=editors&ust=1761180858559909&usg=AOvVaw0g8Ku035rkxUNqWWwYDhnT

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



KERI Auth Browser Extension demo/discussion

Session Convener: Ed Eykholt
Session Notes Taker(s): Ed Eykholt

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

slides https://drive.google.com/file/d/14itDZ9nhx6LexbXxVv0Wc5kra5vZO9Aj/view?usp=sharing

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

Ed presented and discussed the beta version of KERI Auth browser extension for desktop chromium browsers, for organizational workflows using vLEI credentials.

Notarized Verifiable Relationship Credentials (VRC)

Session Convener: Brendan Miller
Session Notes Taker(s): Alberto Leon

Tags / links to resources / technology discussed, related to this session:
Presentation:https://docs.google.com/presentation/d/1RvumrfCiEYZ2Sm6EzYkl40MQKXOA_1g5KfOH3ealgPM/edit?usp=sharing

DTGWG: https://lf-toip.atlassian.net/wiki/spaces/HOME/pages/257785857/Decentralized+Trust+Graph+Working+Group

First Person Project White Paper: https://www.firstperson.network/white-paper

Draft specifications produced based on the input from this session can be found here:
https://github.com/trustoverip/dtgwg-cred-tf/commit/95ecb368a73ec8e466d46820e8d04690b6f61102

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

Summary:
The session discussed the concept of verifiable relationship credentials (VRCs) and the potential benefits of notarization in building trust and preventing fake accounts. Brendan and Alberto from Harvard's Applied Social Media Lab proposed using notaries to endorse VRCs, enhancing trust in social media and other contexts. The process involves session creation, mutual issuance of VRCs, and notary endorsement. Concerns about decentralization, corporate use cases, and the need for trust community credentials were raised. The discussion also touched on the technical and legal

implications of notarization, including the need for asynchronous flows and compliance with regional regulations.

Brendan used the term to describe how this did not use a biometric device as the “anti-Orb”.

The point was made that the notary can be a person or a community agent.

A question came up about timing. Must it happen live, or can the process extend over time, such as over a day.

Notaries could check a credential from the trust community.

There was a good discussion of the different interpretations of what is a “notary”. In the U.S., the notary is responsible for verifying the IDs of the parties being notarized. The same applies to VRC notaries because they are verifying the signatures on the VRCs, thus proving that Alice and Bob both control the keys for their pairwise private DIDs.

Phil Long noted that they should be able to “bail out” of the process.

Brendan proposed that there is a session setup that takes place with the notary. That will include the session duration limit.

Brendan then walked through the protocol flow.

A point was made that the notary is also notarizing the datestamp. This essentially is a decentralized timestamp authority capability.
One of the key topics discussed is how the notary “seal” gets applied. The options were a wrapper, a separate credential, or a linked credential. There was rapid consensus that a linked credential would be the best option; it is the most flexible and privacy-preserving.

A bunch of good questions came up about how a trust community would establish policies for notaries within their community.

Jon Bauer explained that he’s built an actual notary service for document signing. We discussed some of the requirements for that kind of notary that would not apply.

There was a consensus from the terminology that “witnessed” might be a better term. However we may need to qualify that with a term like “fair witness”.

We then discussed whether there is a need to reflect the trust community in the credential. The answer was no: that can be proved via ZKP when needed, but it does not need to be in the VRC itself.

However it could be reflected in the witness credential.

We closed by talking about how the entire fair witness process could happen remotely, without the two parties to the VRCs meeting in person. It was agreed that the whole protocol could work remotely, however remote witnesses may be subject to the fair witness policies of the relevant trust community. An example are events, where the trust community is the event itself, and only event attendees in person can be witnessed.

Drummond noted that all of this fair witness protocol is the work of the ToIP / DIF Decentralized Trust Graph Working Group. All attendees are invited to join that work — both free and paid membership options are available.

Drummond also said that this fair witness protocol should be reflected in the next version (V1.2) of the First Person Project white paper (currently at V1.1).

Alberto's AI Notes & Transcripts

AI Summary
The session discussed the concept of verifiable relationship credentials (VRCs) and the potential benefits of notarization in building trust and preventing fake accounts. Brendan and Alberto from Harvard's Applied Social Media Lab proposed using notaries to endorse VRCs, enhancing trust in social media and other contexts. The process involves session creation, mutual issuance of VRCs, and notary endorsement. Concerns about decentralization, corporate use cases, and the need for trust community credentials were raised. The discussion also touched on the technical and legal implications of notarization, including the need for asynchronous flows and compliance with regional regulations.

AI Action Items

- [ ] Explore the concept of a "fair witness" or "trusted witness" rather than using the term "notary."
- [ ] Investigate how the witness can verify identities and credentials of the parties involved, potentially requiring a trust community credential.
- [ ] Determine if a "wrapper" or cryptographic linking of the two VRCs is needed, or if simply having the witness reference both VRCs is sufficient.
- [ ] Discuss the implications of remote vs. in-person scenarios and the different levels of assurance required.
- [ ] Consider how the witness service could be implemented, including potential integration with existing notary/verification services.

Recording
https://otter.ai/u/MhcF_gTxsTKOFxM6J-EhU1sVJPo?utm_source=copy_url

Transcripts
IIW ASML session 3_otter_ai (1).pdf

Raw Notes:

Topic: Verifiable Relationship Credentials (VRCs) and the concept of notarization / witnessing in digital trust flows

Participants:

- Brendan Miller (Harvard ASML)
- Alberto Leon (Harvard ASML)
- Drummond Reed (First Person Project)
- Darrell O'Donnell
- Fabrice
- John
- Luke
- Dimitri
- DOC Searls
- Rob Aaron

1. Context & Motivation

- All participants were already familiar with **Verifiable Relationship Credentials (VRCs)**.
- The session focused on **adding notarization**—a "witness" or "third-party validation layer"—to VRC exchanges.
- Problem: **Fake accounts, sybil attacks, and false relationships** are major threats in decentralized social ecosystems.
- Goal: Introduce a **"notarized" or "witnessed" VRC flow** that can increase trust in peer-to-peer credential exchanges.

2. Key Concepts & Insights

Digital Sovereignty (Drummond Reed)

- In a Web3 world, the concept of *accounts* disappears, people connect via wallets, not logins.
- The First Person Project (FPP) white paper already hints at notarization as a social-trust layer.
- Having relationships "notarized" could prove authenticity in ecosystems that are otherwise peer-to-peer and pseudonymous.

The Role of the Notary (Darrell O'Donnell)

- Decentralization doesn't mean *removing all middlemen*; some intermediaries add value as validators.
- A notary could play that role , *not as a central authority but as a trust-anchoring participant*.
- Corporate example: the U.S. Chamber of Commerce could notarize employee–employer relationships.

Trust Communities

- Every VRC exchange occurs within a trust community (e.g., IIW attendees, organizations, friend groups).
- A notary could be an agent acting on behalf of that community, verifying the integrity of exchanges.
- The notary's signature would represent the community's endorsement of a relationship.

Other Notes:

- Timestamping is valuable to prevent forgery (Fabrice).
- The notary may check that both parties control their DIDs and hold a trust-community credential.
- Notaries could be human or automated agents.
- Each VRC remains directional, but notarization provides the assurance of mutual acknowledgment.

3. Terminology Debate

- **"Notary" vs "Witness":**
    - In the U.S. and EU, the term *notary* has legal connotations and differing obligations.
    - The group leaned toward using "Witness" or "Fair Witness" (Doc Searls, Drummond, Philip).
    - "Fair witness" evokes *validation without judgment*, aligning with decentralization principles.

4. Governance & Discovery

- Notaries (or witnesses) should have verifiable DIDs and credentials issued by the trust community.
- Discovery could happen via well-known endpoints or within a community registry.
- Governance may vary: some communities might require physical presence, others allow remote notarization.
- A *"Notary Profile"* credential could include authorization proofs and policies.

5. Remote vs In-Person Witnessing

- In-person notarization: simplest case (proximity, shared Wi-Fi/Bluetooth network).

- Remote notarization: requires liveness checks or integration with third-party IDV/KYC services (John).
- Example: use of DIDComm links for secure, pairwise, remote session exchange (Alberto mentioned Bifold link sharing).

- A community might require remote witnesses to have higher assurance or extra credentials.

6. Additional Points

- Personas: Each VRC connects pseudonymous DIDs. Personas can be linked optionally for context (e.g., work, social).
- Proof-of-Relationship ZKPs: Long-term goal, prove that a valid VRC exists without revealing its content.
- Business Models: Trust communities (or states) could charge fees for notarization or certification.
- Terminology Evolution:
    - "Notarized VRC" → "Witnessed VRC"
    - "Notary Service" → "Trust Community Witness"

7. Open Questions

- How to distinguish multiple communities when a person belongs to several?
- How to handle asynchronous notarization flows (e.g., delayed witness confirmations)?
- How to prevent collusion between two parties generating fake relationships?
- Should witness credentials be publicly discoverable or limited to specific verifiers?
- What's the minimal metadata needed in the linking credential?

Phone Home - An Update

Session Convener: Timothy Ruff, Joe Andrieu, Steve McCown
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 #12

SEDI Guardian Demo, Roblox + Social Book

Session Convener: Veridian
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

WTF is a "client_id"?

Session Convener: Justin Richer
Session Notes Taker(s): Andrew Todd

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:

Notes on WTF is a Client ID?

- In original OAuth it was all about two websites talking about each other, servers didn't need to be identified but clients did. Consumer key = Client Id

- Why did we need an ID for a client?
Oauth flows often start with a redirect and we can't pass secure credentials via front channel
Need to associate a request with a client, and need to look up "trusted" values like redirect URI.

OAuth/OIDC is not all about redirect flows
- Mobile apps forced the introduction of "public clients" and we need to base our trust on other things like redirect uri, etc

All kinds of clients today that don't fit the original OAuth models
- ephemeral workloads that get assigned a temporary identifier and then goes away

- mobile clients where the client is a class of software instead of a specific instance of the software
- multi-tenancy web hosts with multiple different users
- in summary client id doesn't have a cohesive meaning anymore, if it ever did

What categories of clients exist today in your use cases?

Question for the room: Are there any cases where we don't need client ids and we can still have secure conversations?
Submitted draft to IETF for using PAR to push a key and potentially client ids are not needed.

Audience Member: With PAR since there has already been a back-channel communication we can already identify where the request is coming from and client id doesn't add anything.

Client ID vs MTLS - client id identifies the class of a software, mTLS identifies a specific instance / workload

Things Client ID can represent:
- instance
- class
- version
- on-behalf-of (multiple client ids for a single class / instance to represent multiple "tenants")
- function
- device (IoT?)

Types of Clients	# instances	durable	# users / instance	ecosystem
SPA	many	no	one	closed
Web	one	yes	many	closed
Native	many	yes	one	closed
agent	many	no	many	open
dist. web	many	yes?	many	closed
browser	many	no	one	open
tenant	one	yes	one	open

^ maybe the agent use case isn't right
^ durable here means whether the client id is persistently used across multiple "sessions" or usages.
^ ecosystem meaning: for a given client, when its shipped, would I know what website this would call out to

For things where the lifecycle of a "thing" is ephemeral and involves dynamic client registration, then you end up with a lot of client "litter".

Patterns for handling client registration
- Client hosted metadata
- Identity Federation
- Use the Spiffe / WIMSE ID to dynamically register a client and map that to a class of caller
- Use PAR to skip client authentication in general
- Dynamic Client registration via client call
- Manual client registration

Discussion of a distributed web use-case, we have a multi-tenant running on multiple machines. They share a bootstrapped state including refresh and access tokens, and would all attempt to retrieve a new access token all at the same time and cause a thundering herd and only one would keep a valid refresh token. Solved by making refresh tokens returned idempotent for a period of time

Lots of discussion about additional types of clients and where they fall in the chart and what they're similar to.

For some IoT devices there is a client identifier that maps to the model / version of the device and an instance identifier that's dynamically fetched (maybe based on user authentication?)

Client ID -> Class of thing
Public Key -> individual instance of a thing

Discussion: It's very common for many instances and use-cases to be shoved into a single client identifier because of the cost and difficulty of creating new client ids, which is often manual and even involve having to be physically present somewhere in some high-assurance environments.

Question to Justin: Since we've discussed how client id is not very valuable, what does that mean for the current client id metadata draft?
- Client Ids has been previously been free text fields and there will be problems and incompatibilities with back-patching that to now be a URL
- Should we require a new claim and/or allow the client id to be a URL

Joke: How do we fix it all: Spiffe?

Title: FeDIDeration: DIDs in OpenID Federation

Session Convener: Lukasz Jaromin (Raidiam) & Fraser Edwards (cheqd)
Session Notes Taker(s): Fraser Edwards (cheqd)

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

https://docs.google.com/presentation/d/1j7FmezQ2spcHKlx8fdEGxF4t7TUXWEwKSt6dFg3XtUY/edit?usp=drivesdk

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

Discussion was mainly focused on whether this is a recognised problem , i.e. whether there is a need to blend OIDF and DIDs and if so, why?

Dmitry (MIT) has actually implemented this already so this is a known problem with some work towards a solution.

Two main challenges remain:

- Getting this appropriately adopted as a spec despite some pushback
- Finding immediate use-cases / business cases for a pilot or MVP

Next steps:

1. Firstly identify a group of the willing to build a pilot or MVP
2. Establish some architecture documents and such which can be leant on
3. Once we have these ideally being them into either LSPs or for clients with proven demand

You've got the wrong use case

Session Convener: Alan Karp
Session Notes Taker(s): Alan Karp / Joe Andrieu

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

https://alanhkarp.com/UseCases.pdf

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

The core idea is that the delegation use cases most of us in identity are using to build systems are oversimplified. Alan's paper & presentation walk through the innate challenges in actually common, non-simple delegation scenarios.

In the jurisdictional case, it was noted that in addition to the risk of Alice's identity needing to be managed in the new jurisdiction, users might just share access credentials which presents the distinct identity, but it also means Alice's actions are indistinguishable from Bob's. That's a problem of its own, arguably worse that the identity exposure.

Transitive Access--root cause of Target breach that cost them $500 million.

In capability systems, the exposures are significantly restricted. An unforgable, transferable permission to use the thing it designates.

Hot tip: use capabilities to revoke, making it possible to delegate revocation.

Q: Are you talking about identity access management generally?
A: Yes.

Q: in Higher ed, we have tons of problems. And a long running history of dealing with all of these kinds of use cases with complicated different parties and systems. We use traditional IAM mechanisms. At scale, 40,000 turn over every year. Those traditional mechanisms can handle it. But what I'm hearing feels like it can't work at that scale.

A: Likely that's because you have signed contracts that agree to treat multiple entities together (which is complicated). One professor complained to me he is using resources from 15 different orgs, and every semester he had to onboard all of his students to all 15 different systems. Capabilities actually made it simpler, as he can just revoke his delegations and delegate to next class (all without interacting with the 15 different orgs).

We have a paper, ABAC to ZBAC that touches on the complexities in this use case. If two organizations federate identities (bilaterally), how does the other party know that a person in this first party is legitimate. That identity is meaningless outside the context of the company. So why do you need that identity in the other system, since the remediation is to the company anyway.

Because there is no way for the second system to go after the party in the first (because they don't have the relationship).

SOMETIMES, the second party *does* need the identity, in which case it is necessary to connect the second party to the identity system.

There is still a significant space in traditional IAM that won't go away.

A; Using the IAM to log in, define roles. But use capabilities for access. That gives you the benefits of both systems (roles and capabilities).

So how do you transition?

Q: I built a system with URL-based access capabilities (deeplink). I wanted to make this more sophisticated. What would I do? I don't have an identity system. So, it's an open system. What is the next thing I can do?

A: What's the use case?

Q… : Out of band, I put a deeplink into the portal, than whoever has access to URL, has access. Is there anything more that I can do.

A: Yes. Certificates. Because then you add metadata.

You also need the browser to be aware that the capability needs to be signed.

A browser plugin could potentially intermediate to sign HTTP requests.

URLS do have length limitations (in practice), so in UCAN they provide a URL to the certificate rather than just embed the cert in the URL.

UCAN features that zCap doesn't have. zCaps are using DIDs. Not sure why (don't like, AKarp).

But they do have wildcard delegation in UCAN (which I like (AKarp)).

per-Credential Metadata (by the issuer…)

Session Convener: Paul, Gareth, Leev, Kristina, etc
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

Domains of Identity - 16 Subdivisions of Use Cases… walking through them + considering developing intersections between domains.

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

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

Link to a summary of the Domains
https://www.identitywoman.net/wp-content/uploads/Domains-of-Identity-Highlights.pdf

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

Here is a link to the slides that I shared in Taiwan at the Verifiable Credentials Workshop
https://drive.google.com/file/d/1Cw-7lz1NJ4tfFxfQs84c0n0X2ZmX0g-P/view?usp=drive_link

What Identity can learn from Home Assistant and home automation.

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

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

homeassistant.com

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

Home Assistant is an open source project that functions as a home automation hub, and bridges and adapts to any protocol and device type. Now, a user can interact with, configure, and automate any home automation device without consideration for the actual connection protocol of the individual devices. Zigbee, ZWave, and Wifi devices all work alongside each other seamlessly.

Identity has a problem now where users have Wallets (equated to a device like a Hue Hub) and all of the wallets don't work with each other. An architectural parallel to Home Assistant would be a 'meta' wallet that integrates with all of the existing wallets a person has, but with a simplified interface that allows the user to focus on WHAT they want to do, without being mired in the details of HOW it'll work.

Privacy In A Surveillance World

Session Convener: Steve McCown
Session Notes Taker(s): Steve McCown

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

Here are the presentation slides that we discussed in the session:

Privacy In A Surveillance World

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

See above…

SESSION #13

Working Session - How to add VC, VP and maybe mDL to CAWG identity

Session Convener: Eric Scouten and Andrew Dworschak
Session Notes Taker(s): Eric Scouten

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

https://ericscouten.dev/2025/iiw41/#session-13a-working-session-on-cawg-integration-with-w3c-vcs-vps-and-maybe-mdl

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

Speed run through CAWG identity assertion data model

I did a speed run through the data model for CAWG's identity assertion. See only slides starting with "Identity assertion in the C2PA data model" and ending with "Identity assertion / CBOR-DIAG example."

Detailed discussion: Andrew's proposals for broader VC, VP, and mDL integration

These notes are available in the following locations:

- Notion *(up to date with discussion from various CAWG members)*
- PDF snapshot

In Andrew's diagrams:

- Blue boxes are VCs.
- Yellow boxes are VPs that contain VCs.
- Green boxes are C2PA Manifests.

KERI's Strategy for Post-Quantum Security

Session Convener: Samuel Smith
Session Notes Taker(s): Kent Bull

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

Presentation slides link:
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KeriStrategyPostQuantumSecurity.pdf

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

The reason why CESR is used is to make it easy for the programmer to do the right thing. CESR was designed with full cryptographic agility in mind.

Retroactive Universal Basic Income

Session Convener: Navis
Session Notes Taker(s): Charles Kirby

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

Adding the deck would be really helpful. We started by agreeing that UBI was Fair (we recognized that nothing is fair but we went with it as a fair conceit.

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

RUBI is based on two key principals: 1B jobs are about to vanish through the art of A.I. and that $12T disappears when money sits stagnant. Navis is suggesting a joystick controller (I suggested it be gold plated with the letter T on it) in order to move the money around and occupy the billions of people out of work.

Navim presented some salient slides about the math. I won't presume to understand or summarize but I can share that I jumped out of my chair and began to draw on the whiteboard. We cut the projector.

My ideas began to flow and we had a wonderful 30 minute chat. We surmised that the crux of the process of how much money people should get should be decided by the people playing the sim.

The biggest decision we tackled was: How often does the cohort receive an additional tranche of RUBIs? I posited the following:

X and Y axis of the decision would be voted on by the humans who were in the middle of the bell curve as represented to fight INFLATION (X axis) vs DEFLATION (Y). The Demurrage Effect is one of Navis' biggest fears. This could mitigate this effect but what about the Billionaires and Unhoused??? They could be thought of as the outside edges of the bell curve. Assuming fairness is a common goal among every human…

We arrived on the possibility that the Z axis could be TIME (cadence of regularity of payouts) as decided by the outliers. So the amount of increase/round of payment is voted on by the mainstream users and the frequency is weighted by the anomalies.

Getting Started on MY TERMS Deployment - Who wants to help? Starting work groups TODAY!

Session Convener: Doc and Joyce Searls w/Kari McMullen
Session Notes Taker(s): Kari McMullen

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

Kari put in charts with notes from the whiteboard inserted after each chart presented. White board photo and QR code to get involved follow in charts as well.

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

This was referenced in the fundraising discussion:
https://www.macfound.org/press/press-releases/humanity-ai-commits-500-million-to-build-a-people-centered-future-for-ai

Credential Usage Policy

Session Convener: Paul, Tobias, Kristina
Session Notes Taker(s):

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

NO NOTES SUBMITTED

Tools For Traps - Managing Identity and Intention on Our Terms

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:

Tools For Traps / Managing Identity and Intention On Our Terms

When we are connected to the digital landscape we are observed in some form(s) and fashion(s). It is fair to say that we have an identity of some sort applied to us. This identity is what could be thought of as a session identity. From the moment the device touches the connected realm, aspects of that device define that machine in those moments of connection. The device's own hardware, hardware drivers, software installations, the data associated with the account you logged in with, ip addresses, LAN MAC addresses, WiFi MAC,…create a specific session related to a specific device entity which is often operated by a person. An identity related to many things forms each time.

How can these spaces be occupied in a way that avoids system profiling funnels and the herding and nudging created by those forces? When we look at screens to operate on the other side of the glass, controlling intention while managing the degree of identity we wish to express, and how that is expressed, is a lot to think about. On the digital landscape that seems wildly complex to have to track, yet we do that all the time as we move through our lives in the Real World (RW). Spidey Senses work better here than there.

A simple mouse trap illustrates a want conveniently placed. As that want, let's call it bait, a signal releases potential energy and the hit is made…or not. With systems able to know what appeals to us and considering system designs built to move us, how can we avoid the allure of being baited. The tooling available is relative to the goal, the landscape related to that goal and the method(s) used while in pursuit of the goal.

Example: I want to hear a broadcast available which not only streams the show for internet connected devices, but also broadcasts on FM, AM or Shortwave radio, I have two very different

approaches to getting that feed with or without being scoped by a system. Can you guess which is more residue free? What is the data cost of the differing paths to make the goal of listening to a broadcast.

Let's talk about the web and journeying there. Just like driving a car, the web is very similar in the sense that a browser (Brave, Firefox, Edge Safari, Chrome) used to surf the web is same as the idea of a car travelling the roads. Let's apply that thought framework to the digital realm.

To the car analogy: If I want to travel (browse) the web without having stickers (cookies and trackers) put on my vehicle (browser) it would be cool to have a car that rejects stickers being put on it everywhere it goes. Some web browsers and add-ons are designed to help your web browser defend against your vehicle being stickered.

Not signing up for certain types of relationships like social media or purchasing is a tooling strategy. Choosing to sign up for relationships and adjusting the settings to match your preferences is a further example of engaging those system forces on your terms. Choosing not to sign up is another tooling choice for your larger relationship with IT systems which would be referred to as Your Real-IT in this space.

The cost of avoiding these systems and their forces may be being left out by community. In social media landscapes "The Tyranny of Convenience" (Tim Wu article) where the One-To-Many (one post to many eyes since it pops up in everyone's feed) allows for one to post news and info of their world, while missing the sense that those not in the space of that system will not see or hear of it except by second hand if at all.

Much more to say:

My Terms (IEEE 7012) terms granularity removes the default hook points favoring the house and that often are mandated in the All or None contracts of "take it or leave it".

Photographic Journalism: even framing a photo to not capture street signs helps defend against fraud; NorCal Fires 2017

NASA JPL Extraterrestrial Return Protocols related to concept of bringing other worldly things down to Earth; AI like bringing an alien back from space for people to lick or not so much…

_Rashmi Siravara: Tools to traps was one of the best sessions in play with real time experience of the concept.

The use of
Goals
Landscape
Tools Sets
Persona to identify and categorize traps was phenomenal.

Human Behaviour interplay with the OS was in reach of accuracy. Manifestation techniques co-related to the traps was touched upon to explore this topic further in IIW-42.

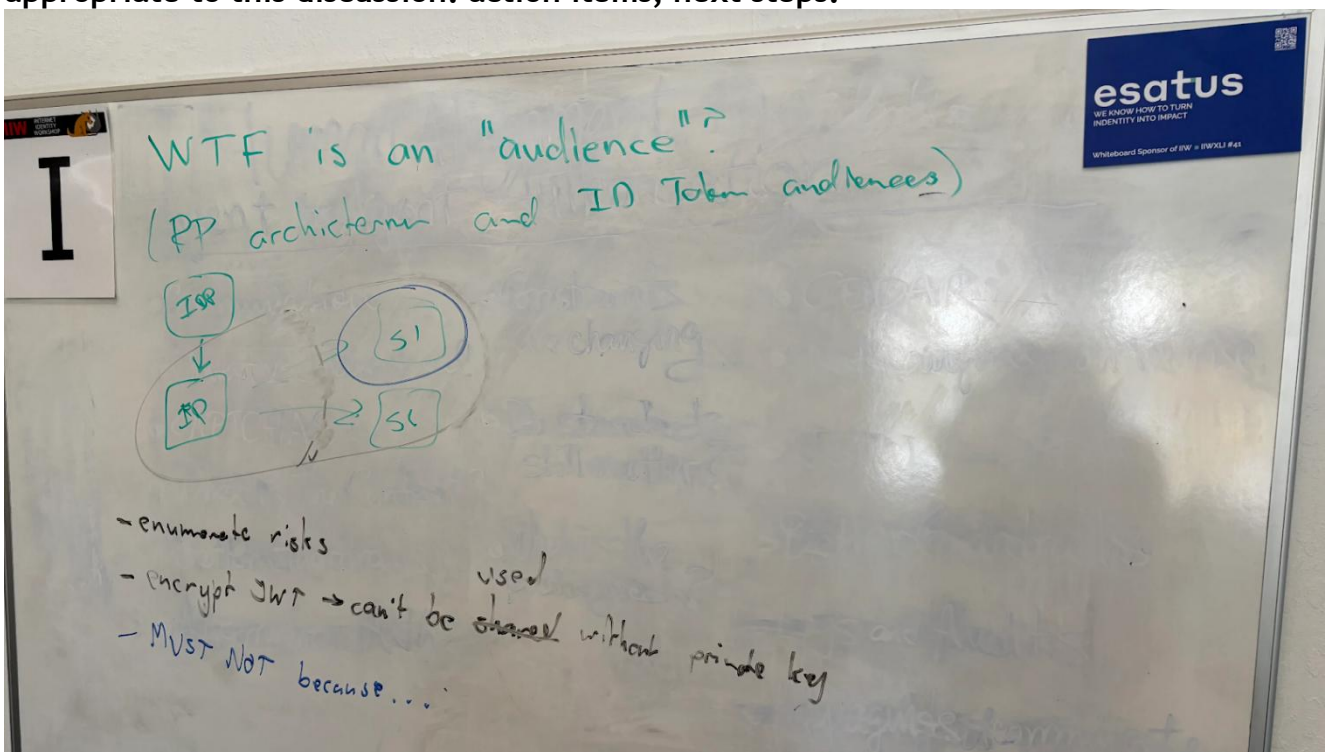
RP Architectures and ID Token Audiences

Session Convener: Frederik Krogsdal Jacobsen
Session Notes Taker(s): Frederik Krogsdal Jacobsen

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

OpenID Connect Key Binding:
https://openid.github.io/connect-key-binding/main.html

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



Discussion about when OpenID Connect Key Binding use cases were okay, from the perspective of the

One interesting option in case you really need to do this is to encrypt the ID Token JWT and only share the decryption key with trusted actors.

RPs are potentially putting the OPs user's at risk by sharing the ID token with other entities.

Conclusion: Key Binding spec should say that RPs MUST NOT send the ID token with the bound key to RPs outside their control, and enumerate the security and privacy risks of doing so to explain why.

Running an OpenID Federation

Session Convener: Nicole Roy, InCommon
Session Notes Taker(s): Chris Phillips

Tags / links to resources / technology discussed, related to this session:
https://openid.net/specs/openid-federation-1_0.html

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

This is an AI assisted summary, raw notes are below this.

Convened to explore **operational challenges in running a federation** there was an emphasis on balancing flexibility, automation, and governance.
Nicole shared a proposed a **managed operational model** that offers consistency but may impose certain constraints and wanted feedback and insight on possible approaches and their characteristics

---

Operational Models and Flexibility

- **OpenID Federation** was highlighted as allowing **intermediaries** to be independently created and configured.
    - *Example:* Frederico from **RNP (Brazil)** shared their model that supports creating as many intermediaries as needed, allowing scalability but introducing potential complexity.
- **Observation:** More **constrained models** are easier to manage and reduce operational overhead.
    - The group acknowledged the need for latitude to centralize certain operations without stifling autonomy. Nicole's outlook was to allow full autonomy for entities within the ecosystem to do what they want.

Operational Barriers and Signing Workflows

- A recurring theme was that **operational complexity is itself a barrier to participation**.
- Nicole described the **signing mechanics** in OpenID Federation:
    - Entities must pass validation before being signed.
    - Signed metadata is hosted at the entity's `.well-known` endpoint.
    - This introduces *real-time operational demands* but improves assurance.

- The concept of **Baseline Expectations** (akin to InCommon practices) was mentioned as a model for readiness and compliance.

Balancing Quality and Centralization

- The group discussed finding a **middle ground** between:
    - **High quality, centrally managed** operations.
    - **Flexible, distributed** self-service models.

- One model proposed using **long-term ACME-issued keys** for authentication and re-use, reducing re-validation costs.
- Another model offered/suggested a way to virtually host the .well-known endpoint for sites as a CNAME or proxied in order to have operational oversight on the mechanics but complete the tasks of handling them.
    - Dialogue was had that this creates a central point of failure or duty of care for a very high SLA of 4 9's or better otherwise trusted operations fails.

Metadata Management and Automation

- Dialogue evolved toward **centralized metadata signing and publication**:
    - Operators could delegate signing to a managed platform that publishes on their behalf.
- **Automatic registration** and **Dynamic Client Registration (DCR)** were recognized as one possible prerequisite for this automation.
- The idea of a **proxied `.well-known` endpoint** was raised—allowing a central host to serve validated metadata for participants.

Federation Onboarding and Access

- Joining the federation could involve:
    - Exchanging a **long-term key** to gain **administrative portal access** (bootstrap credential).
    - Using this credential to register and manage entities.

Trust Resolution and Policy Enforcement

- Operators expressed a need for a **"trust resolver in a box"** — a simple local service that can:
    - Evaluate trust metadata.

- Produce a **binary (Yes/No)** trust decision
- Conceptually similar to a **Policy Decision Point (PDP)** such as Sunet's go-trust project and/or authZen as an engine for this.

Key Rollover Practices

- Discussion compared **daily vs. infrequent** key rollovers:
  - Frequent rollovers enhance security but create fragility and operational overhead.
  - Infrequent rollovers become a **business continuity policy** decision.
- Consensus: this should evolve as a **community practice**, not an imposed rule.
  - The risk of non functional key-roll over capability in the field is concerning thus the more daily-esque model which would quickly reveal any improper behaviour very quickly.

Community Engagement and Fragility

- The conversation closed with a shared observation:
  - **Federations are fragile systems** — small operational missteps can break trust chains thus concentrating excellence with a knowledgeable team is a possible way to mitigate and manage reputationally risk both to the operator and utility of the protocol.
  - Strengthening **community engagement and shared operational practices** is essential for resilience.
  - There is a knowledge and skills gap in the field that is already felt and being felt more acutely with recent specifications being used but not necessarily practiced. No direct solutions were offered to address this problem which is not limited to this space but experienced in many places.

<raw>
Session created as a forum to discuss challenges in operating a federation.
Discussion about an operational model proposed by Nicole that has a managed outlook, but potentially constrained environment.

in OpenID Fed, having an intermediary to be created and configured to whatever they want. Frederico (Brasil RNP, R&E federation operator) shared the model where it's offered to create as many as needed.

Observation is that constrained is more easily managed to avoid operational costs. Observation that hubs are needed.

Other observations from the group were the challenges in operation being a barrier

Nicole shifted to the mechanics of signing operations for entities being added and thus added realtime which means passing validation processwise in realtime, signing of the entity and the entity places this in .wellknown.

- There's a process known as baseline expectations that organizations go through,

discussion of models that strike a balance between higher quality but central operations.
longterm acme issued key, than use that to authenticate and then allow re-using keys.

The dialogue then shifted to management approaches of having the metadata signed for them and then published for them.

Clarifying point, automatic registration which needs DCR as observed.

The notion of .well-known being proxied from a central host platform (like the one issued).

To get into the fed -

- long term key exchanged for my administrative access (bootstrap access to portal)

Desire for trust resolver in a box to resolve the trust and practice to process things.

As an operator there's a desire for a simple Y/N answer 'Do I trust this?'
conceptually similar to the policy decision point: https://github.com/sunet/go-trust

Dialogue on key rollover

- Doing every day vs infrequently → becomes a business continuity policy.

This becomes a community practice question

Dialogue on engagement in the community with regards.
Observation: It's too easy to break and there's fragility.
</raw>

The TXNS are coming from inside the house! How do we think about minting tokens for in-cluster transactions

Session Convener: Andrew Todd
Session Notes Taker(s): Chance Raine

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

Transaction tokens
service to service auth

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

What are TXN tokens
JWT with some extra fields

- Rctx - request context (ip, ua)
- Tctx - transaction context (relevant parms)
- Scope - permission
- Meant to last for one request (1min, 5min depending)

How do they work high level

- Request comes into API gateway
- Request sent to TTS (transaction token service)
  Transaction token returns a token w/some context added
- For instance, add a downstream id + value that can't be modified

How is this different from ZCAP

- Zcap used on the way in w/external users
- Txn token is more internal, used to guide what should happen within a system for a given request

Problem: what if we *aren't* coming in from the outside. For example, a cronjob, event listener, etc
If we have S1 -> S2 -> S3, we want the S2 -> S3 to have the original context of what S1 was trying to achieve to make an auth decision.

Are transaction tokens related to transactions in the rollback sense? No, not prescriptive - could be used for that though

For edge requests, we know that the API gateway would talk to TTS and then maybe each resource endpoint is effectively a separate scope. And the API gateway is somewhat responsible for asking for the scope based on the resource.

However, if the service is starting the call and it's responsible for determining it the scope, you potentially need to allow these services to ask for very broad permissions

‘

It’s *possible* to implement this with a token exchange at each node to be able to make the next hop, but creates a very slow system (if secure).

Devil’s advocate - do we even need txn tokens for s2s auth? Can we just use access tokens? Access tokens require more power than required & grant broad power, txn enforces what you are supposed to do

API gateway (or whichever system is requesting the transaction token) does effectively have some escalated privileges. The txn token really just allows/prevents downstream calls from happening based on that initiating action.

Concrete implementation? Not specified in RFC, AWS has implemented. Could be done in a sidecar, really depends on the use case and requirements

Does txn token allow specifying a specific resource? Yes, you can do this in the tctx, but it’s purposefully not spelled out since authz is implemented in so many ways and this is meant to be more generic.

Benefit vs Overhead? Might be too much overhead to justify the benefit. Requires formulating the scopes well and potentially a lot of frontloading to understand what is required for a given request. Alternatively, it’s a bit of using signals for downstream services to make decisions.

How do you prevent lazy people from just broadly allowing scopes downstream? Does require intervention…

RAR (rich authorization requests) can help with some of this. Basically if scopes were objects.

Breaks encapsulation, but maybe that’s good sometimes in cases where what’s going on in one domain does affect how something should be done in another domain.

One side effect is that you can include relevant information that you might want down the line.

Presenting CoralKM A user friendly protocol for decentralised Key Management and Recovery (Part II)

Session Convener: David Gildeh
Session Notes Taker(s): David Gildeh

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

Slides: CoralKM Protocol
Repo: https://github.com/CoralStackCom/CoralKM

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

- **Overview:**
  - CoralKM is a DIDComm protocol for wallet recovery. It is designed for everyday users to easily onboard and manage Guardian's without having to have any technical knowledge of how it works behind the scenes. It also has a
- **Protocol feedback:**
  - Had discussion on how this could be used to help refugees recover their identity with the UN. The UN could be a guardian, and users can register themselves using a mobile app at a local UN office in their home country or in the arriving country to get their refugee verified credential they can use to identify themselves and get access to services in the arriving country or other countries they later continue migrating too
  - With CoralKM, the user would have a way to recover their identity/credentials even if they lost everything (phone, papers etc.). The UN and other guardians would need a process to identify the user before releasing their recovery shards to a new device, which could be biometrics or other PII data about the user they can use to identify themselves on arrival to a new country
    - Potentially could add the identification setup for biometrics as part of the protocol, so the user submits biometric data and other PII data when setting up a new guardian.
  - Ideally countries would use SSI for birth certificates etc. so the user has a signed, verified credential proving their identity. However, today its carrying physical copies of their documents which can easily be lost or damaged and can easily be faked too
  - Richard Esplin shared a similar protocol design from Hyperledger that he said was very similar to CoralKM and could be developed further with this protocol: https://github.com/hyperledger/indy-hipe/blob/main/design/dkms/dkms-v4.md

- **Next Steps**:
  - Looking for more feedback and help. Please contact me (david@angelfish.app) if you want to work with me on fleshing out the protocol and getting the first version published

Session #14

What's your p(doom) and why?

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

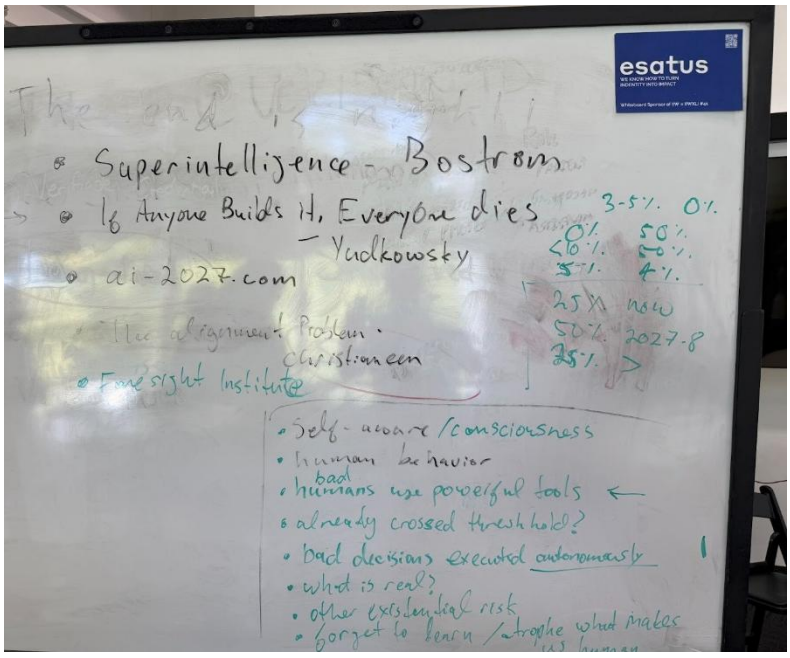
Tags / links to resources / technology discussed, related to this session:

References to relevant reading / materials:

- If Anyone Builds It, Everyone Dies - Eliezer Yudkowsky and Nate Soares
- Superintelligence - Nick Bostrom
- ai-2027.com
- Foresight Institute
- The Alignment Problem - Brian Christian

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

- P(Doom) estimates between 0% and 50%, averaging around 15-20%
- Consensus that AI is a frightfully powerful tool; debate on whether we even need to get to superintelligence for p(doom) to be unacceptably large due to bad human intent or over-reliance on AI-mediated autonomous action leading to disaster
- Inability to distinguish reality from fiction / fragmentation of "reality"
- Atrophe of what makes us distinctly human



Server-to-Server issuance

Session Convener: Hicham, Martijn, Gareth
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

KERI Suite (ACDC CESR SEDI) Ask me anything

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

W3C: Why? a research project's findings

Session Convener: Emily Lauber
Session Notes Taker(s): Emily Lauber

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

The thesis itself: https://dspace.mit.edu/handle/1721.1/162519

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

Emily provided an overview of the research project, best summarized with the abstract of the paper:

> This research investigates the motivational drivers for companies and individuals to participate in the World Wide Web Consortium's Web standards development process. Motivational drivers are identified through a literature review, primary sources, and interviews. Thirteen semi-structured interviews were conducted with questions related to participants' experience with the World Wide Web broadly, Web standards in general, the organization of W3C, and game modeling of the process. W3C was selected as the case study of Web-related standards bodies because of its unique model of paid membership yet open standards available royalty-free. The W3C standards process requires consensus-building, horizontal review, and proof of implementation before the organization officially recommends the specification. Existing research documents the history and value of standardization across industries, the modeling of various Standards Development Organizations (SDOs) in information industries, and the negotiation of international Internet governance. This thesis does not attempt to prove a societal benefit of Web standards but instead focuses on an individual's belief in societal benefit and how that belief drives their engagement with W3C. Initial findings point to members seeking economic, philosophic, and moral value through participation in Web standards development. A game theory framework evaluates the economic value of different players within the ecosystem and identifies that Web browser vendors and long-time consortium members have greater power for their preferred specification outcomes than Web developers or newcomers. Despite changes in the Web ecosystem in the past 30 years, W3C members continue to be drawn to the Web for the same philosophical intents that Sir Tim Berners-Lee designed the Web for. There are shared concerns though that the economic power players identified in the game modeling has damaged or will threaten the philosophy of an open, safe, accessible Web. Interviewees shared personal beliefs that there was a moral responsibility to engage in Web standards development and enable W3C's mission of "empowering humanity". Further research is required to catalogue more motivational drivers, evaluate drivers across other Web-related Standards Development Organizations, and rank the priority of motivations when the different drivers are in tension.

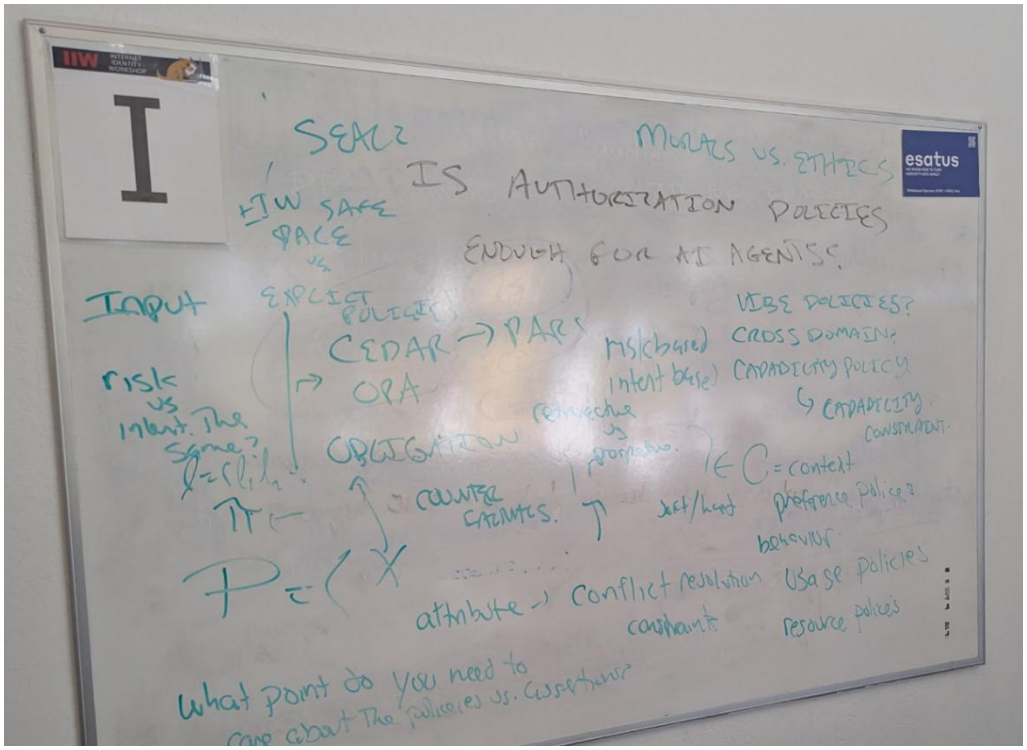
The discussion about the research wandered through a variety of topics.

- Game Theory
    - Browser vendors and long time players have more power than others.
    - examples given of where there is weight given to people's opinions based on their employers. At least until those individuals become long time contributors and their reputation precedes their employers'.
    - discussion of IETF's relationship between members and their companies. While companies don't pay for membership in IETF, the time and travel requirements to participate in IETF does create barriers for those without company support
- is W3C a standards development organization (SDO)?
    - some participants commented that W3C is more like a vendor market than a standards org. Aligns with the game theory argument that browser vendors have greater power than other players like web developers
    - Does not have the "authority" or regulatory power that other orgs like ISO have with government backings
    - checked websites and both IETF and W3C refer to themselves as Standards Development Organizations
- is the web a social good?
    - disagreement from the group about if/how the web could be proved as a social / public good. Social and public good used interchangeably in the conversation
    - the research project took the stance that regardless of proving it is a social good, that individual participants **believe** it is a social good and that is a moral driver for them
- the role of Sir Tim Berners-Lee
    - TBL acted as the backbone and technical direction driver of W3C. With him no longer leading the organization, there has been cultural and vision transformation in the org
    - People would vehemently disagree and be in a locked standstill in calls but when TBL was asked to make a decision, that decision would be respected because he was so respected
- standards "shopping"
    - W3C was split off from IETF and then WHATWG split off from W3C
    - there is some "standards shopping" that happens when people interested in developing a standard will "shop" around to different SDOs to get what they want from the standard and process
    - participants shared their own experiences, and often frustrations, with standards shopping and how it doesn't align with where they think the standard should actually be developed

Defining Policies for AI Agents - Is Auth Policies enough?!

Session Convener: Andor K
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:

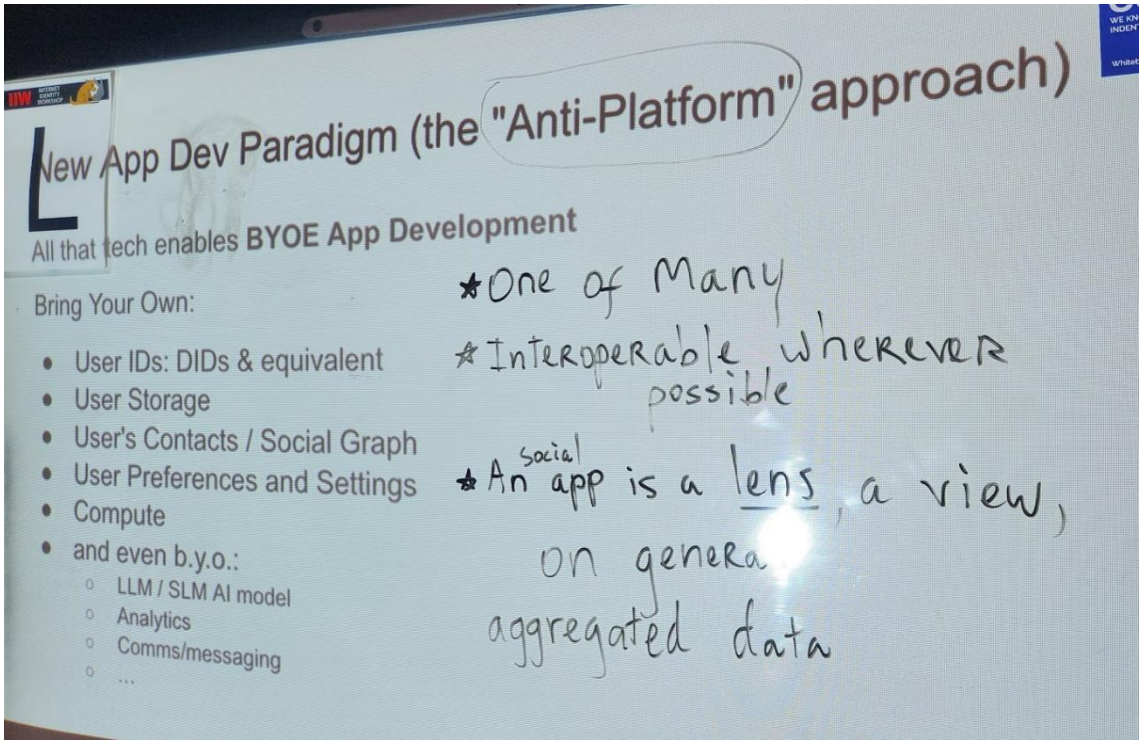
Basic understanding was that we are fundamentally aligning intent and security policies only exist to map / bound error in intent alignment.

Crowd-sourced App Design Session

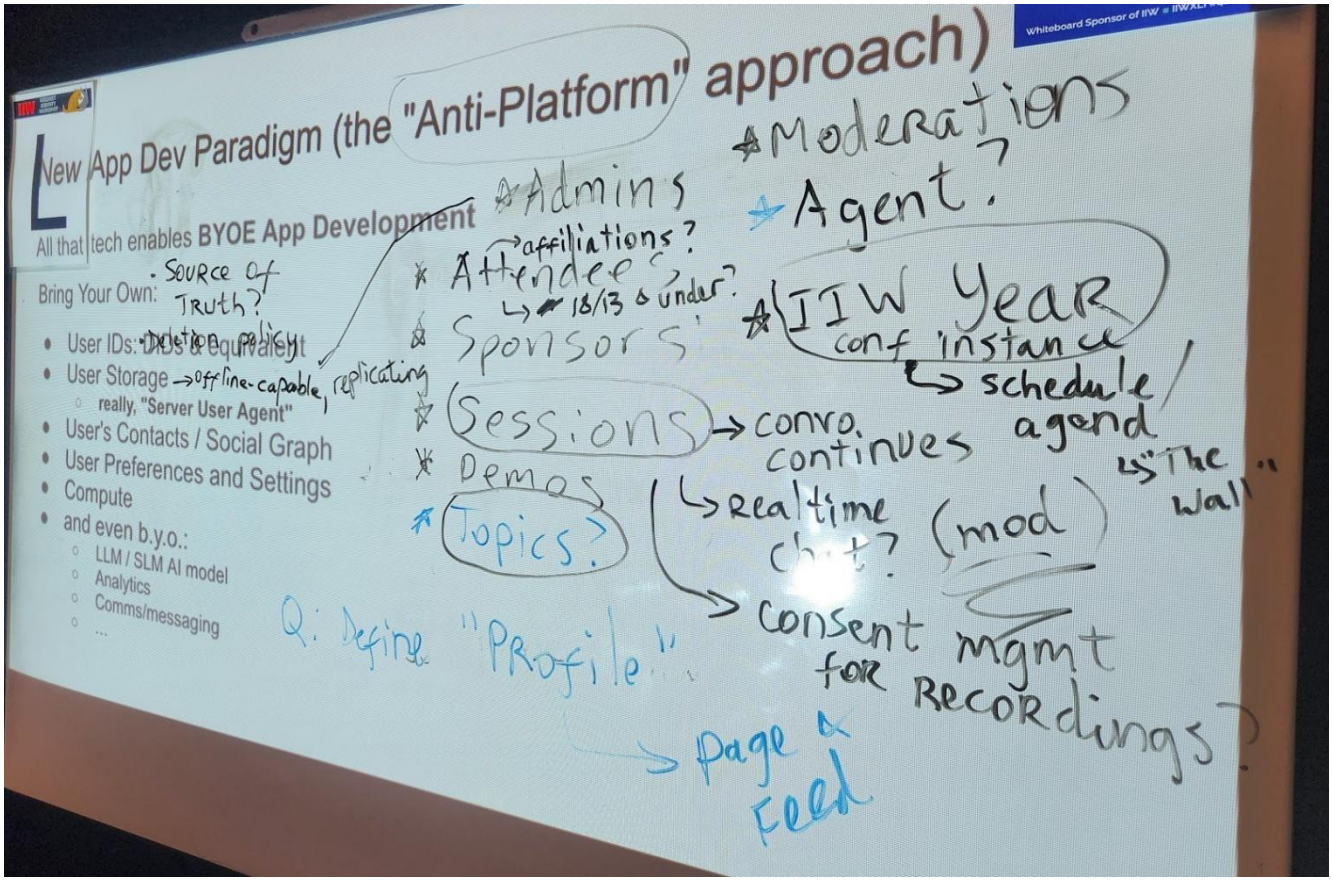
Session Convener: Dmitri, TyChi, Bengo
Session Notes Taker(s):

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

Slide: https://docs.google.com/presentation/d/1oe3zXvVZGVfyuURAI0ERX03QnlYAmrswR5mPVBjtAhc/

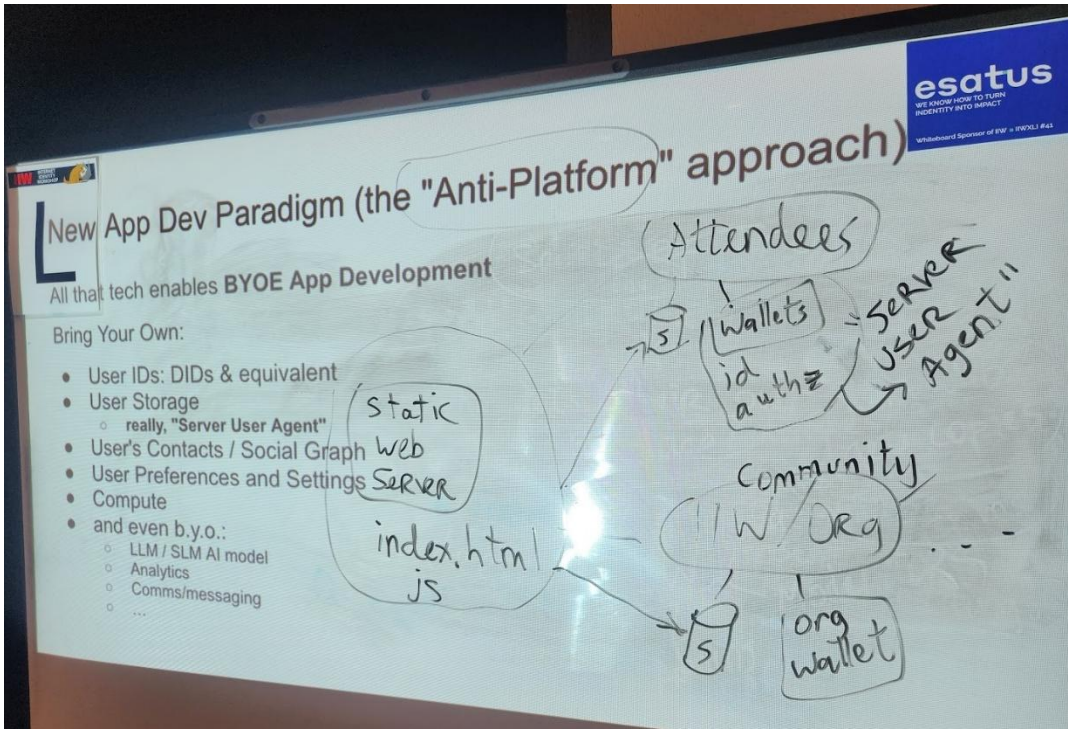


- A social App is a **lens**, a view on aggregated data.
    - View-first, Data-First app development
    - One of Many ("taco rules" instead of "highlander rules")
    - Interoperable / uses standards whenever possible



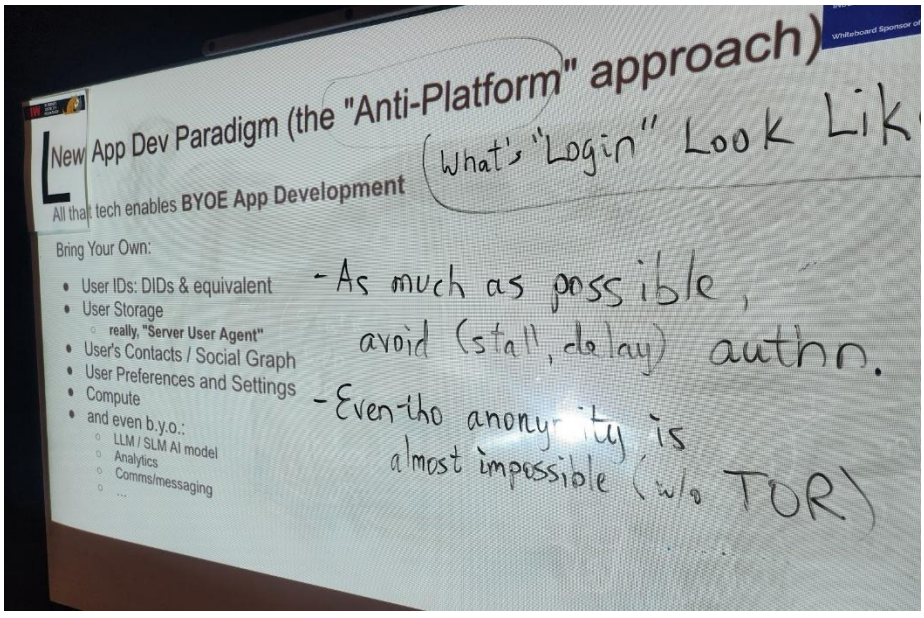
What are the "main" entities (that get their own "profiles" / pages / feeds)?

1. IIW Organization / Conference series
    a. nominates admins, moderators, etc
2. Each individual twice-a-year conference instance (ie IIW 41)
    a. schedule/agenda
    b. "the wall" of stickies
3. Attendees
    a. affiliations
    b. sponsors
    c. volunteers
    d. people's Agents
4. Admins / Mods
5. Sessions
    a. incl. Demo sessions
    b. a way for the conversation to continue after the session ends
6. Topics (a view on multiple sessions over multiple conferences)
    a. possibly also keywords?

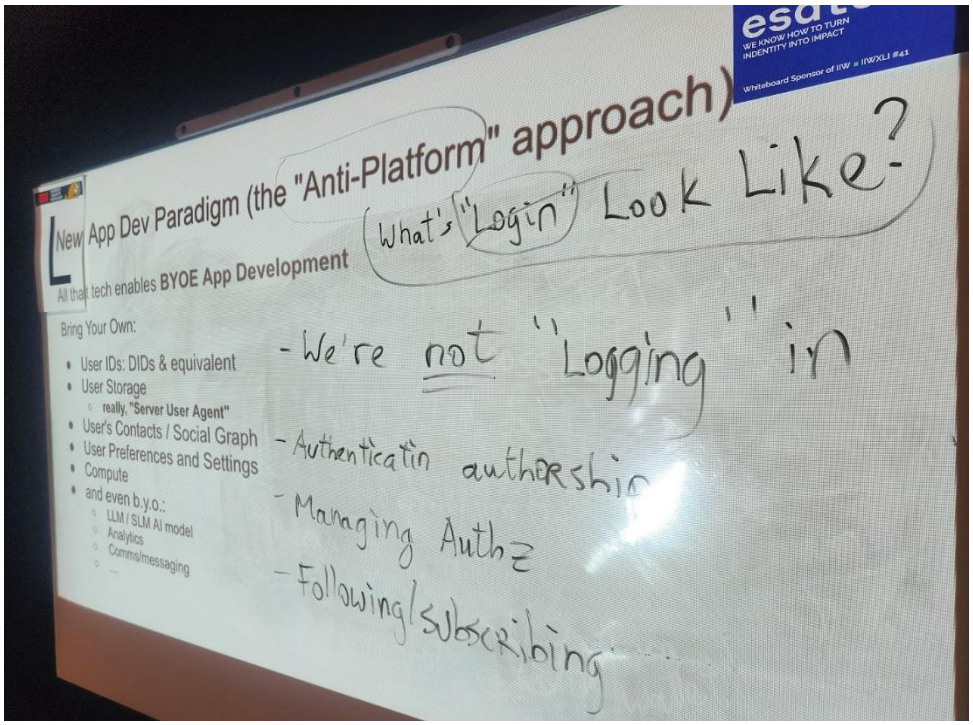


The "Technical" entities / actor diagram.

1. A Static Web Server (serving the app's index.html)
2. IIW Org
    a. brings its own storage instance
    b. brings its own Org wallet
3. Attendees
    a. bring their own storage
    b. bring their own wallets etc



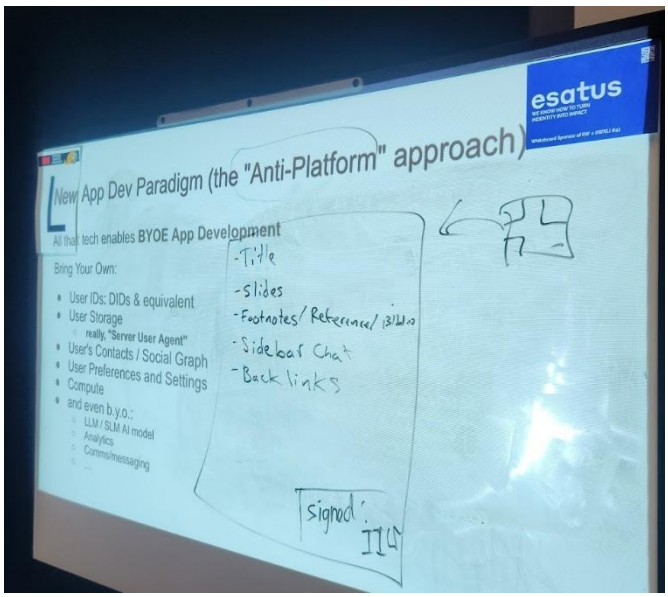
Important:
* As much as possible, *avoid* (as in stall, delay, etc) authentication
* Even though anonymity is almost impossible (without TOR etc)



So what does "Login" look like?

Well, we're NOT "logging in". Instead:

- Authentication, to prove authorship (like of a comment)
- Managing authorizations and data permissions
- Following/subscribing feeds



Example: the **Session** page

- Title
- Slides & notes
- Footnotes and references / follow-up materials
- (optional) discussion thread afterwards
- Topic / keywords
- Links and interconnections to other apps

^ this data lives on IIW's storage, signed by IIW. When users contribute (leave comment, leave links, etc), authorship is recorded, IIW is granted permission to these contributions, etc.

Building a National-Scale IdP: Shortcomings of OIDC

Session Convener: Frederico Schardong
Session Notes Taker(s): Frederico Schardong

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

Link to slides

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

The following summary was generated by ChatGPT based on the transcription of the recorded session. All participants had consented to the recording.

1. Introduction and Overview

The speaker, **Frederico Schardong**, from Brazil, opened the talk by introducing the purpose of the presentation: to share the technical and social challenges involved in implementing a **national-scale Identity Provider (IdP)** capable of serving Brazil's **210 million citizens**. The slides were co-authored with **Brendon Vicente** (his master's student) and **Ricardo Custódio**.

2. The Brazilian Context

Frederico painted a picture of Brazil's social and digital landscape:

- Brazil is a **continental-sized country** with high **regional, cultural, and economic diversity**.
- There is significant **wealth inequality** and **digital inequality**.
- Despite this, **almost everyone owns a smartphone**, typically a **low-cost Android device**, making mobile web-based services a viable channel for nationwide identity systems.

- However, **digital literacy is low**: people know how to use social media (WhatsApp, Instagram, Facebook) but often struggle with formal or secure digital services.

3. The Digital Identity Landscape in Brazil

Frederico described three major systems that currently coexist in Brazil

1. **Gov.br** (Executive Branch)
    - The **main government identity portal**, created around eight years ago to centralize citizen access to digital services.
    - Built on **OpenID Connect (OIDC)**.
    - Widely adopted despite being associated with some security and usability challenges.
    - Despite its widespread adoption, questions remain about its perceived trustworthiness and resilience.

2. **ICP-Brasil** (Executive Branch)
    - Brazil's **public key infrastructure (PKI)** based on **X.509 certificates**.
    - Exists for over 20 years, but is costly and complex; only a small percentage of the population holds a digital certificate.

3. **IdRC (Civil Registry Digital Identity)** – The team's project
    - Developed under the **Judiciary Branch**, which manages Brazil's network of **civil registry offices**.
    - These offices (over 7,000 across the country) are **federated and decentralized**, issuing foundational documents such as birth and death certificates.
    - **IdRC** extends this foundational identity to the digital realm:
        - When a **birth certificate** is issued, a **digital identity (eID)** is automatically created.
        - When a **death certificate** is registered, the eID is **deactivated**.
    - It currently has around **200 million registered users** and around **12 million active monthly users**, but supports only **OIDC/OAuth 2.0** for now, with plans to incorporate **Verifiable Credentials**.

4. Shortcomings of Current Standards

Based on their experience implementing IdRC, the team identified **three core limitations in OIDC** that hinder its use in national-scale systems:

1. **Insufficient Representation of Assurance Levels**
    - Standards like **NIST SP 800-63-3** define:
        - **IAL (Identity Assurance Level)** – how rigorously the user's identity was verified at registration;
        - **AAL (Authenticator Assurance Level)** – how secure the authentication mechanism is.

- **OIDC exposes only one claim (`acr`)** for assurance, which implementers must choose to either expose AAL or to merge both dimensions.

2. **Loss of Authentication Context**
   - The OIDC claim **`amr` (Authentication Methods References)** lists only method names like `"pwd"` or `"sms"`, without metadata.
   - Missing details include:
     - Which IdP validated each factor;
     - The associated assurance level;
     - The time and location of validation;
     - The policies used (e.g., password rules).
   - This becomes problematic in **brokered authentication chains** (e.g., RP → GitHub → Google → RP), where tokens cannot express the complete authentication path.
   - This lack of semantic structure also results in the loss of critical information for applications that demand auditing and adaptive security.

3. **No Standardized Way to Request Authentication Factors**
   - OIDC allows specifying general assurance levels via `acr_values`, but **not logical combinations** such as "password **AND** OTP" or "biometric **OR** hardware key."
   - Furthermore, OIDC does not have a standardized way to negotiate specific authentication factors metadata.
   - This limitation forces applications to implement **proprietary extensions**, harming **interoperability, compliance, and auditability**.

5. Proposed Extension: OIDC4AC (OpenID Connect for Authentication Context)

To address these gaps, Frederico introduced the **OIDC4AC** proposal — a **backward-compatible extension** to OIDC designed to improve **semantic clarity, auditability, and policy alignment**.

1. **New Claim: `amr_details`**
   - Adds structured context to each authentication factor.
   - Each element contains:
     - `auth_method`: method identifier (`pwd`, `otp`, `face`, etc.);
     - `src`: details about the issuer, trust framework, assurance level, and timestamp;
     - `auth_details`: method-specific metadata (e.g., hashing algorithm, biometric score, TOTP length).
   - Enables a **full trace** of how, when, and where each factor was validated.

2. **Declarative Authentication Requirements**
   - Expands OIDC's `claims` parameter to allow **logical operators** (`one_of`, `all_of`, `min`, `max`, `max_age`) so that Relying Parties can request complex multi-factor combinations.

- Example: require **password + (OTP or face recognition)**.

3. **Benefits and Use Cases**
   - **Auditability & Traceability:** every authentication event can be logged and verified.
   - **Relying Party Flexibility:** applications can specify precise authentication needs.
   - **Risk-Based Access Control:** dynamic adjustments based on assurance levels or contextual metadata (e.g., IP location).
   - **Semantic Interoperability:** fully aligned with OpenID Foundation terminology, enabling **gradual adoption** without breaking existing implementations.

6. Closing Remarks

Frederico concluded by emphasizing that while the proposal was born from **Brazil's national identity challenges**, the principles apply globally to any country seeking **secure, transparent, and interoperable identity systems**. He thanked the IIW community and encouraged collaboration to advance **OIDC4AC** as a community-driven standard.

Post-summary notes:

Due to significant background noise caused by another session taking place in the same room, the recording device was unable to clearly capture portions of the discussion, particularly the valuable exchanges with Frederik Krogsdal Jacobsen from Criipto and Andy Barlow from Auth0.

Frederik contributed by presenting European use cases that encountered similar challenges and could potentially benefit from the approach proposed by Frederico. The representative from Auth0 noted having observed comparable ad hoc implementations aiming to address the same issues discussed by Frederico, indicating that standardization in this area could be beneficial. He also suggested that the proposed operators for the authentication factor requests should include additional options such as *equals* and *not_equals*.

Frederik further observed that the level of detail proposed by Frederico for the metadata describing authentication factors might only be appropriate in contexts where the Relying Party (RP) has signed a Non-Disclosure Agreement (NDA) with the Identity Provider (IdP), given the amount of potentially correlatable information involved. Frederico then noted that, although the proposal is broad in scope, it would be valuable to standardize common metadata for each authentication factor. He clarified that the proposal envisions these metadata as optional elements within the specification.

Finally, Frederik pointed out that the next step for having this proposal becoming a standard starts with submitting a draft to the AB/Connect Working Group.

SESSION #15

German EUDI Wallet

Session Convener: Phil Dustin, Kristina Yasuda, and Christian Bormann, SPRIN-D
Session Notes Taker(s): Eric Scouten

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

https://ericscouten.dev/2025/iiw41/#session-15a-german-eudi-wallet (photos there)

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

Talking through implementation of EIDAS 2.0 which was passed into law in May 2024 and will be implemented in 2026. Lays the foundation for digital identity and trust (electronic signatures and time-stamping services) within the EU. Gives legal standing for qualified electronic signatures. EIDAS 1 (circa 2014) did not establish interoperability for digital identity.

In Germany, there is both an official government-sponsored wallet app, but it is possible for private enterprises to create their own. Other countries have very different strategies. There is an EU-wide reference implementation which Germany is building upon.

Demo of signing in with German ID card (which has NFC + PIN) and German ID wallet app. Back-end generates an SD-JWT and mDL that is stored in wallet.

Then demo of opening a bank account (demo bank, of course) using a presentation from the wallet app. Almost instant ID verification.

German law requires relying parties to register (and thus get a registration certificate) and to be transparent about the data that they're requesting.

To become a relying party, must register with German wallet tool. Process yet to be defined. Will have an "ecosystem management portal," but that doesn't exist yet. Looking for serious RPs to do prototype engagements. May be difficult for non-European companies to gain access.

Interesting: The issuance and RP trust chains are still X.509 based. Only the individual wallet presentation is SD-JWT or mDoc based. Look for "Blueprint for the EUDI Wallet Ecosystem in Germany." Also "Architecture Documentation for the German National EUDI Wallet." Look at "PID Presentation."

Resource Owner Passkey Credential Flow for Agentic AIs

Session Convener: Hideaki Furukawa
Session Notes Taker(s): Hideaki Furukawa

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

passkey, agentic AI

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

Usage of the web interface instead of APIs for the AI agents is not the best way, but still better than nothing.
The participants have pointed out that the management of the passkeys for the agents would be complicated.

Can YadaCoin Help Keri?

Session Convener: Matt V
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

MyTerms Next Steps

Session Title:

- What was proposed: “Privacy Dissolution or Reclamation -- How do we reclaim data practically speaking and attach data to a strong ID? What are the protocols?”
- What we talked about: “MyTerms Next Steps”

Session Convener: Beth Porter
Session Notes Taker(s): Beth Porter

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

https://arstechnica.com/gadgets/2025/03/doc-searls-myterms-aims-to-offer-user-first-privacy-contracts-for-the-web/
https://doc.searls.com/myterms/
https://doc.searls.com/2025/08/14/the-case-for-myterms/
https://projectvrm.org/2025/04/06/myterms/
https://www.bladetechinc.com/news/myterms-user-first-privacy

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

Summary of my conversation with Joyce:

- MyTerms comes out of the IEEE standard (under Customer Commons)
- What does the world look like in 2030 with MyTerms and PODs (or Wallets)?
- Many companies don't trade in personal information — so they will start with those sites, since it's an easy lift for a site like that to accept MyTerms.
- Base contract of MyTerms — you can use this information for this transaction only!
- Extensions of the base — you can sign me up for a newsletter (or something); you can share my data with other vendors; etc.
- This is not consent — it's a contract with the end user! Consent doesn't scale.
- For the consumer, this is like a protest! The idea of having agency.
- Should look at Utah! The SEDI project is well underway. They really got it down to rights!
    - MyTerms + Inrupt
    - MyTerms + AskCR
    - MyTerms ++
    - MyTerms + Observability Framework (OtterMon?)
- MyTerms has been approved by IEEE, but it still hasn't been published (should come out in January)
- It's a trust system with mutual audit (by customer and vendor); but, with a penalty system
- Contract is part of GDPR, but nobody has ever done it because it's been deemed to be hard
- (Blockchain as double-entry bookkeeping)
- Who is going to keep the registry of companies that accept MyTerms?
- There are many possible ways to make money with MyTerms in the world.

Cross-Pollinate - Bring Your Ideas to "Server User-agents"

Session Convener: When Leggett
Session Notes Taker(s):

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

A summary of Server User-Agents and notes on IIW

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

This session was the second session on Server User-Agents, and was well attended by folks that had projects and ideas related to Server User-Agents and the session was spent trying to converge on a shared definition, as well as inviting others working in the space to see how their projects would fit.

As a result of this session, an impromptu working group was formed on a Signal chat to continue the work.

Sorta Kinda Digital ID - adding digitally signed printed elements to physical IDs and documents

Session Convener: Elaine Wooton
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

Local First Software + Bridging Communities

Session Convener: David Gildeh
Session Notes Taker(s): David Gildeh

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

Slides: Local First

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

The general discussion was about what local first is and how the community there, focusing on building a new application architecture using sync and Conflict Resolution Data Types (CRDTs) to give data and control back to users, has a lot of similarities with the Identity community and how we are thinking about things but don't seem to be connected.

Overall, local-first needs E2E encryption with key recovery, and the wallets/SSI we're working on is a great fit for that, so can see an opportunity to grow adoption of these technologies alongside the local-first community.

Authorization and Liability in AI Agents

Session Convener: Emu Iizuka
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

CfP Brainstorming - preparing for submissions to EIC and Identiverse

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

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

Links to CfP:

- https://www.kuppingercole.com/events/eic2026/callforspeakers (open until 31 October 2025)
- https://identiverse.com/ (open until Fri 9 January 2026, 11:59 PM PST)

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

Remember that IIW is about incubation. EIC is about solving identity problems primarily in the European market. Identiverse is currently the largest identity-focused conference in the world with about 3500 attendees. It has several different tracks, with Identity for Security generally receiving the most submissions, Professional Skills & Development and Privacy & Ethics generally receiving the least.

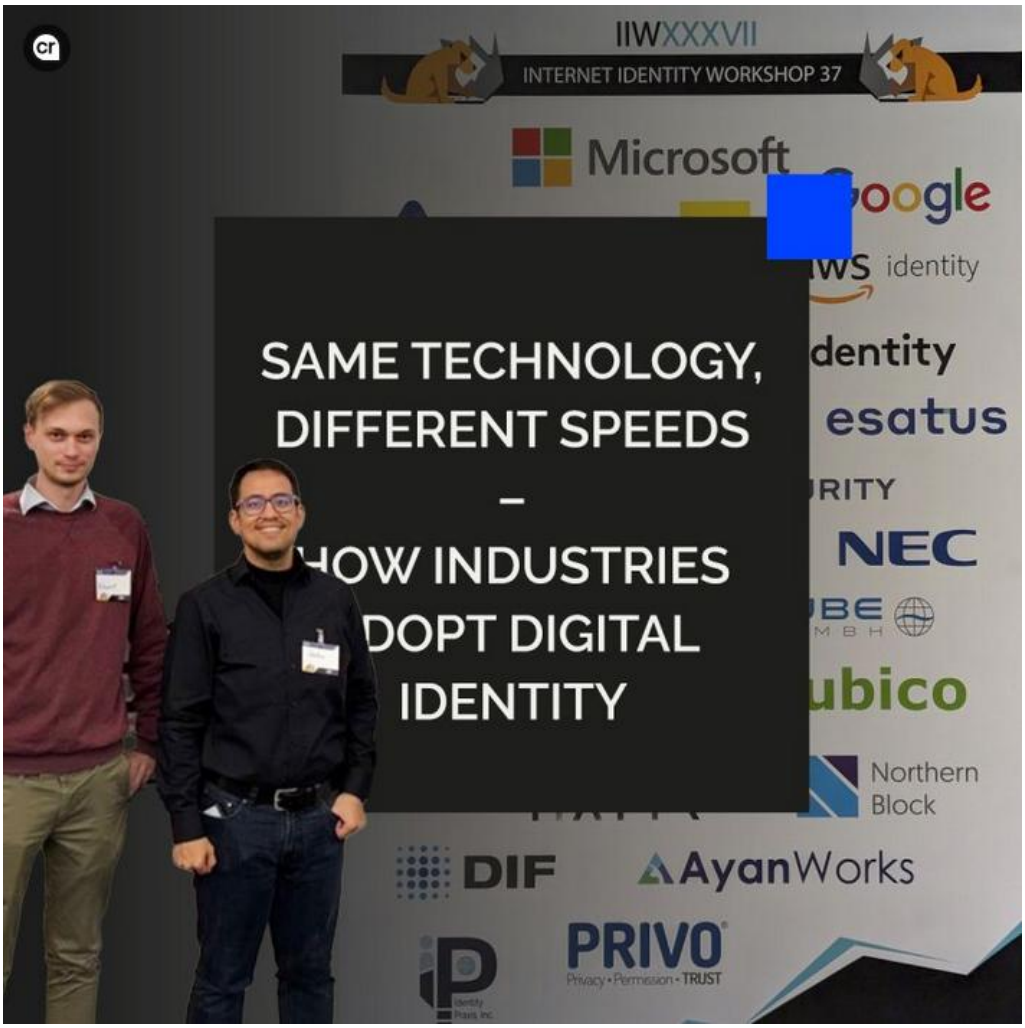
In both cases, make sure to read the instructions and think about what you're proposing is clear about the problem it is solving.

IDPro members have access to a Slack instance that includes a #conferencesubmissions channel that offers people an opportunity for early feedback from peers.

esatus AG
1,573 followers
3w •

Our colleagues **Vincent Kelbel** and Stefan Michel were in California last week for the **Internet Identity Workshop** (IIW) at the Computer History Museum, the meeting place for the global identity community. No keynotes or panels, just real collaboration where anyone can start a session, share an idea and get to work.

This year the focus is on KERI, a model for building trusted connections without central registries, and on vLEIs, verifiable Legal Entity Identifiers issued under the governance of **Global Legal Entity Identifier Foundation (GLEIF)**.



Thank You Speed Demo Hour Sponsor LF Decentralized Trust

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	**Email Verification Protocol:** Dick Hardt and Sam Goto **URL:** https://github.com/dickhardt/email-verification-protocol The Email Verification Protocol enables a web application to obtain a verified email address without sending an email, and without the user leaving the web page they are on. To enable the functionality, the mail domain delegates email verification to an issuer that has authentication cookies for the user. When the user provides an email to the HTML form field, the browser calls the issuer passing authentication cookies, the issuer returns a token, which the browser verifies and updates and provides to the web application. The web application then verifies the token and has a verified email address for the user.	More Info Here
#2	**OpenID Foundation conformance tests for OpenID for Verifiable Credentials:** Joseph Heenan **URL:** https://openid.net/how-to-certify-your-implementation/ OIDF has tests that wallets, verifiers & issuers correctly and securely implement OpenID for Verifiable Credential Issuance / Verifiable Presentations specifications, with ISO mdocs or SD-JWT VC - we demo them, explain their limitations & how you can run tests yourself.	More Info Here
#3	**Oblique:** Maya Kaczorowski **URL:** https://oblique.security/ Oblique is a self-service IGA solution for corporate access. Understand why a user has access, preview the impact of access changes before applying them, and delegate authority to teams to manage their own access.	More Info Here
#4	**SSI² :** Russ Haywood **URL:** this will update for demo into an interactive spreadsheet: Self-Sovereign Identity Squared: certification for platforms using Swiss legal structures to ensure true SSI tech, ethical governance & privacy. Users gain real data ownership & democratic control over their data—protecting both individuals & communities comprehensively.	More Info Here

#5	**Raidiam:** Lukasz Jaromin and Michael Fraser **URL:** https://raidiam.com How OpenID Federation-backed Trust Registry can underpin API, wallet ecosystems, and agentic-AI ecosystems	More Info Here
#6	**Gluu:** Mike Schwartz **URL:** https://gluu.co/cedarling-demo-wasm Enhance security in the front end--the Cedarling WASM browser extension lets you test Cedar policies locally on your laptop. See how to instantly load a policy store, validate JWTs from trusted issuers, and get instant allow/deny + diagnostics for actions on resources.	More Info Here
#7	**Beyond Identity:** Colton Chojnacki, Sarah Cecchetti **URL:** https://beyondidentity.com Beyond Identity brings deterministic, hardware anchored access controls to a non deterministic AI world. It cryptographically verifies every tool call from human users and workloads before execution, blocking rogue actions and logging every interaction.	More Info Here
#8	**SPRIND, German National Wallet**: Kristina Yasuda, Paul Bastian, Christian Bormann **URL:** https://bmi.usercontent.opencode.de/eudi-wallet/eidas2/en/start/ and https://bmi.usercontent.opencode.de/eudi-wallet/wallet-development-documentation-public/ National Wallet of Germany that supports issuance and online presentation of PID (digital eID)	More Info Here
#9	**Verifiable Credentials for Open Social Media:** Brendan Miller and Alberto Leon URL:https://docs.google.com/presentation/d/1geujJss_Dx6IoZg58lGtzlOrma3-eGwzzpULH2R8fNA/edit?usp=sharing Video Presentation: https://www.youtube.com/watch?v=-9pJK1_wRNc A live demo of verifiable credential-based badges (including age verification wit mock mDLs and cross platform authentication) running on our own Bluesky instance. We'll issue and present credentials, then verify on Bluesky, highlighting zero-knowledge proof flows.	More Info Here
#10	**WSO2: Securing AI Agents in Modern Applications:** Hasintha Indrajee & Sachin Mamoru **URL:** https://wso2.com/asgardeo/docs/guides/agentic-ai/ai-agents/ A demo on how AI agents can securely work on behalf of users in enterprise systems. We show how identity, authentication, authorization, and auditing ensure agents act safely and within defined trust boundaries.	More Info Here
#11	**Swisscom / How to digitally sign documents with your Swiss e-ID**: Michel Sahli **URL:** Unlike the EUDI Wallet, Switzerland's Swiyu wallet won't support native digital signing. Swisscom, as a QTSP, will allow partners to use the Swiss e-ID for document signing in the future. For e-ID preparation, we're offering Swisscom clients a Telco-ID, enabling Advanced Electronic Signatures for daily use.	More Info Here
#12	**Codename Yarvis: an agent that won't steal your voice:** w/ Tor Hagemann (dba 121&0n2) **URL:** https://onetooneandon.to/demo Meet "Axel" -- the best parts of Siri and Alexa with a local-first model that understands and respects your contextual identity.	More Info Here
#13	**MAIA - A Medical AI Assistant by HIE of One:** Adrian Gropper **URL:** https://github.com/agropper/maia-cloud-clean/tree/main MAIA is a private AI chatbot that indexes a complete health record and acts as a privacy gatekeeper for chats with a choice of frontier LLMs as well as human consultants. It uses "anyone with the link" security to integrate with text, email, Signal, and hospital portal messaging.	More Info Here
#14	**eID Easy - Universal API platform for eSignatures, eSealing, and eID**: Mats-Joonas Kulla **URL:** https://www.eideasy.com One integration to access a worldwide network of Qualified Trust Service Providers (QTSPs) and Certified Authorities (CAs), for eSignatures, eID authentication, and eSealing while ensuring full compliance with local regulations.	More Info Here

#15	**Paradigma SpA - Unbreakable ID: A Secure Digital Identity Solution:** Phillip Roe **URL:** https://ubid.app Users own the Unbreakable ID Profile and use it to connect to other apps using OpenID Connect. It is persistent, with verifiable credentials, user-controlled digital identity. Users use a Local Web Node to store their identity credentials in a secure Remote Decentralized Web Node. Institutions can create branded identity domains for a seamless, institution-aligned experience	More Info Here
#16	**CoralStack demoing CoralKM**: David Gildeh (Founder) **URL:** Not available yet If Self-Sovereign Identity is going to go mainstream, we need a user friendly key management system. CoralKM is a user-friendly DIDCommV2 protocol for decentralised .key..management.	More Info Here
#17	**Live demo of OpenID Federation in action with MCP:** Chris Phillips **URL:** letsfederate.org We'll share the deployment approach for enabling OpenID Federation with ModelContextProtocol(MCP) to elevate and enable cross-domain capabilities, adding IAM attributes, and use cryptographic trustmarks for improving software supply chain integrity and provenance.	More Info Here
#18	**GLUE.ID**:Justin Magruder from Noetic Partners Inc. & UALR team URL: https://datahub.glueid.com/ GLUE.ID is a patent-pending tokenized identifier for financial & supply chain risk management that delivers unique, verifiable identifiers mined from primary sources. GLUE.ID exposes relationships, links identifiers, and provides critical insights to risk managers and supply chain analysts. GLUE.ID tokens are an immutable digital asset deployed to enable decentralized access to legal entity data.	More Info Here
#19	**Raidiam: Raidiam Connect Trust Platform**: Michael Fraser and Lukasz Jaromin **URL:** https://www.raidiam.com/developers OpenID Federation in action: a standard made to enable trusted multilateral relationships in API, wallet, and Agentic AI ecosystems. Live demo of dynamic trust establishment and automatic client registration between entities with no prior relationship.	More Info Here
#20	**esatus AG / Employee Onboarding with SOWL and EUDI Eallet:** Stefan Michel/ Vincent Kelbel **URL:** https://esatus.com/en/ SOWL speeds up company onboarding processes by granting authorization credentials based on a PID presentation using the employees EUDI Wallet.	More Info Here

Thank You Women's Breakfast Sponsor Open ID Foundation

Martina Kolpondinos, PhD • 1st
Decentralized Trust, SSI & First Person Project ...
3d •

The Internet Identity Workshop number 41 day 2 beginning with the 🍗 Women's Breakfast 💪🏽🫶🏽 which is always a highlight: a space for exchange, encouragement, and reflection among smart, passionate women who are shaping the future of identity and trust in digital interactions.

💫 Next, looking at today's full session board, one thing stands out again: #IIW continues to be a place where collaboration thrives: no stages, no keynote speakers - instead, people co-creating, sharing, and advancing solutions for identity and trust in digital spaces.

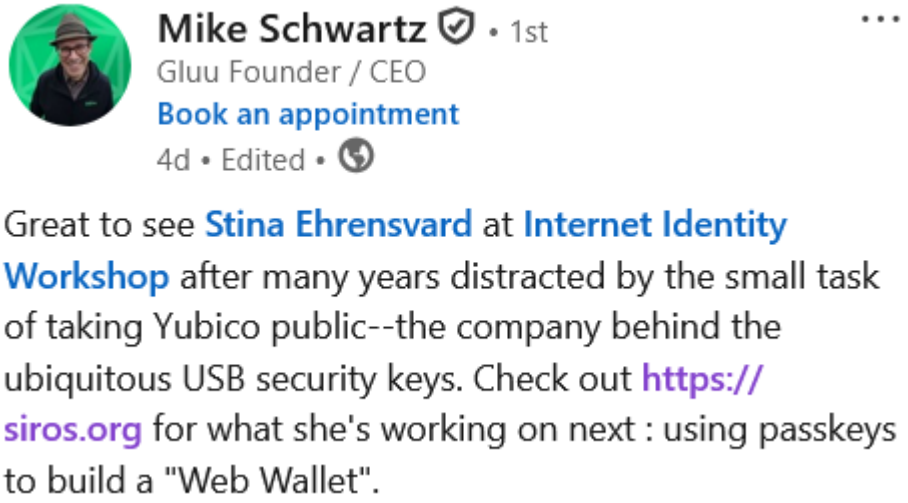
💫 As someone working at the intersection of identity, trust, and human-centered innovation, I deeply value moments like these - where ideas move from theory to practice, and networks turn into communities - and, where even coffee celebrates the context 😉

💫 Grateful to be part of this evolving community and also to see more women's voices actively shaping it.

Event Photos taken by Doc Searls

Doc Searls has several hundred candid photos IIW on his Flickr account

Link to Album of all 3 Days:
https://www.flickr.com/photos/docsearls/albums/72177720330129293



Identity Funnies – (comic strips) shared by Alan Carp!

One-Step, Two-Step Verification

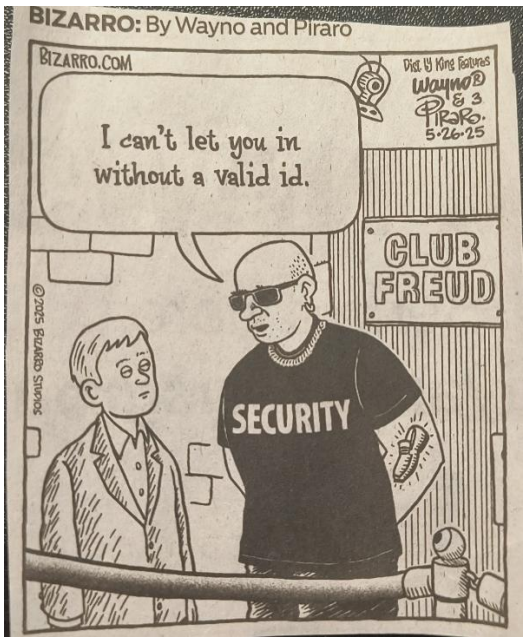
Insecurity Questions

We buy personal information for cash!

A name…

Identity Theft

Club Freud



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/

IIW Inspired™ Regional OpenSpace unConference Events

Did:unConf Africa | With Our Partner DIDx

Bridging the Digital Identity Gap in the SADC Region
February 24 - 26, 2026 Cape Town, South Africa

🗓️ Please Join Us: 24–26 Feb 2026
📍 STIAS: Stellenbosch Institute for Advanced Study, Stellenbosch, South Africa
🎟️ More information and Register Here

🚀 Day 1 Kick-off: A dedicated African-Focused Business & Alignment Program, designed to help institutions, commercial platforms, and service providers engage meaningfully with the open identity ecosystem.

🐝 Followed by a 2-Day IIW Inspired Open Space unConference

Digital Identity unConference Europe | DICE Europe 2026

Fostering Digital Identity Collaboration across Europe

June 2026 - Location to be announced in December
Follow on LinkedIn for updates

APAC Digital Identity unConference

Fostering innovation and collaboration between emerging digital identity companies and projects across the APAC region / **Next Event Date/Location TBD**

Hope to See you April 28, 29 & 30, 2026 for IIWXLI

The 42nd Internet Identity Workshop
April 28 – 30, 2026
Computer History Museum
Mountain View, CA

REGISTRATION OPEN in December
www.InternetIdentityWorkshop.com

AND IIWXLII #43 is November 3.4 & 5. 2026

Follow IIW on LinkedIn for Updates on All Our Events!

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