IIWXL

INTERNET IDENTITY WORKSHOP 40

Book of Proceedings

Group Photo of (most) Attendees of IIWXL
April 8 - 10, 2025

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: Procivis & Spherical Cow Consulting

Contents

Attendees of IIW I in the fall of 2025

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.

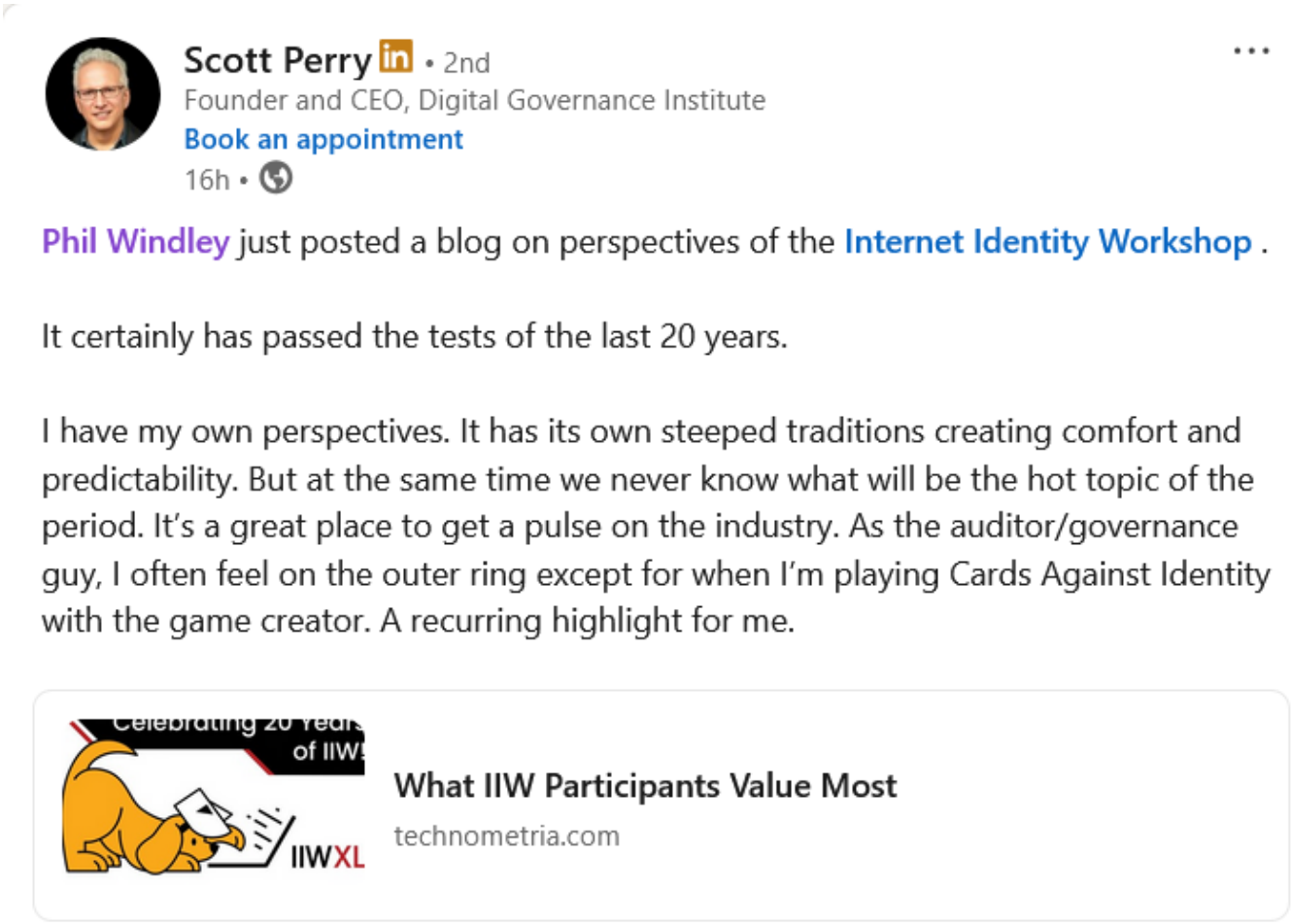
Watch this short documentary film: ***"Not Just Who They Say We Are: Claiming our Identity on the Internet"*** http://bit.ly/IIWMovie to learn about the work that has happened over the first 12 years at IIW.

The event is now in its 20th year and is Co-produced by Phil Windley and Heidi Nobantu Saul

Next Event is IIWXLI #41
OCTOBER 28,29 and 30, 2025

https://internetidentityworkshop.com/

What IIW Participants Value Most



Phils Post

Last week, I posted a report on IIW XL, our fortieth event. When participants register, one of the questions we ask them is what they value most about IIW. Over 100 people answered that question. Rather than bore you with the raw data, I asked *ChatGPT* to summarize the responses. Here's what it said:

'Attendees of the Internet Identity Workshop (IIW) overwhelmingly value the event for its strong sense of community, collaborative spirit, and the opportunity to connect in person with peers, innovators, and industry leaders. Many describe the environment as one of mutual respect and openness, where "creative, open discussions" thrive and "everyone is there" to engage deeply on current and emerging identity challenges. The unconference format stands out as a major strength, allowing participants to shape the agenda, dive into interactive workshops, and experience "productive conversations with other attendees" in a way that feels dynamic and inclusive.

Another consistent theme is access to cutting-edge knowledge and thought leadership in digital identity. Attendees appreciate being "in the room where the future of identity is being designed," hearing about "the latest developments in enterprise IAM," and learning directly from experts in topics like decentralized identity, verifiable credentials, OAuth, and OpenID Connect. The opportunity to "catch up on standards," "inform product roadmaps," and "gain knowledge about key trends" makes IIW not just informative but strategically valuable.

Crucially, IIW is also seen as a place where real progress happens. Participants value the ability to test ideas, gain feedback, and move forward on shared goals in a collaborative setting. As one attendee put it, it's a rare opportunity "to explore problem spaces and solution spaces together," while another highlighted the value of "making progress on standards or other collaborative efforts." The event's unique mix of expertise, spontaneity, and shared purpose creates the conditions for meaningful breakthroughs that extend well beyond the workshop itself.

Beyond the sessions, many emphasized the personal and professional relationships formed over time—"the relationships that have been developed over many years" and the chance to "collaborate in person with colleagues around the world." Several first-time attendees expressed excitement about joining a space described as "unlike any other" and "highly recommended" by peers. Whether returning veterans or newcomers, participants consistently frame IIW as a place of learning, contribution, and genuine connection.'

Phil had an extra exciting start to IIWXL!

Thank You to Our Sponsors!

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

IIWXL 3 Day Schedule

TUESDAY, April 8 / 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 Reception & Dinner 6:00
Off the Rails Brewery 111 S Murphy Avenue Sunnyvale, CA 94086 (408) 773-9500

WEDNESDAY, April 9 / 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**	Speed Demo Hour	1:30 - 2:30
Opening Circle / Agenda Creation (SHARP)	8:45 - 9:30	**IIW40 Cake!**	2:30 - 3:00
Session 1	9:30 - 10:30	Session 4	3:00 - 4:00
Session 2	10:30 - 11:30	Session 5	4:00 - 5:00
Session 3	11:30 - 12:30	Closing Circle	5:00 - 6:00
Lunch	12:30 - 1:30	Conference Dinner	6:00 ~

Conference Reception & Dinner
BackAYard Caribbean Grille (w/plenty of V&V options) - Here at CHM!

THURSDAY, April 10 / 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	**IIWXLI October 28 - 30, 2025**	

Drinks/Dinner 5'ish No Host @ Das Bierhauz 135 Castro Mountain View https://dasbierhauz.com/

IIW40 Agenda Creation = Schedule & Workshop Sessions

147 distinct sessions were called and convened over 3 Days.

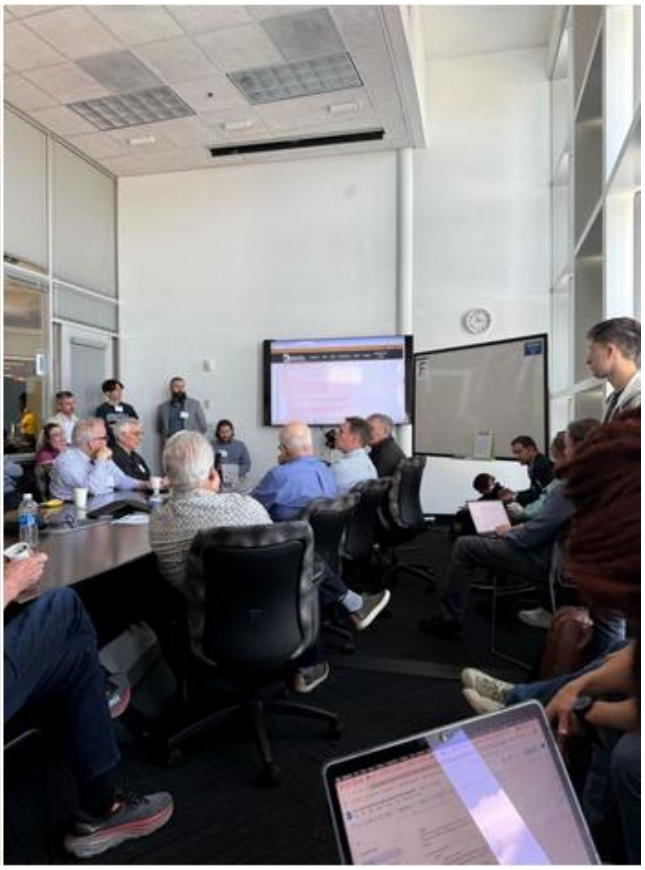
We received notes, slide decks, links to presentations and photos of whiteboard work for 106 of these sessions.

SpruceID
4,114 followers
1w •

We joined in on the **Internet Identity Workshop** in Mountain View this week alongside a global community of developers, standards architects, policymakers, researchers, tech leaders, and more committed to building open, user-controlled digital identity.

Over dozens of participant-led sessions, we explored everything from verifiable digital credentials and wallet interoperability to trust frameworks and governance models. We're feeling energized by the collaboration and inspired by the work happening across the ecosystem.

Thanks to everyone pushing toward a more secure, privacy-preserving digital future. Can't wait to see you at the next one.



Notes Day 1 / Tuesday / Sessions 1 - 5

SESSION #1

OpenID4VC and DC API 101

Session Convener: Kristina Yasuda, Tim Cappali
Session Notes Taker(s): Lukas Han / Bjorn Hjelm

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

Presentations:

- OpenID for Verifiable Credentials Road to Final: https://drive.google.com/file/d/1Ulnos2T24FGNmDIoX6Fj2hf8Xg-xv9eu/view
- Updates from the OpenID Foundation to W3C Web Payments WG: https://drive.google.com/file/d/17BQZJ0o-scca61BByaiGwmYR7C-aE6Vg/view
- Digital Credentials API: https://drive.google.com/file/d/1QjTX9OLfuIY96ahMpRX7Hq6Kd6A7VyFG/view?ts=67f572cb

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

The session provided an overview of OpenID for Verifiable Credentials and Digital Credentials API.

OpenID4VC Overview

- OpenID for Verifiable Credentials (OpenID4VC) refers to the set protocols OpenID for Verifiable Presentations (OpenID4VP specification, OpenID for Verifiable Credential Issuance (OpenID4VCI) specification, and OpenID4VC High Assurance Interoperability Profile (HAIP) specification. The latest version of the specifications can be found at https://openid.net/wg/digital-credentials-protocols/specifications/.
- The timeline for all specifications is to be 1.0 Final around June 2025 with no breaking changes after 1.0 (any updates to be published as versions 1.1, 1.2, etc.).
- The presentation also included the problem statement, highlighting the global adoption (EU, US/NIST, Japan) of these specifications, list of Open Source libraries and (selected) completed interoperability events.
- OpenID4VC Conformance Tests are available (separate presentation) as well as security analysis with White Paper in development.

OpenID4VP Updates

- DCQL (see https://docs.google.com/document/d/1WV7Dd_erFKtOW8pJN87rKobUrovEcnkCayJVo3-L3Qs/edit?tab=t.0)
- Digital Credentials API
- Transaction Data

OpenID4VCI Updates

- Optimizing Issuance of Credential Batches.
- Credential, Credential Dataset and Credential Configuration.
- Wallet Attestation and Key Attestation.

HAIP Update

- Document restructured to be a collection of 4 profiles that can be used independently.
  1. Issuance of IETF SD-JWT using OpenID4VCI.
  2. Presentation of IETF SD-JWT VC using OpenID4VP.
  3. Presentation of IETF SD-JWT VC using OpenID4VP over W3C Digital Credentials (DC) API.
  4. Presentation of ISO mode using OpenID4VP over W3C Digital Credentials (DC) API.

Transaction Data

- Brief overview of Transaction Data (feature in OpenID4VP) to authorize transactions using a payments use case and flow.

SD-JWT VCDM

- Brief overview of the proposed SD-JWT VCDM

Digital Credentials API

- Background and design goals
  - Challenges with custom schemes
  - Learnings from passkeys
  - Overview of design principles
- Overview of the Protocols and Credential Formats (ISO mode, SD-JWT VC, W3C WCDM)
- Roles and responsibilities between Browser (web platform), OS Platform (app platform), and Credential
- Reviewed various flows (available at tcslides.link/dc-layers)
- Overview of the API with code examples

OpenID4VC Demo tomorrow.

OAUTH 101 What and Why (an IIW 101 Session)

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

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

NO NOTES SUBMITTED

Scammers Steal Your ID from WALLET

Session Convener: Hideaki Furukawa
Session Notes Taker(s): Naohiro Fujie

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:

There are three checkpoints to mitigate the misuse of information in ID Wallet

- Before presentation
- During presentation
- After presentation

Before presentation (preparation to prevent Holder from passing information to malicious Verifier)

- Register a trusted verifier
- Reputation-based Verifier evaluation mechanism

During presentation

- Transaction protection (unnatural time lag, prevention of consent by others, etc.)
- Exchanging messages expressing that the transaction is in a trustworthy state can be considered, bringing in the idea of a trust framework.
- There may be countermeasures similar to anti-phishing, such as simply filtering by domain name.

After presentation

- Combining monitoring with SSF may be helpful.

An additional consideration is whether the Wallet is good or bad.

- In the EU, Wallet Attestation determines if the Wallet is authorized.
- Code analysis is complex on a large scale.
- Reputation-based evaluation will be applied not only on the verifier but also to issuers and wallets.

Zero Knowledge for MDOC and JWT

Session Convener: Matteo Frigo, abhi shelat
Session Notes Taker(s): David Waite

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

https://drive.google.com/file/d/16gqPYykY0hcBJDFMcLRHBf9E7uEU_xeA/view?usp=share_link

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

(Conversations outside of s
For revocation - need to reduce the amount of work for the issuer. For instance, the issuer may issue a credential once a month but not need to be involved in potential hundreds of uses.

Question on TLS-ZK, where there's a notary - the models do not have a lot of similarities although they do use several similar techniques.

Question from Kim - can you get relying parties to accept this? If a relying party trusts mdoc, they should trust this zk process because there are no setup parameters.

Christian - how efficient could the verifier get? Since there is still a lot of processing needed by the verifier. Suspicion it is more like a factor of 5 than a factor of 100.

Does the time it takes on the prover change by device type? Processing is running on a 4 year old pixel on a single core. But so far, none of the UX people consider it a problem due to the proving happen in parallel to the UX flow.

When revoking, is there an efficient way to revoke large batches of credentials for an infrastructure issue? You can revoke a whole range of credentials

Do you download the list then give a bucket, e.g. herd anonymity? There are options there

Observation - the credentials hold personal information, so the optimal revocation scheme may vary depending on the mutability of the information and how often credentials get reissued

How does this get correlated? The version of the revocation chain is one of the input parameters.

For ZK-SD-JWT, do you need to generate the KB-JWT, since you aren't disclosing it? We would prefer this to act as an optional layer, so that we have the same logic on the mobile device as a fall-back if ZK is unavailable on the verifier.

For BBS, would it be acceptable to have a fixed order or attributes to prevent differentiation of credentials? Very difficult in practice once you are proving from one of a set of issuers, optional attributes, group attributes

Marketing Identity to the General Public - Lesson Learned over 20 Years

Session Convener: Brad Topliff
Session Notes Taker(s): Frederik Krogsdal Jacobsen

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

Link to UK study?

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

As people involved in the community, we know about privacy, security, user control, etc.

A lot of initiatives are driven by governments or big institutions.
How do we engage to get the kinds of systems we would like in real implementations?
We need to convince the people making the decisions.

The dominant identifier is an email address - especially to the general public.
What do the general public want? They don't want to care about identifiers or how it works.
UK study: young people don't use email, they use SSO via big tech and don't know any alternatives.
But if you have a GMail and Google decides they don't like you, you're cut off.

People now know how to use biometrics, and are used to everything working seamlessly with it.
Passkeys will probably gain acceptance soon, but they seem a little scary for people used to "regular" MFA. We need to be careful of tech that lets you blindly trust by hiding complexity.
"Tyranny of convenience": convenience is more important (to the general public) than security/privacy/anything else. The user just wants to get the job done - security needs to be built into the workflow.

Cybersecurity is really about trust. A lot of technology misses the basics of identity - i.e. cryptocurrency "rug pulls."
But what is trust? You can think of vulnerability vs. ability - i.e. if I let you have some data, I get some benefit.

We need to continually remind ourselves that the general public knows absolutely nothing about identity or technology. Our core values need to be reinvestigated continually.
Way of thinking in the general public: "I want security, but not if I have to do anything."
But security is not necessarily the opposite of convenience. If you have this mindset, you will create systems where security is in tension with convenience.
The feeling of security is often more important than the fact of security. If a system is completely seamless, the user cannot distinguish between a secure system and an insecure system.

Inclusion: not everyone has access to e.g. a smartphone.

Do you even need a digital identity? In a lot of cases, users don't want an account.

In the EU, people start by thinking about what could go wrong, then the value. Can this approach work?
Caution: you can keep going forever if you don't allow some level of insecurity.

What can overcome the tyranny of convenience? Government/enterprise mandates you have to do it.
But people might work around it - creating vulnerabilities. If users don't understand the consequences of their actions, they will work around inconvenience. Work-arounds are usually only temporarily successful and usually lead to worse outcomes.
Usability is different for each user.
Consequences: organisations and end users may have different value propositions and they may conflict.

We need to be careful not to be distracted by "shiny new computer science things" that don't actually solve a problem. What value are you bringing to the user/the customer?
How are you going to use this? Why would I bother using this if it causes friction?

It is utopian to think that there will be one universal ID for every purpose.
Sometimes you need privacy, sometimes the whole point is not to have it.
Ecosystems need to focus on making it easy for the general public.
Interoperability is paramount.

Trust needs to be built slowly, but how do you do that in a "move fast and break things" world?
Influencers/thought leaders are a big factor in what people trust.

Unintentional consequences: sometimes attempting to design for security may lead to irrational decisions because of a lack of risk modeling. Attempting to avoid one problem at all costs can make other problems worse.

The bar is high for consumers to actually pay for security services. Education is really difficult and it is hard for the general public to determine whether one solution is more secure than another one.
The general public understands that there is an issue, but not what to do about it.
20 years ago, the general public did not believe that there were issues, but now there is an appetite to take ownership of their identity and up their security.

Rough consensus points:

- Start with the user experience
- Now is the time to capitalize on the awareness of security which is much better than it was 20 years ago
- No consensus on whether now is the right time to market to individuals

Utah's new Digital Identity Legislation.

Session Convener: Chris Bramwell, Steve McCowen, Timothy Ruff, Sam Smith, Joe Jackson
Session Notes Taker(s): Alyssa Morgan

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

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:

bill link (sb260)
identity could be owned by a corporation, or a gov't- fundamentally needs to be owned by individual

definitions are CRITICAL! everything comes back to the language in legislation (and at the same time, something is better than nothing, incremental change is the goal- basically, they don't want people to not write laws because they're worried about having all the wording Exactly Right)

definitions included in bill:

- guardian
    - who's the custodian? who is authorized to do things with your identity?
- what's identity?
    - what is state endorsing as digital ID?
    - what does it mean to be a person/individual?
- what is a physical identity? what is personal data? what is a person? what is an individual
    - diff b/t person and individual
        - individual- living human being
        - person- can be a person or a corporation
- 'state endorsed dig ID program"
    - who owns ID? who controls it? very uncomfy rn
    - state can do things that other companies/entities can't
        - state is the only legal entity that can have a monopoly on anything
        - **state job: empowers indivs, lets them verify who they are and lets them flourish**

personal q: does nc law have a definition for identity? either physical or digital
**stopped recording at 7:55

each indiv has their own identity. the state *does not establish* indiv identity (important!) but can recongise or enforce an identity

ex; when you're born, you parents choose a name for you, register it and then the state enforces it (accepts it and refers to you as such) that's the different between creating andd enforcing. children don't get named by the state, their guardians choose a name to attach to the invidiual and gov't falls in line

note: this law is about more than dig. identity- it's an identity bill *first* and then goes into digID (which is just a digital representation of the physical inidivual)

christmas tree analogy: individual's identity is the christmas tree. it stay up and is (mostly) unchanging, things get added on top of it (drivers license, marriage license, boating/fishing license. all relate to the person ((ornaments on the tree)) but the person is fundamnetally the same, and the ornaments can be changed/removed at any time. still the same tree (individual)

bill: lays out what state endorsed dig id should look like (policy discussion) + will need to work in interstate compatibility

bill- only about ID, not entitlements
biometrics: within definition of ID- can include personal/phys characteristics, biometric info, (current working definion of biometrics within the bill/conversation arround the bill) VERY important because it helps authenticate that a person actually is who they say they are (which is why we have pictures on drivers licenses and passports)

current bill- establishes the principles. next step/bill will hopefully establish the framework/set up the system

BIG QUESTION: who owns the binding between (see around 18 mins into recording- i missed it)

- how to future proof this against misuse by oppositional authority
- response to security state " march towards dig ID is not going to stop. trying to oppose it…is not realistic. the argument sounds silly, but the argument is powerful. had to go to those people and win their support- winning argument: **dig ID will keep marching forwards and w/out privacy preserving policy we'll end up with something bad**" if we don't put forward an alternative, you'll end up with something bad

DID Methods Update

Session Convener: Markus Sabadello
Session Notes Taker(s): Eric Scouten

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

(See links within notes below.)

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

Update on the various working groups working on DID methods.

W3C

Has ratified the as a DID Core 1.0 standard recommendation. New W3C DID WG is currently building:

- DID 1.1 standard
  - No breaking changes
  - Adding dependency on the CID 1.0 spec (controlled identifier), which is a generalization of the DID document for non-DID identifiers. Note that the DID document spec is moved from DID Core 1.0 to CID 1.0, but is backward compatible.
  - Introduces a new media type `application/did` which can be used as a simplification compared to `application/did+json` or `application/did+ld+json`
- DID resolution and DID URL dereferencing 1.0 -- adds detail around
  - Algorithms
  - Parameters, metadata, error coes
  - HTTPS bindings
- DID extensions registry
  - Helping to specify behaviors of DID resolver, for example:
    - Translate public key representations
    - Translate relative URIs to absolute URIs
    - Constrain to public keys that are used for specific purposes
    - Look up DID document at a specific version or point in time

DIF DID Methods WG

(Collaboration between DIF, W3C CCG, ToIP, and INATPA.)

This WG is intended to address the question of "which DID methods should be used and implemented." This is an effort to curate the currently-overwhelming list of DID methods.
So far, this group has:

- Selection criteria (How would the WG choose a shortlist of DID methods?)
- Proposing approved/endorsed DID methods (currently about 10 are under consideration)

Related to currently-proposed W3C DID Methods WG.

Likely outcome: A curated list of "DIF-endorsed DID methods" which may be formally standardized elsewhere (DIF, EBSI, W3C, ToIP, etc.).

See also (crunched for time at the end):

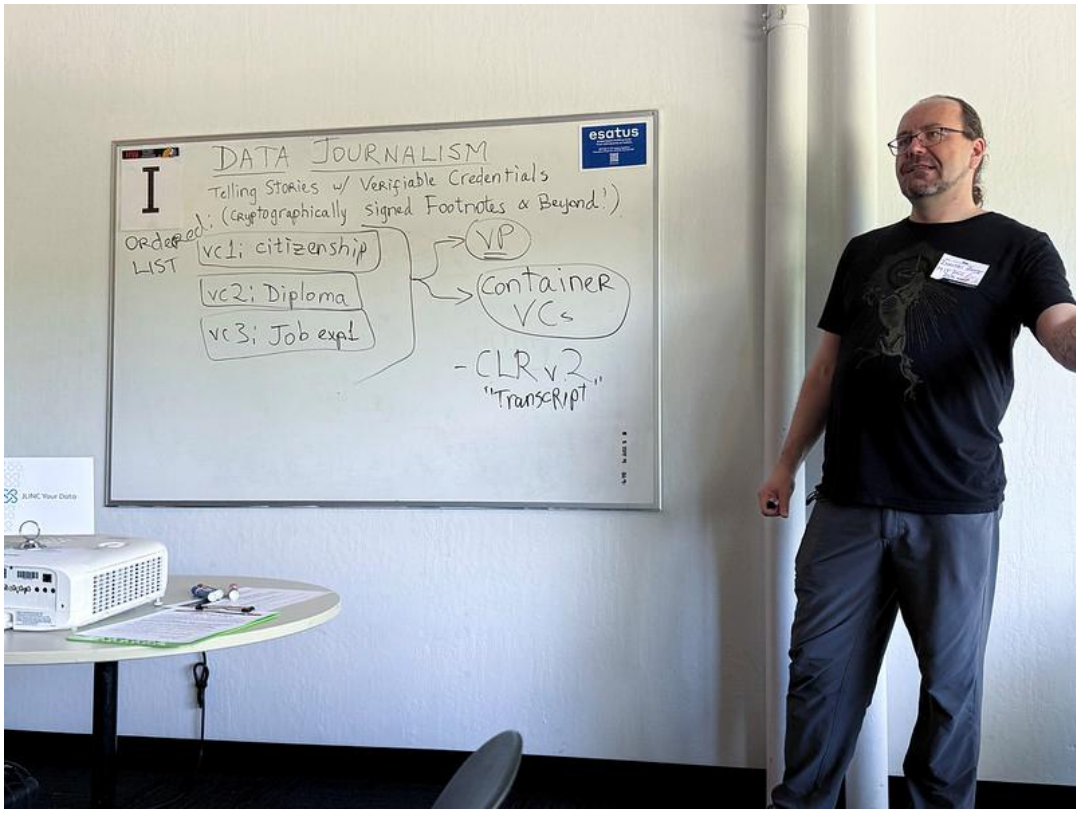
- DID Traits
- Linked VPs
- Trust Over IP High Assurance VIDs *(linking DIDs to X.509 or web domain)*

DATA Journalism -> Telling stories w/ verifiable credentials

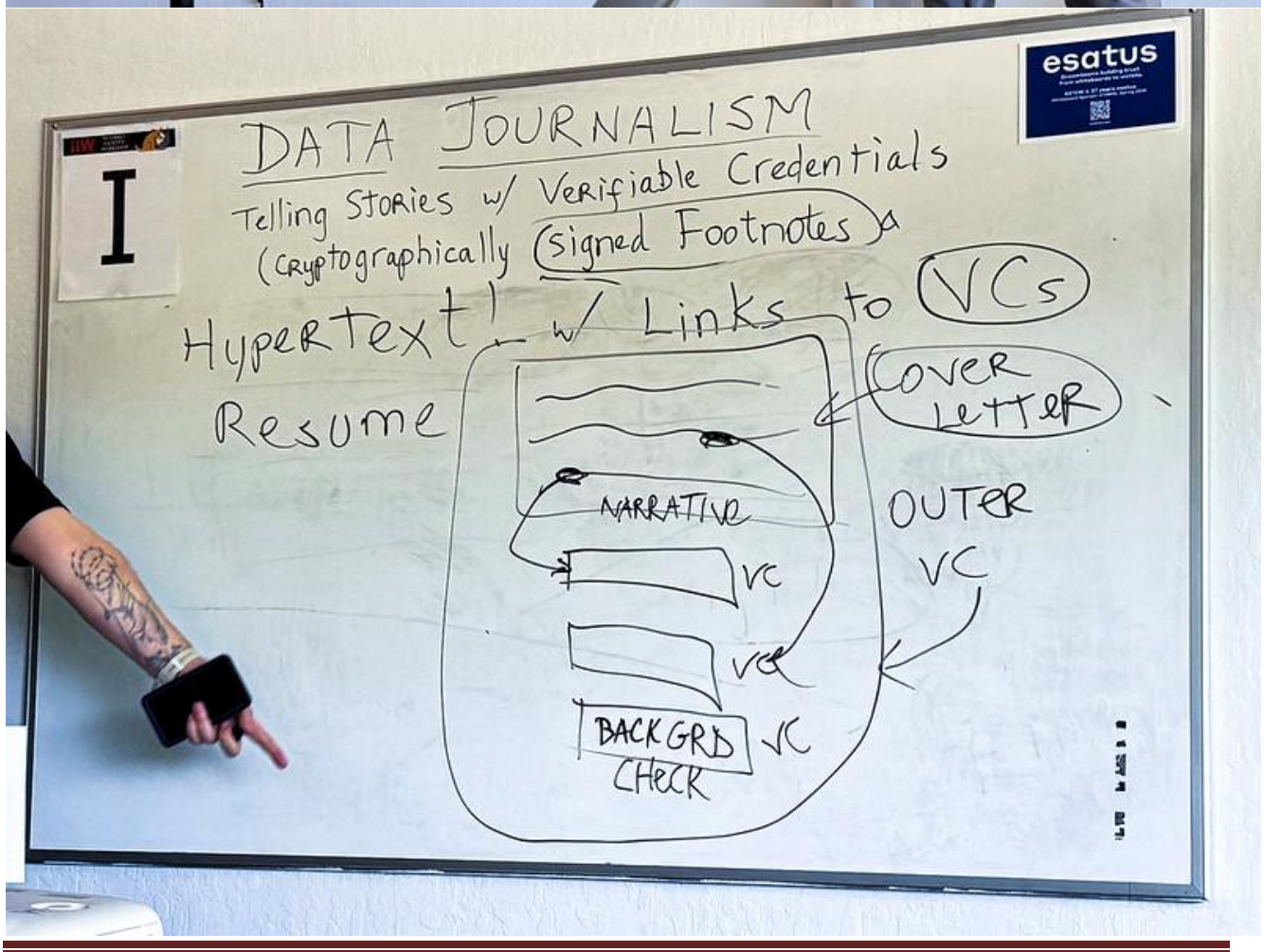
Session Convener: Dmitri Zagidulin and Phil Long
Session Notes Taker(s):

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

Thanks to Photos taken by Doc Searls and the IIW Documentation Center Team - we have some screenshots of the session. NO notes were submitted -




esatus
I
DATA JOURNALISM
Telling Stories w/ Verifiable Credentials
(Cryptographically Signed Footnotes)
Hypertext! w/ Links to VCs
It was a dark & stormy night.
VC proof of time & LOCATION


esatus
I
DATA JOURNALISM
Telling Stories w/ Verifiable Credentials
(Cryptographically Signed Footnotes)
Hypertext! w/ Links to VCs
Resume
COVER LETTER
NARRATIVE
OUTER VC
VC
VC
BACKGRD CHECK
VC

SESSION #2

Wallet Attestation

Session Convener: Paul and Christian
Session Notes Taker(s): Lukas Han

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

https://docs.google.com/presentation/d/1enx0a8fWtHnNBnuSSql2Buhal-AEiYPRWVD_CGWNCSM/edit?usp=sharing

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

Issuer have to check the wallet is okay.
how about the RP?

legal aspect of EU
—
base setup and revocation reason

credential data changes or invalid
security vuln
user revoke wallet
user revoke PID
fraud event
—
if 50 cred in wallet, if user lost wallet. 50 cred should be revoked not just wallet.
for event, Issuer need mechanism to revoke cred.
tell every issuer in ecosystem
—
what if the security event happen after the issue?

Event 1
Credential data changes / invalid
issuer revokes own cred

Event 2
security vuln

1. RP is responsible and acting
    issuer only checks during the issuance
2. issuer is responsible and acting
    live for long term

—
trust the issuer for the choosing wallet to issue a credential?
Lots of CVE in android and zerodays in chrome, we can't say we cannot trust those thing.
—-
issuer policing. we can put data in the credential

Introduction to OpenID Connect

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

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

The presentation used in the session to drive the discussion is available at https://self-issued.info/presentations/OpenID_Connect_Introduction_8-Apr-25.pptx and https://self-issued.info/presentations/OpenID_Connect_Introduction_8-Apr-25.pdf.

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

We had a very interactive discussion about OpenID Connect, its history, how we created it, its goals, and how it has progressed since originally approved in 2014.

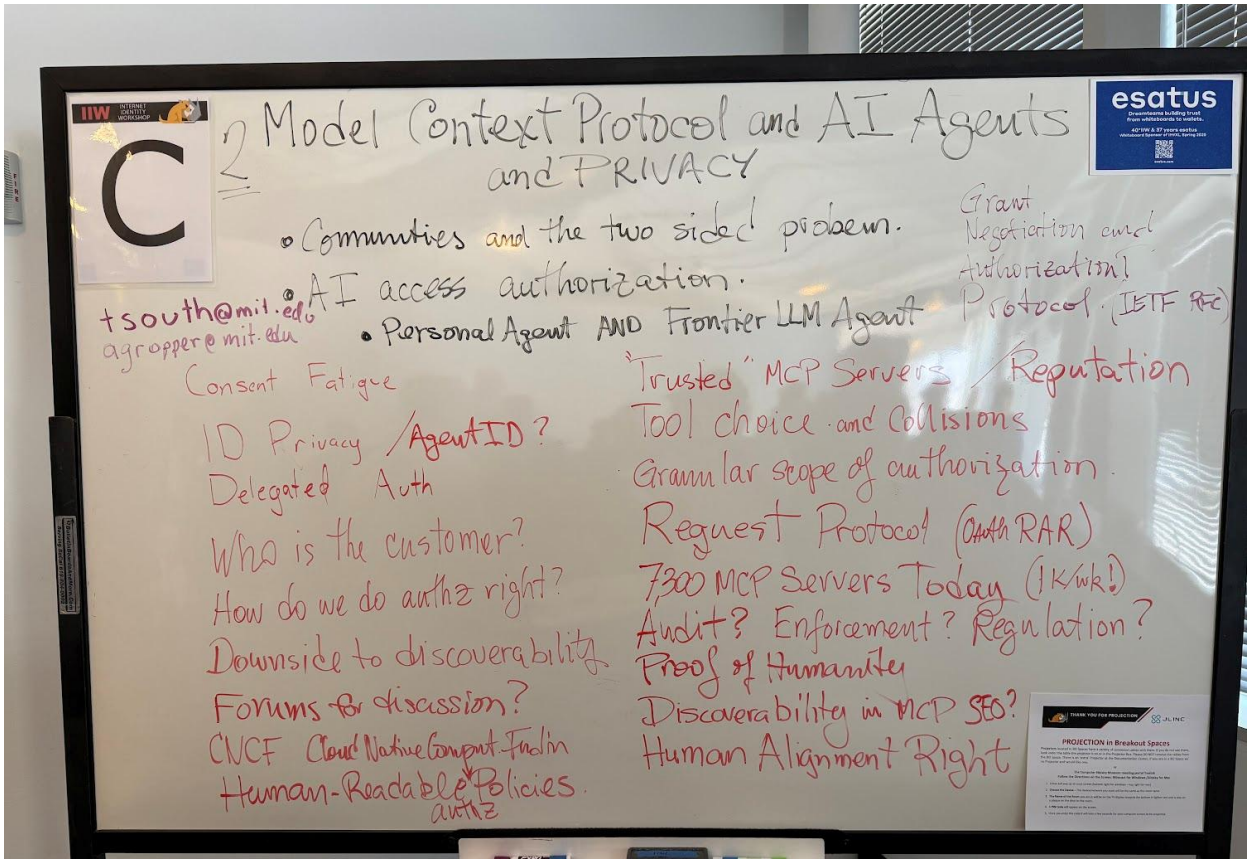
AI (agents/MCP) + Auth and Model Context Protocol and Privacy

Session Convener: Tobin South & Adrian Gropper
tsouth@mit.edu & agropper@mit.edu
Session Notes Taker(s): Colin Jaccino / Dean H. Saxe

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

Model Context Protocol
A good explanation of MCP: https://www.youtube.com/watch?v=7j_NE6Pjv-E
GNAP - https://www.rfc-editor.org/rfc/rfc9635.html
Rich Authorization Requests - https://www.rfc-editor.org/rfc/rfc9396.html
OAuth in MCP https://aaronparecki.com/2025/04/03/15/oauth-for-model-context-protocol

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



IIW: MCP Discussion

- Communities and the two-sided problem
- AI access authorization
- Things we're not talking about:
    - RAG
    - Agents (AI that takes action)

GNAP - a successor to OAUTH2
In a AI deep research comparison of MCP and GNAP, one of the first things it came up with was the problem of consent fatigue.
With AI, this is going to be 1000% worse.
Consent Fatigue

- ID Privacy
- Delegated Auth
- Who is the customer?
- How do we do authz right?
- Downside to discoverability?
- Trusted MCP Servers / Reputation
- Tool choice and collisions
- Granular scope of authorization
- Request Protocol (OAuth RAR)
- Proof of Humanity
- Discoverability in MCP SEO?

Partitioning the conversation

- MCP as a protocol. How do we do this right?
- Personal Agent AND Frontier LLM Agent

Differentiating Authorizations toward AI between the ai-enabled application being authorized and the underlying AI/LLM infrastructure
What about MCP-to-MCP-to-MCP scenario
“Nested MCP servers”
“What rights to privacy do you have toward the third party vendors that the AI agent relies on?”
What channels do I have to those vendors?
(Is this something that the legal concept of “strict liability” can be applied to?)
Concerns over highly autonomous workloads.
7300 MCP servers today (1k/week!)
Audits? Enforcement? Regulation?
CNCF - Dapr - Is this an alternative
Cloud Native Compute Foundations
Bot blocking blocks AI agents
Human-centric Web via AI-centric Web
“The right to human alignment”

- The right that you as a human have a right to choose your bot before a provider can attach a service to you
- If you want your agent to connect my personal data, first you have to make sure that I have the right to proxy that data with my agent?

Are people going to want to manage their own permission authority / personal agent?
Future session:

- How do we make policies human-understandable? And portable?
    - You (AI) have access to the emails related to my expense report

******

Dean's Notes:

- We are not talking about chat bots when we discuss AI
- RAG - pull in factual information (e.g. Gemini accessing data on the web)
    - There are access control paradigms here already
- AI taking actions on behalf of users
    - Previously called tool use
    - Now done using Model Context Protocole
    - MCP is simply a wrapper around APIs in
    - Aaron's blog: https://aaronparecki.com/2025/04/03/15/oauth-for-model-context-protocol
    - User types in "find my medical records", MCP surfaces the data for the user from data sources, but there was no authZ
    - MCP adds AuthZ recently
        - Using OAuth
- Question: Today with OAuth can I delegate claims to MCP to perform actions for me?
    - Tobin: No… yes… it changed last week
    - Lots of competing implementations
    - Discussion on the "right way" is ongoing
- Comparison of MCP vs GNAP
    - Consent fatigue is an issue with OAuth per Adrian
    - If the intent is to use OAuth, we're going to end up with consent fatigue for users
- In the shopping scenario, service providers can sell me more APIs (not sure I caught that correctly)
    - Privacy question: who owns the right to the conversation that's happening across all of these APIs?
    - Privacy problem for MCP is like the old screen scraping we saw with financial aggregators
- Tobin: Two issues
    - What's MCP and how do we do it right? MCP is blowing up, but how do we ensure it's used correctly?
    - AI and Agents are here and autonomous, how do you deal with consent fatigue? How do you deal with authZ at scale? How do you deal with privacy at scale in this environment?
- MCP protocol today has no built in authZ?
    - This is not correct today, there is recent work to implement OAuth
- Issues with MCP
    - Due to volume, it's hard to parse what's a trusted MCP server that I want to use?
    - How do you deal with namespaces in MCP? Names are used to connect to the services, name collisions are causing practical issues.
- Biggest area that is not being considered - Humans are slow and clunky. Concerned about granularity and speed and the ability to revoke access in a timely manner

    - An MCP works as a file system server, you can give it access to your underlying file system
- Tobin: Consumers DON'T CARE. They just want it to work. But because AI can do a lot fo things, we need to consider how to restrict the scope
- Fine grained authZ for AI agents? How do we establish this?
    - Need Fine grained authZ on what models remember
- UMA/GNAP allow for fine grained delegated authZ
    - GNAP https://datatracker.ietf.org/doc/rfc9635/
- Confused deputy issue - if I pass on credentials to an agent, how do we restrict access?
    - Innocuous access is not always innocuous
    - OAuth is fine for MCP, but does it have the right scope?
- Enterprise space - accessing Bloomberg, paying for a seat, how do I give access to my bot on my behalf? What about access for multiple bots?
- Number of AI agents - if a consumer has one AI agent and delegates access to many different items to the agent, how do we ensure the agent doesn't cross contexts inappropriately?
- Consumers need to use AI agents, services need to know that AI agents are accessing the services on behalf of consumers
    - How do you delegate control to the AI agent in a structured manner?
    - This matters in every context when you're using an agent
- Is it clear to consumers that the apps they use are using AI? How do we encourage transparency?
    - Operator from OpenAI gets a user session cookie and can do whatever it wants once you've provided authN credentials to the service
    - Delegated authZ is to be able to provide AND revoke access
- OAuth RAR - rich authZ requests and AI
    - These requests have to be processed, but this is expensive
    - Asks the question how to encode policies into personal agents (e.g. compiled from source)? How do you encode this into models run by a third party?
- MCP registry is growing by 1000+ servers a week
- MCP servers now talk to each other, so there's a potential for a supply chain attack with a bad actor standing up a MCP server
- Transparency - What's logged? How does a user discover the chain of MCP servers that are being used?
- What privacy rights does a user have if the agent shops for you on a site? Can the site obtain user information from the agent to contact the end user? Can the agent agree to a vendor's terms of service on my behalf?
- At some point, we'll collapse into a centralized set of MCP servers rather than the current growth that we're seeing. So how do I trust 2 - 3 authorities that deploy "root" MCPs?
- Tobin is very worried about autonomous workloads and the impact of that
- Where is the latest discussion happening on MCP and related concepts?
    - Twitter
    - RSS
    - Very rapidly evolving state, so it's hard to follow everything
- Tobin is writing a whitepaper with the OpenID Foundation about these issues

- Can we use a standards body? Doubtful
- MCP is not the only mechanism, Dapper AI agents from CNCF also exists
- NIST is going to start an AI working group, seeking input
- Tobin: We need
    - Identification of agents
    - Authentication of agents
    - Authorization of agents
- Conformance: How do you differentiate good vs bad bots?
- IETF bot auth mailing list came out of the bot auth side meeting at IETF122
- Adrian suggests that you cannot regulate the tool, only regulate the use of the tool
- Stanford workshop today on regulating AI agents
- Tobin: Many of the use cases already have regulation frameworks (e.g. in the financial context).
    - Delegation simplifies liability questions
    - We have the tools we need, we need to package them up for AI
- Is there discoverability of a service from an MCP?
    - MCP explicitly has discoverability
    - Startups are wrapping this to become the Amazon marketplace
- How do Agents deal with CAPTCHA? This is the issue that the IETF bot auth work is focusing on
- How will bots access services?
    - Today access the human centric web, UI and all
    - Models either screenshot the site or process the DOM to pull out the text
    - Not every service has an API, so using the "human centric web" is a requirement today
- Will we build a reputation system for bots?
    - Tobin says this is an alignment problem to not make bots dumb
    - Also includes the issue of access controls which we have to build
- How do we prevent bots from DDoSing sites?
- How do we give an agent an identity?
- We need monitoring for the real world uses of bots. We don't know what audit controls look like for bots.
- Are there any carveouts in the regulatory space for AI?
    - EU regulates use cases and models
    - AI models must be identified
    - Carveouts for when a human must be in the loop of the agent's work
- Adrian: Human alignment in AI
    - As a human, you have a right to pick your particular AI agent
    - This is a new privacy right for how access is granted/managed?
- How do we create human understandable policies for delegation?
    - AI interpretation of natural language policies
- Email Tobin if you have information to share or want to chat tsouth@mit.edu
- Adrian - agropper@mit.edu
- Stanford WG with Consumer Reports is building this out
    - Mailing list access - -email Tobin

Registry of registries. Verifiable Public registries and related business models for issuing and verifying credentials

Session Convener: Fabrice Rochette
Session Notes Taker(s): Ariel Gentile

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

https://verana-labs.github.io/verifiable-trust-vpr-spec/
https://drive.google.com/file/d/1z6i7Nrby0FGz9fqPftuyOgThhPxt9-yg

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

Credential Schema Permissions: a model that Trust Registries to define rules to issue and/or verify credentials of a certain type, establishing fees for issuance and verification.

Each participant follows a Validation process where permission grantors are involved.

Are there factors of spam? Trust registry can be created, but as it needs a trust deposit, it will become expensive.

This can be used for trust resolution and build reputation based on deposit and number of credentials issued, verified, etc.

A DID Directory can be created based on crawlers in a decentralized manner.

Inside eID Integration: The Good, The Bad, The Ugly

Session Convener: Bart van der Geest (Head of Compliance, Hopae) & Jungmin Moon (Sr. Software Engineer, Hopae)

Session Notes Taker(s):

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

Intro

There are 150+ different eIDs worldwide, with rapid growth (19+ mobile driver's licenses in the US alone)
However, despite growing numbers, eIDs remain "country-locked islands" with:

- Different rules, structures, and capabilities
- No cross-border interoperability
- Complex integration requirements

This fragmentation creates significant barriers for global businesses needing to verify users internationally. In this session, we share our experiences, challenges and frustrations with integrating eIDs.

eID Integration Process

To integrate an eID, the process follows four steps:

1. **Research**: Understanding eID capabilities, user base, validity
2. **Compliance**: Preparing for integration (most eIDs exist in closed ecosystems)
3. **Technical Integration**: Connecting to development environments, testing
4. **Production Deployment**: Setting up live connections

Reality: There is no standardized approach across eIDs. Integration processes vary widely, requiring:

- Simultaneous work between technical and compliance teams
- Frequent iteration between steps
- Adapting to different integration sequences (e.g., Italy's SPID requires technical integration before administrative steps)
- Adapting and reacting to unexpected roadblocks along the way

Case Studies

1. Swedish BankID

- One of the largest Digital ID schemes in the Nordics (8.5M users)
- **Key Challenge**: Access restricted to existing customers of Swedish banks

- Requires either direct bank agreement or use of approved resellers

2. US Mobile Driver's Licenses (mDL)

- Growing interest in online verification capability
- Most state mDL apps designed primarily for in-person verification
- **Integration Challenge**: Each major wallet platform has different requirements:
    - **Apple Wallet**: Limited web verification support, restricted to specific industries
    - **Google Wallet**: Uses latest standards but with limited browser support
    - **Samsung Wallet**: Requires proprietary SDK/API with complex documentation
- Result: RPs must implement multiple technical approaches
- Development time often 2× longer than expected due to documentation issues

3. Swiss eID (Swiyu)

- Recently released in public beta
- **Integration Success Factors**:
    - Open-source verification server
    - Clear documentation and developer guides
    - Developer-friendly tools (Docker images, Swagger UI)
    - Responsive support

Key Learnings

1. Every eID integration looks different
2. Not all eIDs are available or support remote verification
3. Integration timelines can vary greatly
4. Relationships are very powerful
5. Open-source is very powerful
6. Sharing feedback and struggles is helpful for Devs

Delegatable, Revocable Authorization Capabilities Who is doing it? How?

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

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

NO NOTES SUBMITTED

Introduction to Ayra and the First Person Project

Session Convener: Drummond Reed, Darrell O'Donnell
Session Notes Taker(s): Drummond Reed

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

First Darrell O'Donnell, Executive Director of the Ayra Association, gave this introduction to Ayra as a global trust registry fabric to connect digital trust ecosystems.

Then Drummond Reed gave this introduction to the First Person Project (through slide 62), of which the highlight was showing how people can form digital trust relationship using verifiable relationship credentials (VRCs), which are a way of implementing "the ultimate instant key signing party" (46 and 47) and to r-cards (relationship cards — slide 61).

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

All the key points are summarized in the linked slides.

This session set the stage for the demo of VRCS in session #4.

There will be follow-up sessions on the second half of the First Person Project presentation on Wednesday and Thursday.

Preserving Liberty in an Age of Gov't ID

Session Convener: Timothy Ruff and Joe A
Session Notes Taker(s): Alyssa Morgan

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:

preserving liberty in an age of government ID

important difference: private industry goal is to make money. gov't id goal: ??? various things
gov't overreach/gaining ability to track citizens could have massively bad implications

mobile drivers license is fundamentally flawed (5 mins in)

gov't getting into dig id and gaining ability to surveil gets them closer to surveilling/getting more info on citizens- and they WILL use that power and access

- already happening in certain places- (happening in china rn?)
- cultural differences- in the US, surveillance works because it's assumed to not be happening, in china there's assumes surveillance

thesis: how do we bind the gov't to protect privacy

credentials vs identifiers

- issue: reliance on drivers license to prove personhood- not what it's meant for (esp bc they're revocable and not everyone has one)
- who can access revocation status of drivers license? should they be able to?

data brokers- get around the proper channels of data collection
asymmetric cryptography

liberty vs privacy:

- privacy companies can't protect liberty. the gov't **can**

phone home and preserving liberty:
2 parts to surveillance: knowing who's doing something and knowing who they're doing it with
ex: liquor store: if you know who went to the store but dont know who, you don't know enough. if you know someone bob went somewhere but you don't know where, you also don't know enough. once you have both pieces, you can start connecting dots and surveil (asking what time, how long, infer about what for…)
there are ways to blind that information but they're not doing that
they can dip into databases and check for things like double checking that it actually *was* bob- all those deeper dives

how ro break liberty threat? break one or both of those elements. either not know it was bob or not know it was the liquor store. preferably both

threat of action- (opinion) the threat moves from privacy to threat to liberty when theres ACTION
[speaker] argues that there's already action right now, and that the possibility (slippery slope) is enough to act and protect ourselves
ex: tufts student detainment, and anti palestinian activist detainment across the country

move from dig id to gov't id. it's happening across the world. they might not immediately move to nefarious action and surveillance but it can (and likely will) happen
we ([cyber]security professionals) are the defensive line against that capability . once they have the power they will NOT Let It Go. gov't doesn't shrink. it increases its sphere of influence.
imagine the value to gov't of knowing what dig citizens do at all/any times.

another side of this: data fusion!! even if we solve the (phone home?) problem, there's still the problem of data fusion
group privacy: (book by dr. lynette taylor)

deference to state risks liberty! the more we use dig id as a form of id, the more people will ask for it and the more it will be used

SESSION #3

Relying Party AuthN and AuthZ EUDIW

Session Convener: Mirko Mollik
Session Notes Taker(s): Lukas Han

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

Link to presentation

wallet relying party

- issuer
- verifier
- pseudonym login
- transaction authZ

= everything that interacts with EUDI wallet

There is no statements in the law, EUDIW can only interact with registered RP or not
—
AuthN

issuer's certificate , wallet get pub key from registar and check the signitrue
RP is registered in what member state they based.
—
For AuthN
format: x509
(member state) - (RP certiciate)

registration cert
format JWT
overasking = not good
same = okay
under asking = okay
-
it's a machine readable version of privacy policy
—
AuthZ

- no policy
- allow list
- root of trust (only member state)

—
overask, unauthorized request can be overruled by user.
intermediary is allowed by eIDAS

Authorization 101 - The 'AM' in IAM (an IIW 101 Session)

Session Convener: Steve Venema, Microsoft
Session Notes Taker(s):

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

Slides (pdf)

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

Slides were presented with interactive Q&A

~15min remaining for discussion after the presentation.

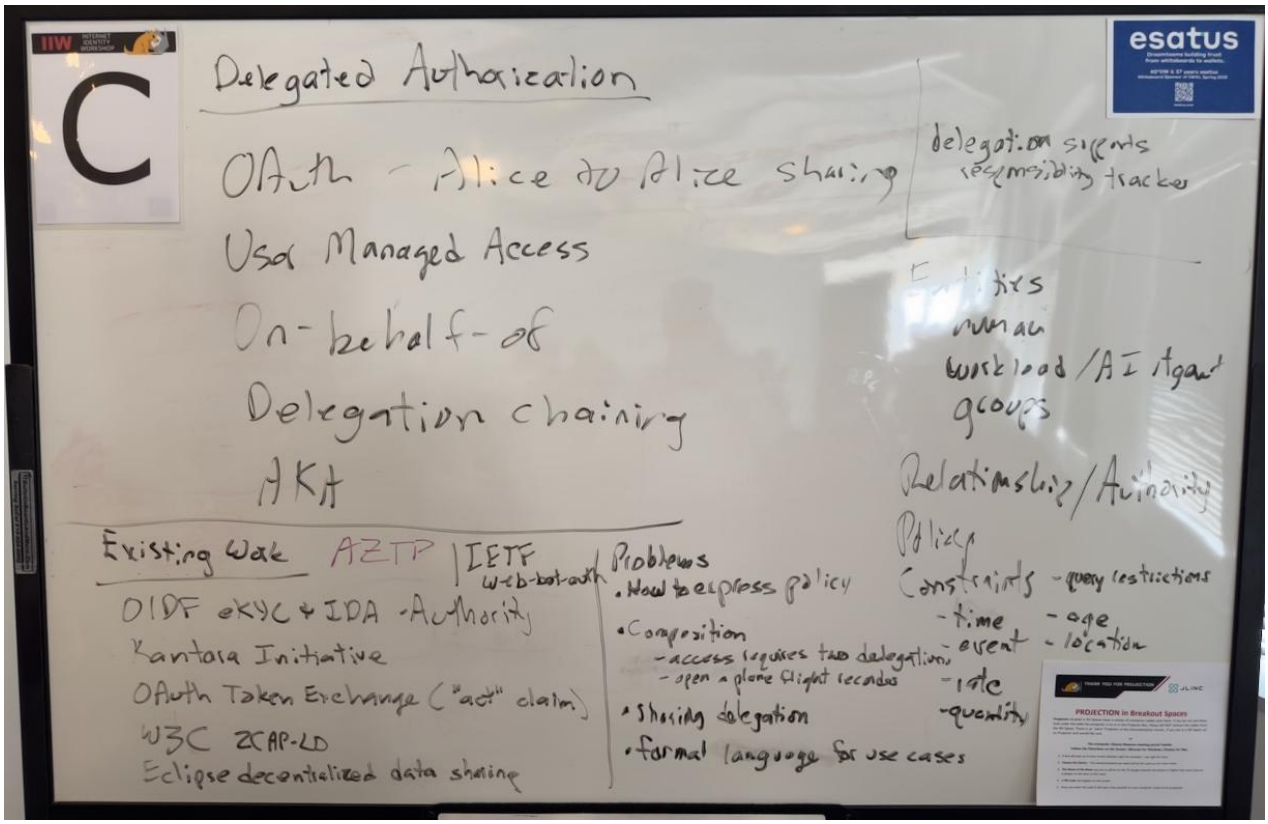
Discussion mostly focused on how to organize large policy sets. A few ideas included:

- Organize policies into a hierarchical decision tree so that each step in the policy list eliminates large sections of the tree from having to be evaluated.
- Parallelize evaluation – horizontal scaling
- Organize policy into modules that partial policy decisions and then link them together for evaluation with a particular use case

Delegated Authorization

Session Convener: George Fletcher & Dean Saxe
Session Notes Taker(s): D Venkatasubramanian

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:

Motivation : Use cases such as how do we deal with cases like death of an individual and how to have a delegate. Additionally, use cases where an agent is running on a website, to determine when a non-human is interaction.

What is standard OAuth? The delegation to a software from a human with some form of authorization. Classic OAuth represents single step authorization.

Started out with OAuth - Alice to Alice sharing. Where a person is authorizing access to themselves for certain use cases.
User Managed Access - Evolved into Alice to Bob sharing, where an entity is authorizing another entity for limited access.

On-behalf-of - One entity is delegating access to another entity to act as the first entity in an official capacity (e.g. a customer care agent performing some task on -behalf-of the caller).

Use case 1)

_____

Discuss a use case : My kid is going to a camp. During the camp, I would like to delegate authority to the camp, where my kid is participating, to be able to take the kid to the hospital if the need arises. The camp is going to delegate to a human who is incharge of the camp.
This is delegation chaining use case where a human delegates to an entity which in turn delegates to another human, based on a relationship.
I am authorizing an entity, which is authorizing its employee.

_____

There is a difference between on-behalf-of and delegation chaining, and they are not the same.

Use case for on-behalf-of - A user interacts with a customer care, and the agent takes some actions on your account on your behalf.

We also discussed personas :
Jen's persona as Jen Corporation
Jen's persona as an individual.
Jen known by different names, using maiden name vs married name

The same entity may have different names, or representations, representing different personas.

When we start adding AI into the mix, this would further add more dimensions.

There are a few different classes on this model.

The first one are the entities and delegation :

1) Human
2) Workload
3) Groups

Then their interactions involve :
1) Relationships
2) Policy
3) Constraints
- time
- age
- event
- location

Relationships / Authority

Some of the discussion areas :
2) How to express policy
3) Composition
- access requires two delegations
4) How to Share delegation
5) Formal language for expressing different use cases

Some of the organizations and initiatives exploring solutions for these are :

OIDF eKYA and IDA - Authority
Kantara Initiative
OAuth Token Exchange ("act" claim)
W3C ZCAP-LD
Eclipse decentralized data sharing
AZTP
IETF / web-bot-auth (Birds of a feather session) - opt in header of a bot

Use Case 2)

_____

Lets discuss a somewhat complicated example :

I have a daughter who is under 13 years old.
As a minor below 13 years of age, most of the delegation is to me as a parent.
Once she attains the age of 13, I should no longer have access to her medical records. I am still the delegate for any payments etc.
Once she attains the age of 18, I am no longer delegate on other stuff such as payments.

_____

So, even though there is delegation, the scope of delegation changes on different trigger actions.

Use Case 3)

_____

Another use case is : When a person dies, the domain names may pass to a delegate.

_____

Trigger actions could be based on age, location, death etc.
No policy language exists that can model this kind of delegation.

Use Case 4)

_____

Lets discuss another use case :

I want to delegate my son to go to Costco (Retail club), and buy or pickup specific items. When returning, my son notices that we are out of gas, and would like to fill up, using my credit card. I am fine with this use case.

But when an AI agent is interaction, I dont want to allow the AI agent to be able to go beyond its remit.

_____

There is a need to understand and code reasonableness into the system.

How do you represent reasonableness in online systems, similar to an offline space?

Yesterday in the OIDF Workshop, there was a panel discussion on AI where this concept of fuzziness or reasonableness came up. This is something we need to account for in the context of humans defining authorization policy.

Alan Karp mentioned : We can only request not to re-delegate, but it is not possible to enforce.

How do we define :
1) Relationships between entities
2) Policies connected to the relationships

How do we package all this, possibly embedding policy (e.g. Cedar) inside JSON object

Use Case 5)

_____

Audience Member mentioned that at the OAuth Security Workshop, one of the audience members from Norway talked about a use casse :

A person needs immediate medical attention. An ambulance arrive and needs access to the person's medical records.
What kind of authorization can be available when the person cannot consent.

_____

We need to figure out the boundaries of the areas that has already been solved and areas that still needs investment

Use Case 6)

_____

I want to allow software to be able to read my emails for specific purposes. But I dont want the agent to read my emails related to Password Reset and click the reset link on my behalf.
Read only access, but how do we restrict password reset emails.
Most systems allow full access to the inbox, and there is very little protection.
Giving access to some threads instead of full mailbox access

_____

In these use cases, OAuth scopes will not work.

Mike (gluu) mentioned : How to Share data - delegation of access for certain types of data

Audience member : Delegating an action along with the query. I am going to delegate only if the request is for this query
This is similar to OAuth with Rich Authorization Requests

Jen mentioned : How different delegations work together. Can you mix two different permissions to do one task.

George discussed on :
Transaction Tokens - Once the transaction has commenced, we want it to complete.
Can the lifetime of the transaction tokens be more than the lifetime of the access token.
The topic of Transaction Tokens was pushed to another session.

Use Case 7)

_____

To Open a plane flight recorder, we need
- Airline
- Airline contractor
- Pilots union

_____

This is Quorum based authorization.

There are also tokens created to allow access for a trigger event, but the entities that are need that do not exist.

For e-g- Power of Attorney : The token hasnt changed

Use Case 8)

_____

Bank accounts have Pay on Death - Give a death certificate - No access until death certificate is presented.

_____

Use Case 9)

_____

How do you share delegation - In my will, I want to pass on my assets to my kid when I die. But the kid gets access to all the assets only when they attain a certain age.
For the delegation, first I would have to die and also the kid should have attained a certain age.

_____

So, this is based on triggers.

But in the case of the retail club run, there may be delegation but no triggers.

Use Case 10)

_____

What happens when you share your credentials with another person.

_____

If credentials are shared, we know who is responsible, but we do not know who did it.
The system cannot prevent credential sharing

We could share credentials, or you could get access to a group resource, such a family subscription.
Delegation is different from impersonation.

Rohit mentioned : Agents work for me, but bots are bad. What motives do we ascribe for this?

What is the identity of the agent, what is the identity of the person the user is part of.

Use Case 11)

_____

My company has a policy who can access resources of another company, but the other company does not know my policies. There are ways to do this using tokens and policies. So, the receiving entity may fallback and ask that the policy checks are run from the source to provide go ahead.

_____

Conclusion :
Bringing in an arbitrary policy language would be difficult, but formalizing a system is way harder.
Its better to have a broader definition.
We dont even have the language that can encompass all this.

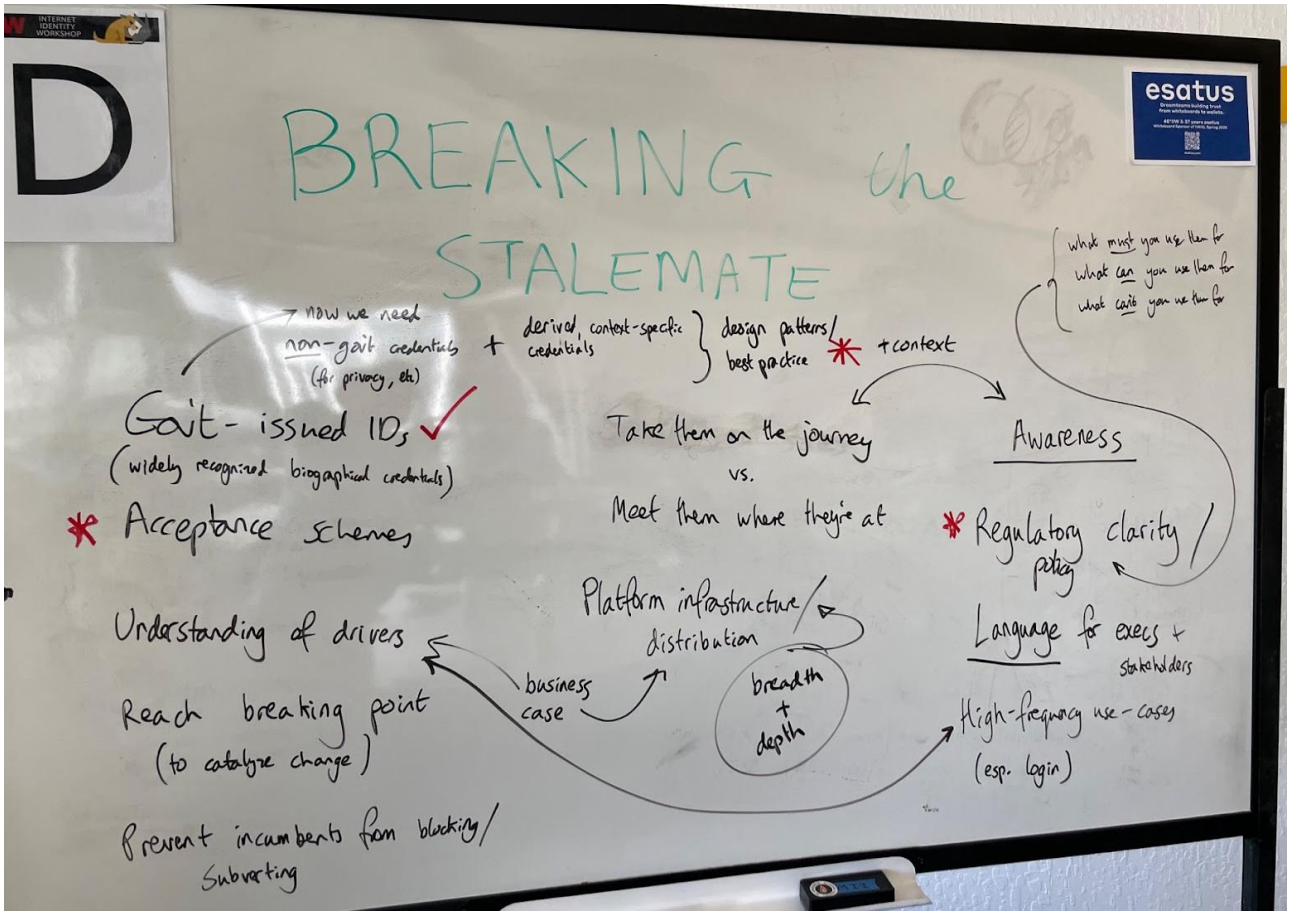
We need more discussions and hope to discuss further.

Thank you for attending.

Breaking the Stalemate: Top 3 Blockers

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

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



Question:
We are moving towards a world where 100s of millions of government-issued standards-based digital ID credentials will be available in citizen-controlled wallets. It may not be as self-sovereign as some have wished for, but nonetheless, the question of "how do we get issuers to the table" is at least partially answered by governments stepping up. So what are the *next* most critical blockers to widespread adoption?

Brainstorm:
See photo of whiteboard above

Top 3 blockers:

1. Regulatory clarity & policy
2. Design patterns & best practices (particularly around high-frequency use cases)
3. Acceptance schemes

Mastodon + FedID

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

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

https://fedid.me
https://mastodon.social

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

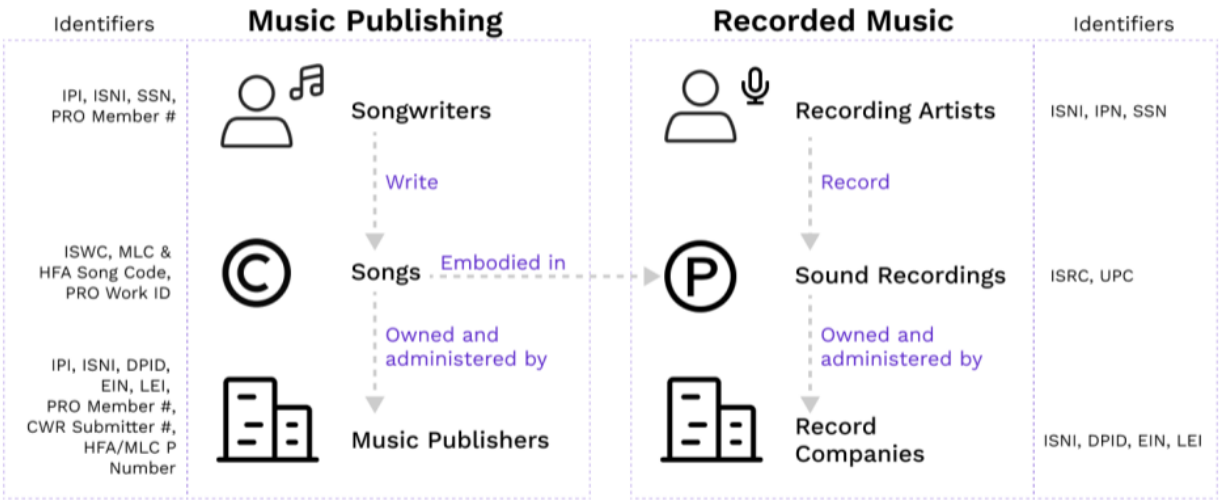
Discussion occurred around how federated DIDs could be used to support ActivityPub in much the same way AT Proto is used today. Future consideration around the benefits of distributed identifiers vs those of non-distributed identifiers was had, along with options to consider for the most efficient ways to implement distributed identity with ActivityPub.

Switchchord + did:webs for vLEI

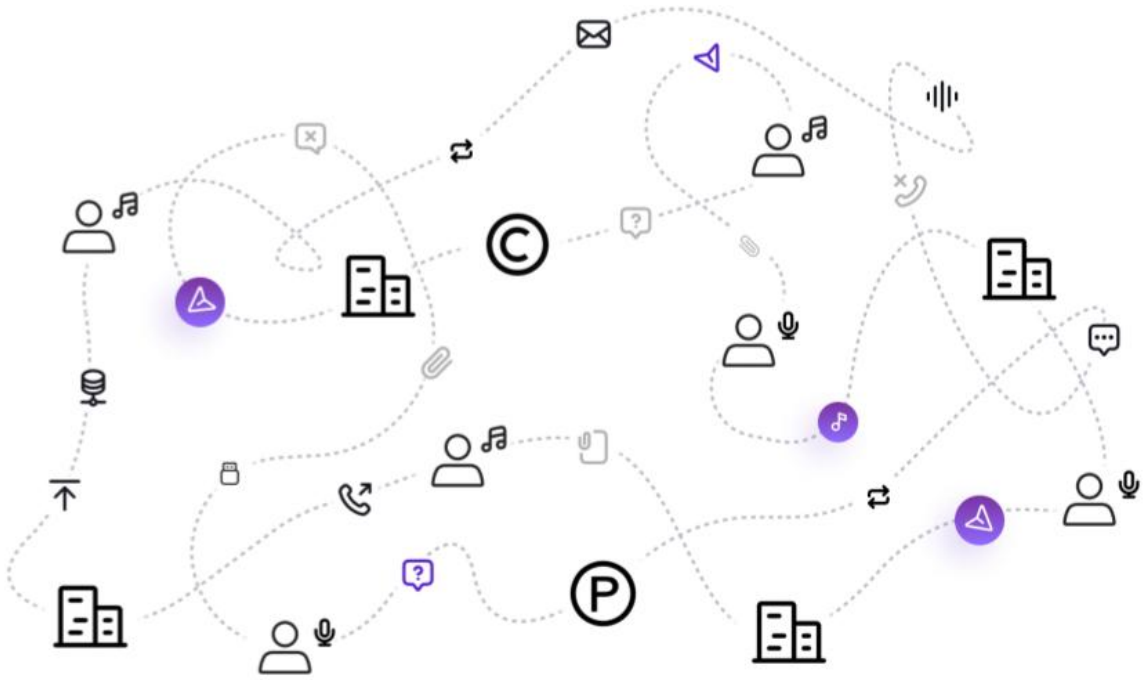
Session Convener: Cole Davis, Lance Byrd, Jonathan Rayback
Session Notes Taker(s): Jonathan Rayback

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

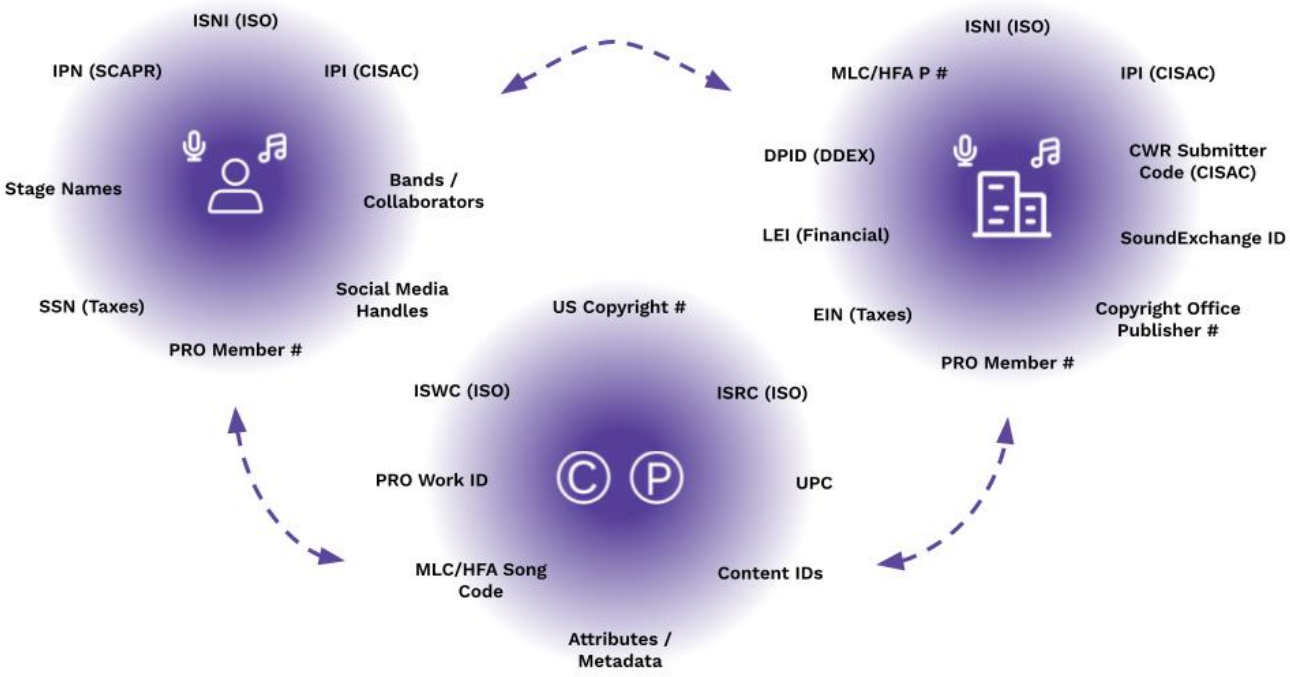
To	Person Person Person
Cc	Person
Bcc	Person
Subject	

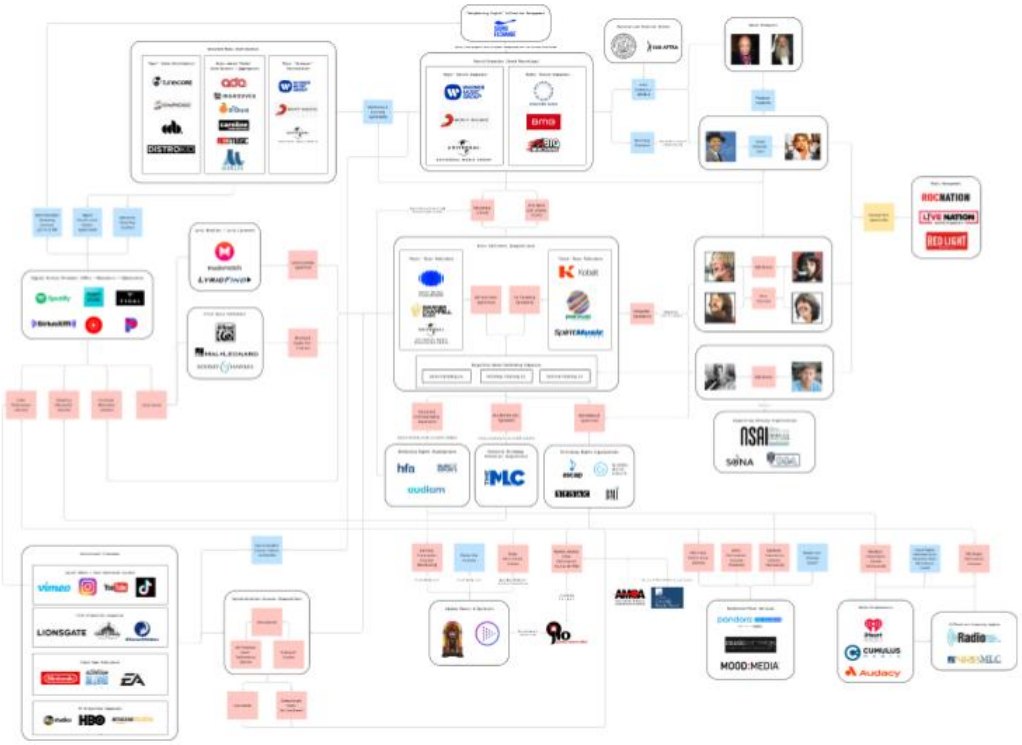

Identifiers
Music Publishing
Recorded Music
Identifiers
IPI, ISNI, SSN, PRO Member #
Songwriters
Write
Recording Artists
Record
ISNI, IPN, SSN
ISWC, MLC & HFA Song Code, PRO Work ID
Songs
Embodied in
Sound Recordings
ISRC, UPC
Owned and administered by
Owned and administered by
IPI, ISNI, DPID, EIN, LEI, PRO Member #, CWR Submitter #, HFA/MLC P Number
Music Publishers
Record Companies
ISNI, DPID, EIN, LEI

2



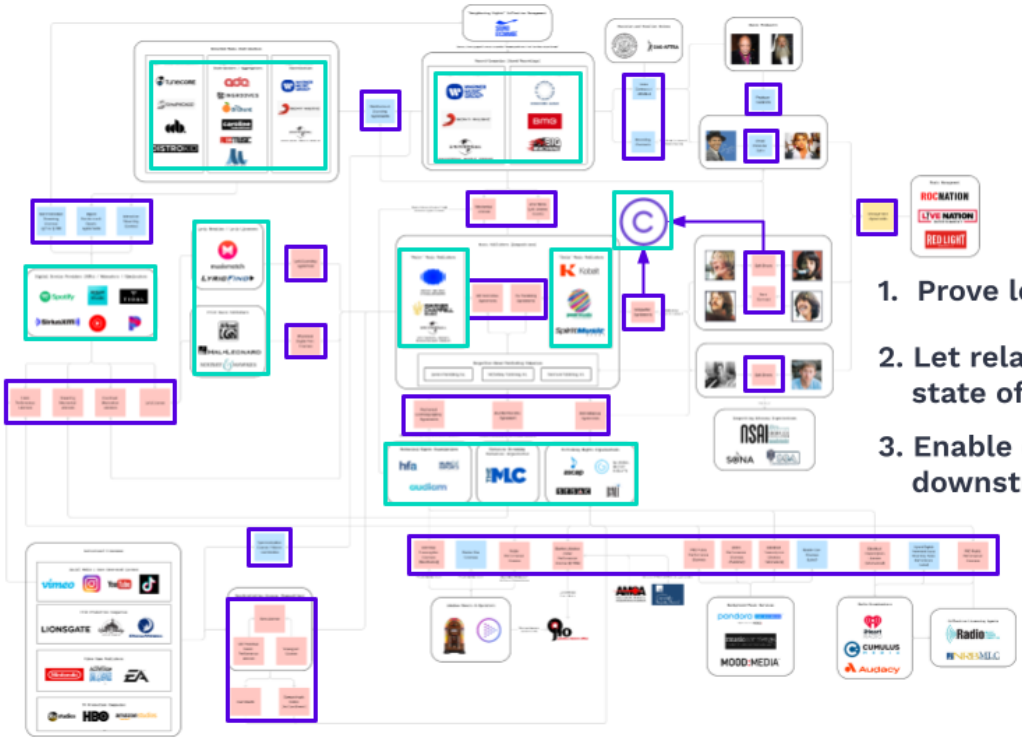

Curve
Synchtank
OpenPlay
Simply Royalties
RYTEBOX
Vistex
That Green Thing
REPRTOIR
DISCO
monday.com
Airtable
zapier
The Orchard
ada
tuneCORE
Virgin Music
FUGA
SYMPHONIC
ALLTRACK
ascap
BMI
SESAC
GLOBAL MUSIC RIGHTS
THE MLC
SOUND EXCHANGE
The Verge / Tech / Reviews / Science / Entertainment
Metadata is the biggest little problem plaguing the music industry
It's a crisis that has left, by so
unpaid to musicians
Data issues are at the heart of half a billion pounds a year of unallocated or misallocated streaming royalties for songwriters and rightsholders
The Ivors Academyhas published a new report estimating the size of the global song streaming data gap – streaming royalties for songs that are unallocated or misallocated due to missing or incomplete data.
billboard
How Hits by Drake, Ye & More Get Released Before Songwriter Pay Splits Are Settled
Billboard explains the common practice of songwriters' exact owne
getting figured out months after the work is publicly released.
THE WALL STREET JOURNAL.
Who Really Wrote Your Favorite Song? It's Complicated
From Bob Dylan to Shakira, music catalogs are selling for big bucks, but songwriters increasingly struggle to get paid. Here's why.
DIGITAL MUSIC NEWS
Warner Music CEO Says Metadata Problems Make the Industry More Vulnerable to AI — 'It Takes the Teeth Out of Things'
billboard
MARKET WATCH
MUSIC INDUSTRY EVENTS CALENDAR
PRO CHARTS
ACCOUNT
The MLC's Kris Ahrend on $1B in Payouts, 'Illuminating' Black Box Royalties & More
Bloomberg
Subscribe
Opinion | Lionel Laurent, Columnist
Fix the Spotify Economy Before Worrying About AI: Lionel Laurent
Unallocated royalties highlight the music industr
April 27, 2023 at 11:00 PM CDT
billboard
MARKET WATCH
MUSIC INDUSTRY EVENTS CALENDAR
Brick By Brick: How Companies Are Chipping Away at Music's Big Data Problem
Awkward or not, the nitty-gritty details of writing and recording songs, and the metac
behind that work, are all a big part of one of the music industry's biggest headaches.
DIGITAL MUSIC NEWS
CATEGORIES
DMN PRO
EVENTS
SYNC NEWS
JOBS LISTINGS
Mechanical Licensing Collective (MLC) 'Unmatched Royalties' Approached $562 Million in 2021, Documents Reveal


ISNI (ISO)
IPN (SCAPR)
IPI (CISAC)
Stage Names
Bands / Collaborators
SSN (Taxes)
Social Media Handles
PRO Member #
ISNI (ISO)
MLC/HFA P #
IPI (CISAC)
DPID (DDEX)
CWR Submitter Code (CISAC)
LEI (Financial)
SoundExchange ID
EIN (Taxes)
Copyright Office Publisher #
PRO Member #
US Copyright #
ISWC (ISO)
ISRC (ISO)
PRO Work ID
UPC
MLC/HFA Song Code
Content IDs
Attributes / Metadata

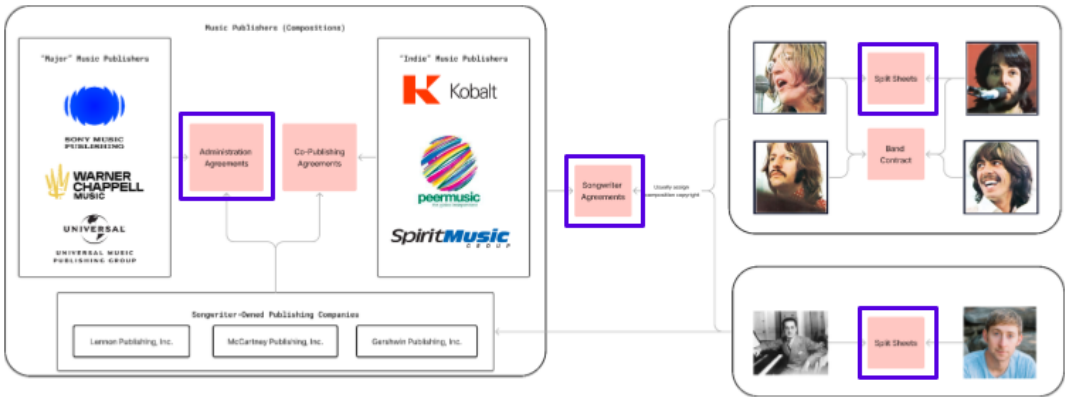


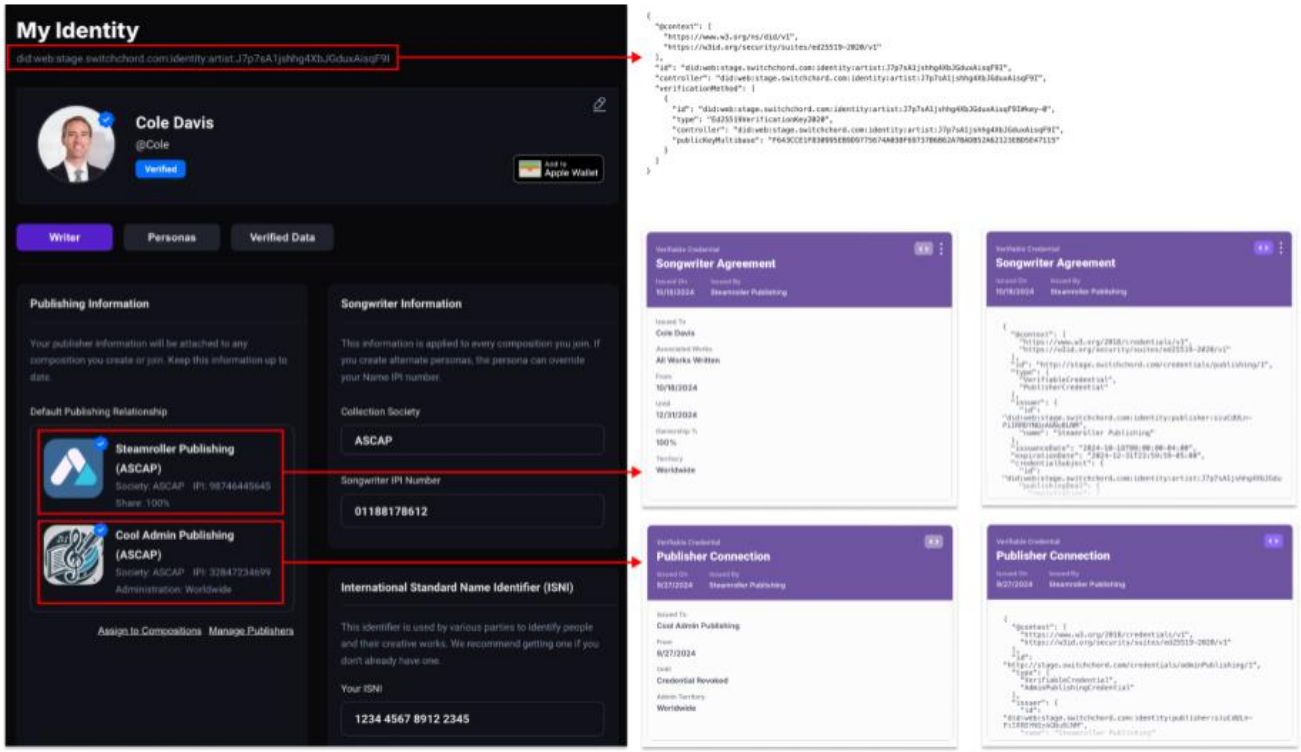

Theory
Reality
Legal
Identity
Legal
Identity

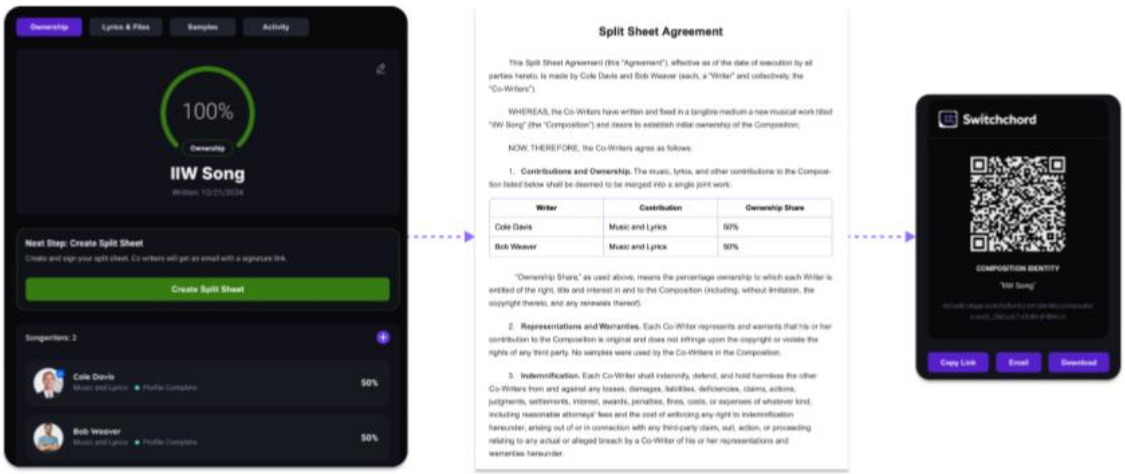

Music Identity
Authentication
Are you who you say you are?
Legal Authority
Authorization
Can you do what you say you can do?



Case Study: Switchchord




My Identity
did:web:stage.switchchord.com:identity:artist:J7p7sA1jshhg4XbJGduxAisqF9I
Cole Davis
@Cole
Verified
Add to Apple Wallet
Writer
Personas
Verified Data
Publishing Information
Your publisher information will be attached to any composition you create or join. Keep this information up to date.
Default Publishing Relationship
Steamroller Publishing (ASCAP)
Society: ASCAP IPI: 98746445645
Share: 100%
Cool Admin Publishing (ASCAP)
Society: ASCAP IPI: 328472346699
Administration: Worldwide
Assign to Compositions
Manage Publishers
Songwriter Information
This information is applied to every composition you join. If you create alternate personas, the persona can override your Name IPI number.
Collection Society
ASCAP
Songwriter IPI Number
01188178612
International Standard Name Identifier (ISNI)
This identifier is used by various parties to identify people and their creative works. We recommend getting one if you don't already have one.
Your ISNI
1234 4567 8912 2345
Songwriter Agreement
Cole Davis
All Works Written
10/18/2024
12/31/2024
100%
Worldwide
Publisher Connection
Cool Admin Publishing
9/27/2024
Credential Revoked
Worldwide


Ownership
Lyrics & Files
Samples
Activity
100%
IIW Song
Next Step: Create Split Sheet
Create Split Sheet
Songwriters: 2
Cole Davis
50%
Bob Weaver
50%
Split Sheet Agreement
Writer
Contribution
Ownership Share
Cole Davis
Music and Lyrics
50%
Bob Weaver
Music and Lyrics
50%
Switchchord
COMPOSITION IDENTITY
'IIW Song'
Copy Link
Email
Download

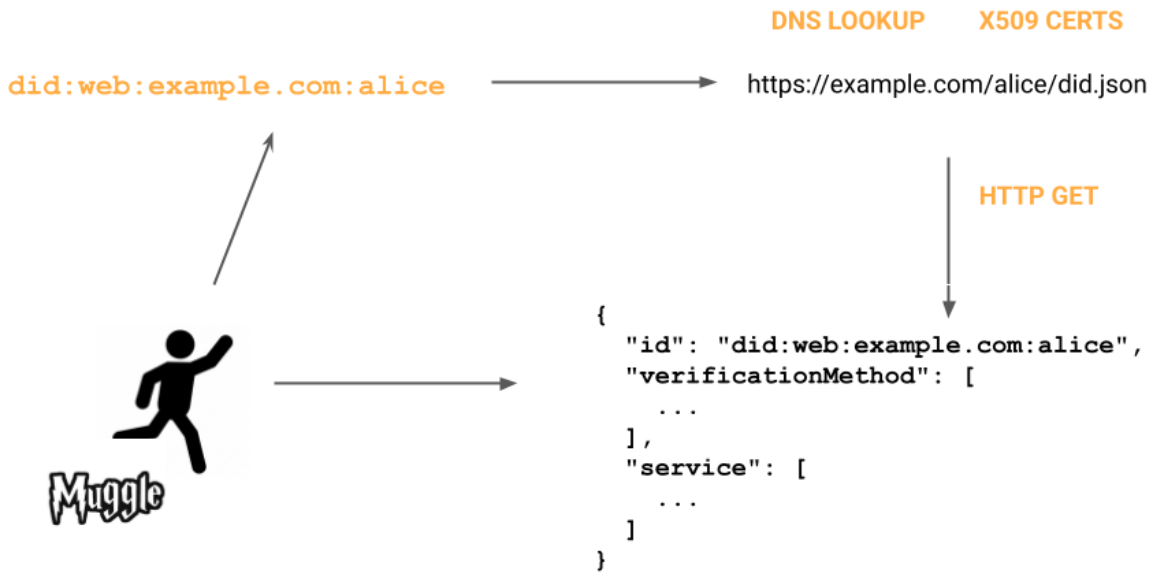
did:webs in Seven Easy Steps

#1: did:web is familiar

Benefit #1

did:webs identifiers are fully backwards compatible to **did:web** identifiers

#2: did:web trusts the web

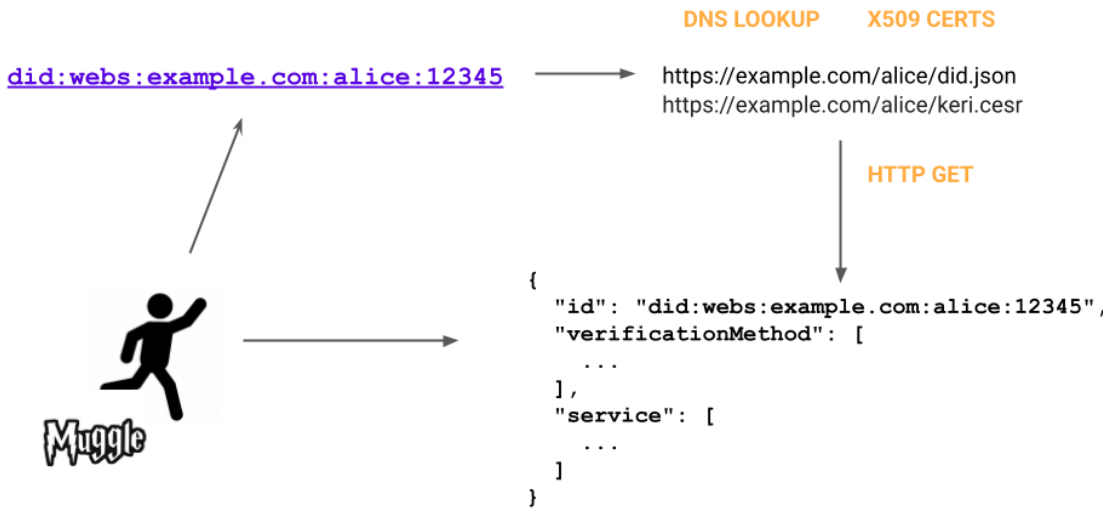


Benefit #2

did:web inherits all the strengths and weaknesses of the web

did:webs leverages the strengths but also fixes the weaknesses

#3: did:web and did:webs are familiar



Benefit #3

did:webs applies KERI from the point-of-view of the web and DIDs

You can start using did:webs without knowing all of KERI

#4: did:webs trusts cryptography

The identifier syntax is just like in did:web

```
did:webs:peacekeeper.github.io:did-webs-iiw37-tutorial:
EKYGGh-FtAphGmSZbsuBs_t4qpsjYJ2ZqvMKluq9OxmP
```

BUT: The last path segment is a KERI **Autonomous Identifiers (AID)**

- Trust lies in entropy, cryptography
- Key event logs (micro-ledger)
- Pre-rotation
- Multi-sig
- Delegation
- Uses "vanilla" cryptography
- Keys at the edge (KATE)

Benefit #4

KERI is a first-principles approach to identity, with security first

#5: did:webs is a more discoverable KERI

KERI AIDs

`EKYGGh-FtAphGmSZbsuBs_t4qpsjYJ2ZqvMKluq9OxmP`

"Native" KERI-based DIDs

`did:keri:EKYGGh-FtAphGmSZbsuBs_t4qpsjYJ2ZqvMKluq9OxmP`

"Web-discoverable" KERI-based DIDs

`did:webs:peacekeeper.github.io:did-webs-iiw37-tutorial:EKYGGh-FtAphGmSZbsuBs_t4qpsjYJ2ZqvMKluq9OxmP`

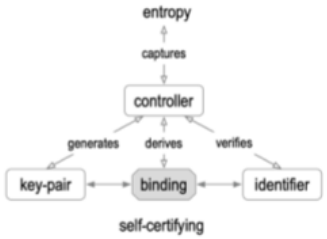
Benefit #5

Discovering KERI identifiers from the web is easy

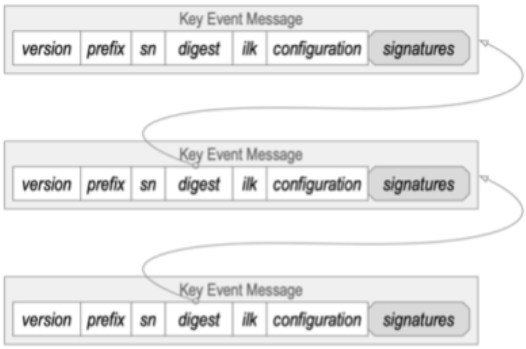
#6: did:webs is a more secure did:web

did:webs:example.com:alice:12345

https://example.com/alice/did.json
https://example.com/alice/keri.cesr




```
{
  "id": "did:webs:alice:12345",
  "verificationMethod": [{
    "id":
"#DFkI8OSUd9fnmdDM7wz9o6GT_pJIvw1K_S21AKZg4VwK",
    "type": "JsonWebKey",
    "controller": "did:webs:example.com:alice:12345",
    "publicKeyJwk": {
      "kid":
"DFkI8OSUd9fnmdDM7wz9o6GT_pJIvw1K_S21AKZg4VwK",
      "kty": "OKP",
      "crv": "Ed25519",
      "x": "FkI8OSUd9fnmdDM7wz9o6GT_pJIvw1K_S21AKZg4VwI"
    }
  }]
}
```



Benefit #6

did:webs DID documents are verified against the underlying KERI identifier key-state, etc.

#7: did:webs adds bonus features to did:web

```
{
  "id": "did:webs:example.com:alice:12345",
  "alsoKnownAs": [ "did:web:example.com:alice:12345", "did:keri:12345" ],
  "verificationMethod": [{
    "id": "#12345",
    "type": "ConditionalProof2022",
    "controller": "did:webs:example.com:alice:12345",
    "threshold": 2,
    "conditionThreshold": [
      "#1AAAAg299p5IMvuw71HW_TlbzGq5cVOQ7bRbeDuhheF-DPYk",
      "#DA-vW9ynSkvOWv5e7idtikLANdS6pGO2IHJy7v0rypvE",
      "#DLWJrsKIHrrn1Q1jy2oEi8Bmv6aEcwuyIqgngVf2nNwu"
    ]
  }]
}
```

did:webs:example.com:alice:12345?versionId=2

didDocumentMetadata.versionId
didDocumentMetadata.nextVersionId
didDocumentMetadata.equivalentId

Benefit #7

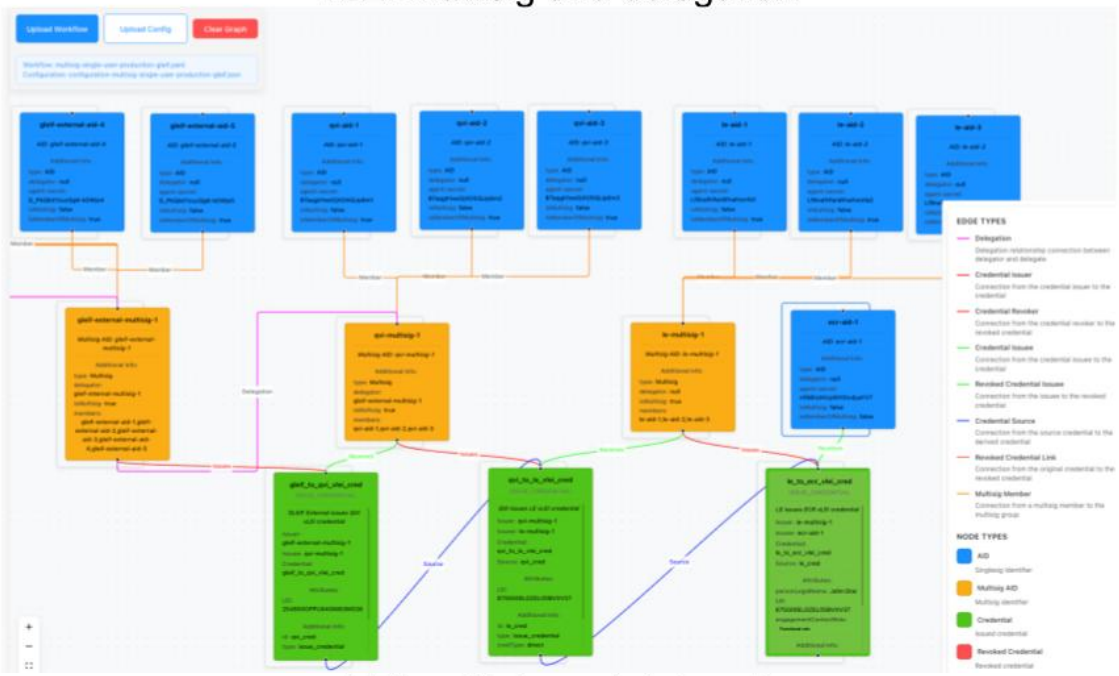
did:webs identifiers are more secure, but also add useful new capabilities beyond did:web

Benefit #8

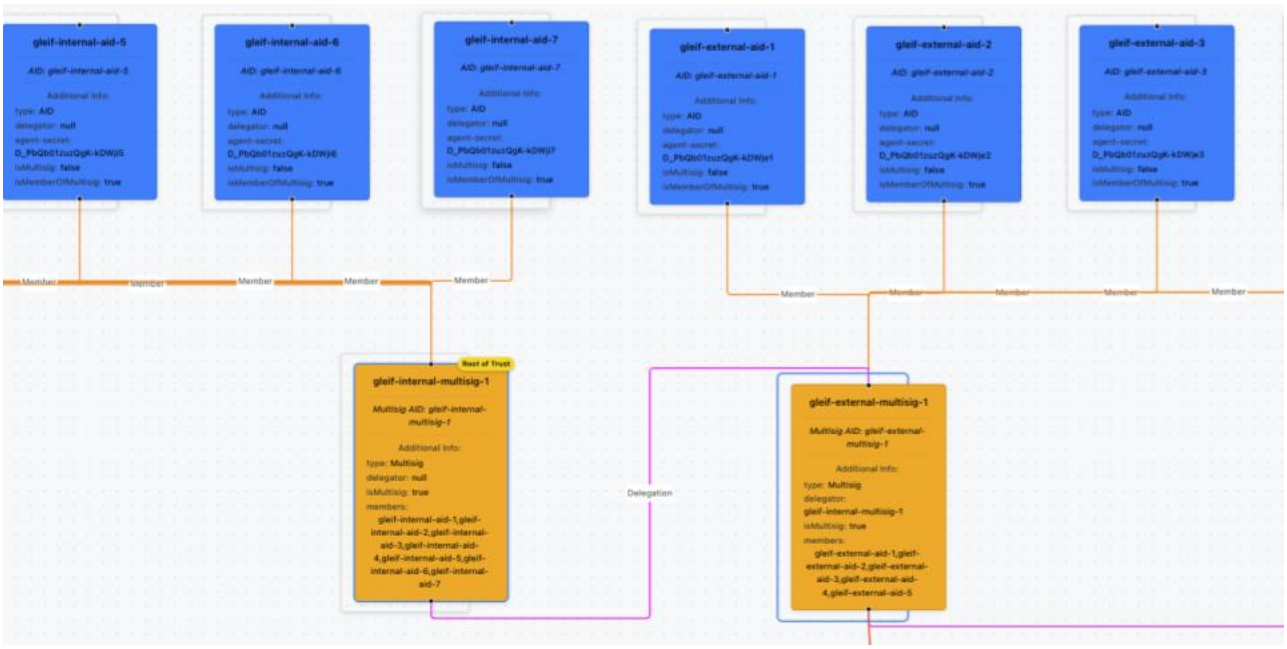
did:webs identifiers are portable

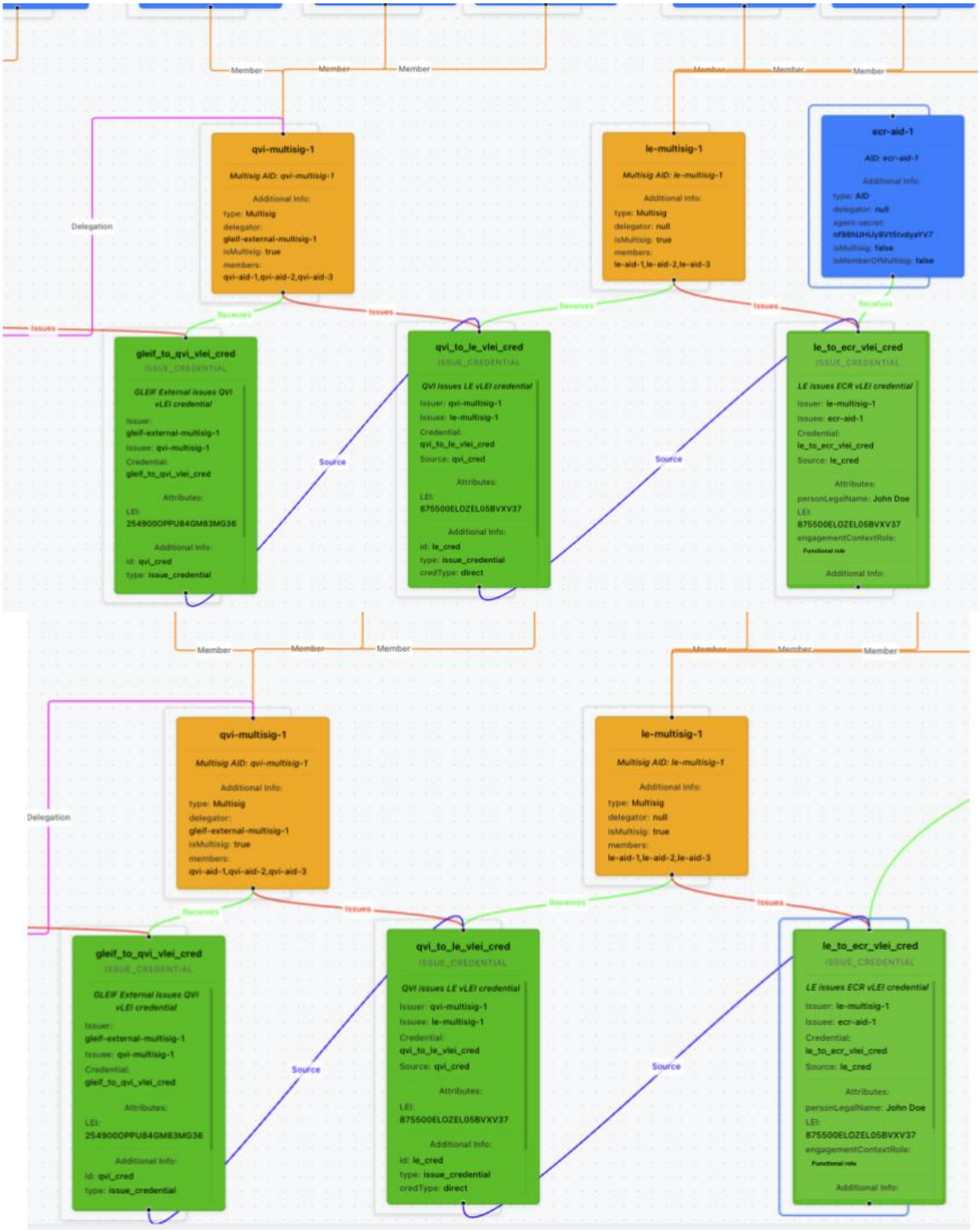
cross-border, cross-platform, cross-chain

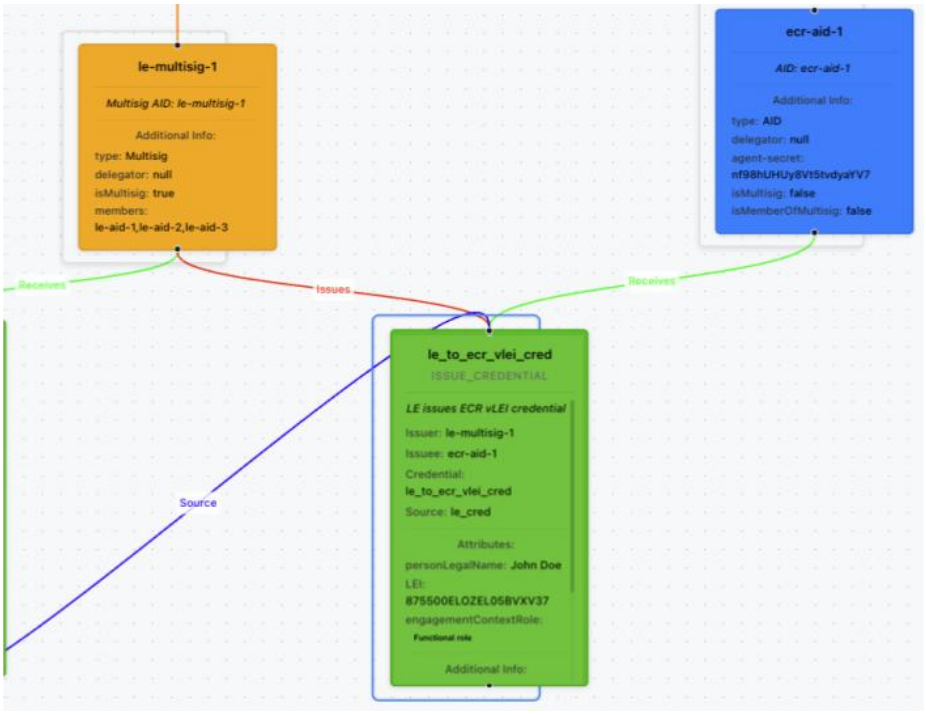
vLEI multisig and delegation



vLEI multisig and delegation




Member
Member
Member
qvi-multisig-1
Multisig AID: qvi-multisig-1
Additional Info:
type: Multisig
delegator:
gleif-external-multisig-1
isMultisig: true
members:
qvi-aid-1,qvi-aid-2,qvi-aid-3
Delegation
Issues
Receives
gleif_to_qvi_vlei_cred
ISSUE_CREDENTIAL
GLEIF External issues QVI vLEI credential
Issuer:
gleif-external-multisig-1
Issuee: qvi-multisig-1
Credential:
gleif_to_qvi_vlei_cred
Attributes:
LEI:
254900OPPU84GM83MG36
Additional Info:
id: qvi_cred
type: issue_credential
Source
qvi_to_le_vlei_cred
ISSUE_CREDENTIAL
QVI issues LE vLEI credential
Issuer: qvi-multisig-1
Issuee: le-multisig-1
Credential:
qvi_to_le_vlei_cred
Source: qvi_cred
Attributes:
LEI:
875500ELOZEL05BVXV37
Additional Info:
id: le_cred
type: issue_credential
credType: direct
Member
Member
Member
le-multisig-1
Multisig AID: le-multisig-1
Additional Info:
type: Multisig
delegator: null
isMultisig: true
members:
le-aid-1,le-aid-2,le-aid-3
ecr-aid-1
AID: ecr-aid-1
Additional Info:
type: AID
delegator: null
agent-secret:
nf98hUHUyBV1StvdyaYV7
isMultisig: false
isMemberOfMultisig: false
Receives
Issues
Source
le_to_ecr_vlei_cred
ISSUE_CREDENTIAL
LE issues ECR vLEI credential
Issuer: le-multisig-1
Issuee: ecr-aid-1
Credential:
le_to_ecr_vlei_cred
Source: le_cred
Attributes:
personLegalName: John Doe
LEI:
875500ELOZEL05BVXV37
engagementContextRole:
Additional Info:



Supporting vLEIs means supporting multi-sig and AID delegation:

- Spec covers multi-sig
- Does not cover delegation

Proposal for delegation to leverage `capabilityDelegation` field in DID Document

For example, here's delegation and multi-sig together:

```
"capabilityDelegation": [
    // Multiple keys will require threshold information like in verificationMethod
    {
    // To be definitive, the identifier can't be a key. Presumably, it is the AID like in
verificationMethod
     "id": "#ECwJlFWWcXQRwMDP80dmDgEO949AqKOSR2sTGFli9aSc",
      "type": "ConditionalProof2022",
      "controller":
"did:webs:example.com%3A8080:path:to:dids:ECwJlFWWcXQRwMDP80dmDgEO949AqKOSR2sTGFli9aSc",
      "threshold": 2, // Can be integer or array of fractions
      "conditionThreshold": [
        "#DMg3bHLEt86yNqb9YsQJwoJusIxhF_QUJQP6PQiQboP6",
        "#DA-vW9ynSkvOWv5e7idtikLANdS6pGO2IHJy7v0rypvE",
        "#DLWJrsKIHrrn1Q1jy2oEi8Bmv6aEcwuyIqgngVf2nNwu"
      ]
    },
    // The keys...
    {
      "id": "#DMg3bHLEt86yNqb9YsQJwoJusIxhF_QUJQP6PQiQboP6",
      "type": "JsonWebKey2020",
      "controller":
"did:webs:example.com%3A8080:path:to:dids:ECwJlFWWcXQRwMDP80dmDgEO949AqKOSR2sTGFli9aSc",
      "publicKeyJwk": {
        "kid": "DMg3bHLEt86yNqb9YsQJwoJusIxhF_QUJQP6PQiQboP6",
        "kty": "OKP",
        "crv": "Ed25519",
        "x": "yDdscsS3zrI2pv1ixAnCgm6wjGEX9BQlA_o9CJBug_o"
      }
    },
```

```
  {
        "id": "#DA-vW9ynSkvOWv5e7idtikLANdS6pGO2IHJy7v0rypvE",
        "type": "JsonWebKey2020",
        "controller":
  "did:webs:example.com%3A8080:path:to:dids:ECwJlFWWcXQRwMDP80dmDgEO949AqKOSR2sTGFli9aSc",
        "publicKeyJwk": {
          "kid": "DA-vW9ynSkvOWv5e7idtikLANdS6pGO2IHJy7v0rypvE",
          "kty": "OKP",
          "crv": "Ed25519",
          "x": "D69b3KdKS85a_l7uJ22KQsA11LqkY7YgcnLu_SvKm8Q"
        }
      },
      {
        "id": "#DLWJrsKIHrrn1Q1jy2oEi8Bmv6aEcwuyIqgngVf2nNwu",
        "type": "JsonWebKey2020",
        "controller":
  "did:webs:example.com%3A8080:path:to:dids:ECwJlFWWcXQRwMDP80dmDgEO949AqKOSR2sTGFli9aSc",
        "publicKeyJwk": {
          "kid": "DLWJrsKIHrrn1Q1jy2oEi8Bmv6aEcwuyIqgngVf2nNwu",
          "kty": "OKP",
          "crv": "Ed25519",
          "x": "tYmuwogeuufVDWPLagSLwGa_poRzC7IiqCeBV_ac3C4"
        }
      }
    ],
```

did-webs-ts:
https://www.npmjs.com/package/@gleif-it/did-webs-ts

For more about did:webs Spec:
https://trustoverip.github.io/tswg-did-method-webs-specification/

Details about proposed approach to delegation
https://github.com/trustoverip/tswg-did-method-webs-specification/pull/148
https://github.com/trustoverip/tswg-did-method-webs-specification/issues/149

Reference Implementation:
https://github.com/GLEIF-IT/did-webs-resolver

Past IIW Tutorial:
https://github.com/peacekeeper/did-webs-iiw37-tutorial

Universal Resolver:
https://uniresolver.io/

Why is this good for Switchchord?

Non-custodial key management options.

Publicly-traded and large enterprise music companies have vastly different security requirements from medium to long-tail users.

Bridges the KERI and W3C communities.

We're able to issue W3C VC and ACDC credentials for our legal workflows. Enables integrations with DWNs, DIDComm, etc.

Enables GLEIF vLEI integration.

We are in discussions with a prominent government-sponsored music industry database looking for an organizational identity solution.

Baby steps into full decentralization.

I can phish your Signal

Session Convener: Yuriy Ackermann
Session Notes Taker(s): Wendy

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

https://webauthn.io/

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

Attack: “Daria scam” QR code shared for “support my child in competition”, goes to a Telegram/Signal/WhatsApp link new device flow. Estimated 2-5 MM compromises in Ukraine, Russia, Belarus.

Proposed solution use Passkeys. Device proximity (bluetooth hybrid) thwarts the remote attack. Yuriy has/will open source code, whitepapers.

[to add Yuriy’s slides]

mDL: Privacy Concerns - How can it track you?

Session Convener: Steve McCown, Chris Bramwell, Timothy Ruff
Session Notes Taker(s): David Kelts (from audience, incomplete)

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

Presentation slides:
https://www.dropbox.com/scl/fi/gysbckw4gc0bn4me2s937/IIW-40-mDL-Privacy-Concerns.pdf?rlkey=vif2r8188hng49y8mrhh9opjp&st=uptgpu3x&dl=0

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

This session did not cover Utah's recent privacy legislation. That was covered elsewhere in sessions.

Discussed by audience adjacent to any presentation slides were the **advantages of having variable "Interaction Modes"** (defined in section 2 of https://www.mdlconnection.com/the-mobile-drivers-license-mdl-and-ecosystem/) in ISO/IEC 18013-5 implementations. These various interaction modes support reader devices with all communications types. For example, POS devices have NFC, no Bluetooth for PCI compliance, and good network connectivity therefore a Tap & Lookup interaction mode best fits those devices.

Referenced was the **Privacy Annex of ISO/IEC 18013-5** that adds non-normative requirements for privacy of implementations above and beyond the protocol for signed-data sharing and the mdoc formats.

Presented authoritatively (verbally) were the existence of AAMVA's mDL Implementation Guidelines that provide a set of **privacy requirements for mDL implementations in North America** that opt to place their public key in AAMVA's Digital Trust Service directory.

Utah's mDL implementation has attested to conformance with the ISO privacy annex, the AAMVA Guidelines, and Utahs privacy laws as of the launch date in 2022.

A few of the **advantages of using "server retrieval"** from the mDL standard were brought up by the audience, however that list was cut short and therefore incomplete. Specifically discussed, however, was the operational model and security policies of the Utah mDL implementation that do not permit any government official to have login access to the cloud platform where transaction data is processed (but not stored - it is significantly harder to breach data that is not stored, you must sniff it). Government officials only have login access to a statistical portal. **Choice is critical to privacy.** Choice of wallet app, consent for sharing, choice in mobile device, choice in how the user manages their credential signed by the government. mDL Implementations with single "interaction mode" implementations or single wallet choice, limit the ability for the

end-user (resident) to choose what they prefer and migrate between systems for highest privacy effect (you cannot choose the Duck-Duck-Go of wallets for the highest privacy).

Presented from the audience were several of the **privacy holes in "device retrieval"** (device to device transmit of signed data). Please note that these are addressed non-normatively in the privacy annex of 18013-5 and addressed normatively as policy in the AAMVA mDL Guidelines:

- The wallet application has the transaction log and, if branded or issued by the State as in several implementations, has the ability to correlate those transactions and phone home with them.
- Credential refresh guidelines and the mechanisms for revoking on-device credentials create a "phone home" channel from the wallet app or wallet back-end services to the Issuer. In addition, air-gapping the app from the Internet allows for long-lived credentials on devices after refresh/revocation.
    - Revocation of driving privileges is a refresh.
    - Revocation of credentials happens when one is found to be fraudulent through investigation
    - Revocation of credentials happens when people move out of Utah.
    - Refresh or revocation of credentials can happen when the holder changes or surrenders their physical credential
- MSO-refresh to resist tracking is implemented per AAMVA mDL Guidelines, however Relying Parties still have the opportunity to correlate data sets based on demographics shared unless policy prevents them from doing so (Utah legislation killed at the time of rollout)
- Discussed was how Utah law requires Restaurant and Bar RPs to log customer data from age-verification in the event of forensic research on an overserved patron. This vector has breach potential and privacy implications coded into law.
- Reader Identification/Authorization creates a vector for restriction of the open ability to read mDLs by all relying parties. Big Tech implementations of mDL wallets do not respond to a reader application unless it has applied for an entitlement from the Big Tech vendor. This creates a registry of readers permitted to perform device-retrieval with simple correlation by Big Tech from the transaction logs to the readers and locations of usage.

<end notes>

Proof of Humanity: World ID

Session Convener: Gabe Cohen, Priyanka Kohli
Session Notes Taker(s): Priyanka Kohli

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:

- Introduction to World: https://world.org/
- The discussion was in question & answer format involving the following topics.
- Proof of Personhood/Proof of Human
- The Orb is a hardware that's used in determining a unique human being. Any data is stored on the user's phone, and is not saved in the Orb or World Chain
- No PII is known to World, and hence cannot be shared with a Relying party, except a proof of unique human
- Account recovery and Account reset are critical features that are technically possible but have not balanced in a way that existing relying parties business continuity is not disturbed
- A suggestion was shared about considering integrating passkeys with World ID
- Relying parties may decide to have qualification criteria to detect fraud, and revoke their relying party IDs. This is at the level of relying parties, not with respect to World ID.
- Backup and Restore feature is available
- Reputation system development was discussed, however it is a unique system per relying party. Multiple relying parties cannot share information since we don't identify users uniquely yet. Discussion around enabling individual users to share reputation across relying parties was interesting.
- Orb hardware is custom but not meant to be proprietary. It is meant to be open source and decentralised.
- World ID and World ID Credentials are available currently
- World Event on April 30 in San Francisco was discussed

OpenID Connect with Deferred Token Response?

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

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

Slides from initial presentation of session:
https://fkj.github.io/slides/iiw-oic-dtr-apr-2025.pdf

OpenID Connect:
https://openid.net/specs/openid-connect-core-1_0.html#OAuthParametersRegistry

OpenID CIBA: https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0.html

OpenID4VCI Deferred Credential Endpoint:
https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-ID1.html#name-deferred-credential-endpoin

OAuth 2.0 Multiple Response Type Encoding Practices (None response type):
https://openid.net/specs/oauth-v2-multiple-response-types-1_0.html#none

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

The purpose of this session was to determine whether there are any existing solutions for deferring the return of identity tokens in OpenID Connect.
This is useful e.g. for KYC flows with machine learning-assisted validation of physical documents.

Nobody at the session knew of an existing solution that was not a hack. It would be good to have a standard because it makes integration much easier for Relying Parties.

Consensus that there are no obvious problems with the following design:

- Use the approach from OpenID4VCI Deferred Credential Endpoint
- Require DPoP to make long-lived access tokens secure
- Attend the session on poll/ping/push for OpenID4VCI later to see what they have to say about it

The eKYC working group in OIDF is somewhat interested in the concept. There are some potential issues with evidence validation/timestamping related to KYC.

Unclear: how should the protocol communicate that we are in this flow?
One option that seems designed for the purpose: response type “None” in OAuth 2.0.

SESSION #4

DCQL Next Discussion

Session Convener: Christian Bormann, Paul Bastian
Session Notes Taker(s): Paul Bastian

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

https://docs.google.com/presentation/d/12Tcta_MhupcYhDLci4wtBFJAAbNLSqp_g3Cy3MG1dr0/edit?usp=sharing

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

Introduction to DCQL

- DCQL became the only query language for OpenID4VP, PE2 got removed to make things simpler, less implementation effort
- limited feature set for simplicity
- good implementation feedback so far

Purpose

- purpose is currently optional freetext field
- worries about phishing attacks (not bufferoverflows etc)
- purpose in unsigned seems more dangerous
- purpose in signed requests makes more sense, could be integrated in RP certificate
- sign over prose? i.e. put it into KB-JWT?
    - in transaction_data we show and sign RP-chosen text
    - increases accountability
- 18013-5 defining integers/enums/codes for common use cases, e.g. buy alkohol
    - codes may be limited and there are more use cases than codes
    - codes are better for being language independent
- freetext may be harder to display for Wallets, e.g. max length?
- user decision may not be significantly influenced by the purpose string
    - purpose may give guidance why certain credentials are requested
- unclear if purpose was a requirement by ISO group
- rough consensus to remove it, Brian will do a PR

Advanced Features

- currently we only have exact value matching
- is there a need for functions, e.g. greater-than, array membership etc..
    - e.g. matching if nationality is within array
- Dimitri: operators look very similar to JSON Schema
    - current ideas are based on Daniel Fett's draft
- things will be added to OpenID4VP 1.1, as 1.0 ship is sailing in the next days

- we should be careful to not add too many features, as the niceness of DCQL is its consensus feature set and still easy-to-implement
- David: matching attribute values across multiple credentials is an important feature
    - Gareth: matching names does not work very well in practice
- Ahbi + Matteo: strong typing is required for ZKP features
    - problem that we have multiple credential formats with different typing
    - Hicham: be aware that we potentially add lots of complexity
    - Paul + Lee: Basic Value matching is important and may add privacy
- Helen: Array matching seems the most important use case

Passkey.101 (an IIW 101 Session)

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

Attestation of Authentication Material

Session Convener: Monty Wiseman
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

Governance driven trust registries by Digital Governance Institute

Session Convener: Scott Perry Founder and CEO
Session Notes Taker(s):

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

https://4sure.tech/wp-content/uploads/2025/03/Whitepaper-Governance-Driven-Trust-Registries.pdf

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

This presentation explored the critical role of governance-driven trust registries in addressing challenges of trust, accountability, and transparency in decentralized digital ecosystems. It outlines a comprehensive model for digital governance and trust establishment, emphasizing the need for risk assessment, conformance programs, and governance frameworks. The presentation introduced trust registries as a flexible, scalable alternative to traditional hierarchical trust models, enabling the validation of claims through decentralized authority statements within a shared governance structure.

This presentation explored the role of governance and trust registries in addressing this complexity and outlined their importance in enhancing ecosystem trust. Specifically, it:

1. Defined the roles of governing authorities, governed parties and trust registries within an ecosystem.
2. Detailed the processes to establish a governance framework upon which a trust registry is based.
3. Discussed the complementary relationship between trust registries and the ecosystem's governance framework.
4. Highlighted technical considerations and standards that can support the implementation of proper governance and trust registry operation.
5. Concluded with actionable steps for the ecosystem leadership to explore governance and trust registry solutions with its stakeholders.

Key topics included the distinction between organizational, ecosystem, and registry of trust registries, as well as their role in enabling high-integrity digital interactions. By decoupling authority from centralized models, trust registries democratize trust establishment, fostering inclusivity, interoperability, and scalability. Technical considerations, standards compliance, and governance alignment are discussed as essential components for successful implementation.
Type You Notes Here

How can we build trust across borders? Explore TRUST MECHANISMS

Session Convener: JC Lee
Session Notes Taker(s): JC Lee

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 discussion explores mechanisms for establishing cross-border trust in digital identity systems and transactions. As our world becomes increasingly interconnected, the need for reliable, secure methods of verifying identities and establishing trust across national boundaries has become critical. We examine several established frameworks and emerging approaches that enable organizations, governments, and individuals to confidently engage in cross-border interactions.

Discussion Points:

- **Federated Trust & OpenID Federation:** Industry-recognized federation systems play a crucial role in cross-border identity verification. We examine how global recognition lists (such as international university accreditation systems and open banking initiatives) already provide robust trust infrastructures that shouldn't be reinvented but rather leveraged and expanded. The limitations of these systems are also explored, including challenges with scalability across diverse legal jurisdictions and varying technical standards.
- **Trust Registries:** These centralized or distributed databases act as authoritative sources for verifying the legitimacy of identity providers, credential issuers, and other entities in the digital trust ecosystem. We discuss how trust registries establish a common foundation for cross-border recognition, allowing entities to confidently interact with previously unknown parties.

Passkeys are Better for Authn -or- Stop trying to move digital cred. Presentation for Authn Happen!!

Session Convener: Matthew Miller
Session Notes Taker(s): Bill Fisher

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:

Can we use credential presentation for authn?

- Totally valid question. Potential to reduce implementation burden.

Passkey are better since they are purpose built

- DCs have a variety of credential types and presentation protocols
- DC impose large implementation friction on the verifier who needs to support all the different protocols

Discussion 1:

Passkeys are easier to implement, less specifications to deploy
More mature usability, less friction, especially on desktops where DCs must be presented in a cross device flow.

Discussion 2:

- Passkeys are available across desktop, laptop and mobile
- Support Syncing
- Passkey providers are more mature than wallets currently

Discussion 3:

- Digital credentials can come with attributes and PII which we don't want to assert to RPs each time the user authenticates

Comment:

- Potential to use DCs as a secondary verification to trust a passkey since passkeys can be sync'd
- Currently using SMS OTP as a step up to passkeys, which promote poor usability and bad optics.
    - DCs models are similar to federation models, where you are passing attributes.

CASE STUDY - Org-ID in City Administration Hardware-Crypto secured

Session Convener: Andre Roeder, KAPRION Technologies
Session Notes Taker(s): Janet Gonzales, Andre Roeder

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:

- Results of three years project together with city administration of Dresden (Saxony, Germany)
- broad organizational structure of different departments and hierarchical levels, linked to various areas of responsibility and rights of representation
- mapping the “digital municipality” in “DepartmentID” credential
- Organizations are only virtual. They do not act themselves.
    - Individuals can act on their behalf
    - Bots can act on their behalf
- Individuals and bots proof their identity by using asymmetric keys
    - Copies of private keys must be avoided by all means
    - Hardware Security Modules (aka Crypto chips) are the only solution
    - Same solution for bots and individuals to keep complexity low
- Trust is built upon
    - Non-repudiation of one's own identity
    - Non-repudiable statements by trusted actors
    - Transparent processing rules (a credential is the result of a process)
- Information to transport: Right to
    - Represent the organization
    - Issue a credential of a certain type/scheme
    - Verify a credential of a certain type/scheme
    - Define a process for the organization
    - Participate in a process (make decisions)
    - Gather information (GDPR)

  in the name of the organization
- Delegation Credential scheme presented
    - covers rights to represent, issue, verify
    - rights to define a process and to gather information are under discussion
    - delegation credentials are chained (SD-JWT VC)

Help me build the future of Identity on Social Media

Session Convener: Alberto Leon @ASML @Harvard
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

Demo of First Person verifiable relationship credentials (VRCs)

Session Convener: Drummond Reed, Day Waterbury, Brad deGraf
Session Notes Taker(s): Drummond Reed

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

This was the followup session to the second session where Drummond Reed gave this introduction to the First Person Project (through slide 62), of which the highlight was showing how people can form digital trust relationship using verifiable relationship credentials (VRCs), which are a way of implementing "the ultimate instant key signing party" (46 and 47) and to r-cards (relationship cards — slide 61).

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

The demo First Person app (iOS and Android) is available at the QR codes at the start of the slide deck.

Roughly 40 people tried the apps and forming their first connections. The app is at a very early stage of development, so there were multiple UX challenges and several bugs, but the overall reception to the idea of VRCs was well received.

There was a good discussion of suggested improvements and features to add to have no later than the next IIW.

There will be a follow-up session on the second half of the First Person Project presentation on Thursday.

What happens after VC adoption? What does our world look like?

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

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

Reputation, Advanced VC use cases

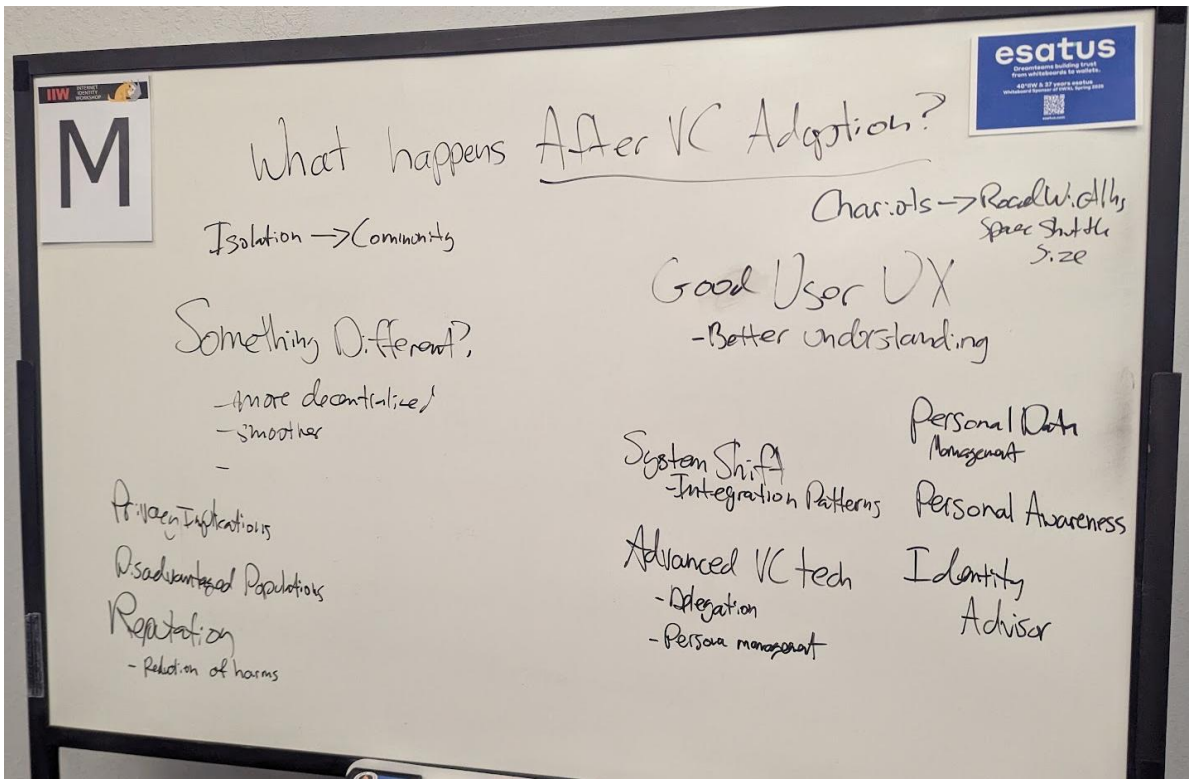
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Imagining a day where VC Adoption is common, in that VCs are regularly issued, easily held, and presented regularly, what does the world look like?

We discussed a variety of interesting things, including advanced VC issues, personal data, etc. Good UX was mentioned early, as helping users understand the choices they make will be a significant portion of improving privacy and security.

A big one discussed is the possibility of advanced reputation systems. This enables a much higher level of trust for small, common interactions.

A point brought up early was the hope that this leads to Something Different. This means that we have opportunities for interaction and regular technology use that provide something very different than just the same stuff we keep doing with only a different name.



SESSION #5

KERI Security Deep Dive: 1. Why "all" of KERI is necessary and sufficient!

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

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

Session Slides: Same for all KERI Security Deep Dive I, II, and III
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI_SecurityDeepDive.web.pdf

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

Type Your Notes Here

Intro to SSI & DIF (an IIW 101 Session)

Session Convener: Kim Duffy, Steve McCowan
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

Inventory of error states in the DC API / DID4V Ecosystem

Session Convener: Tim Capalli
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:

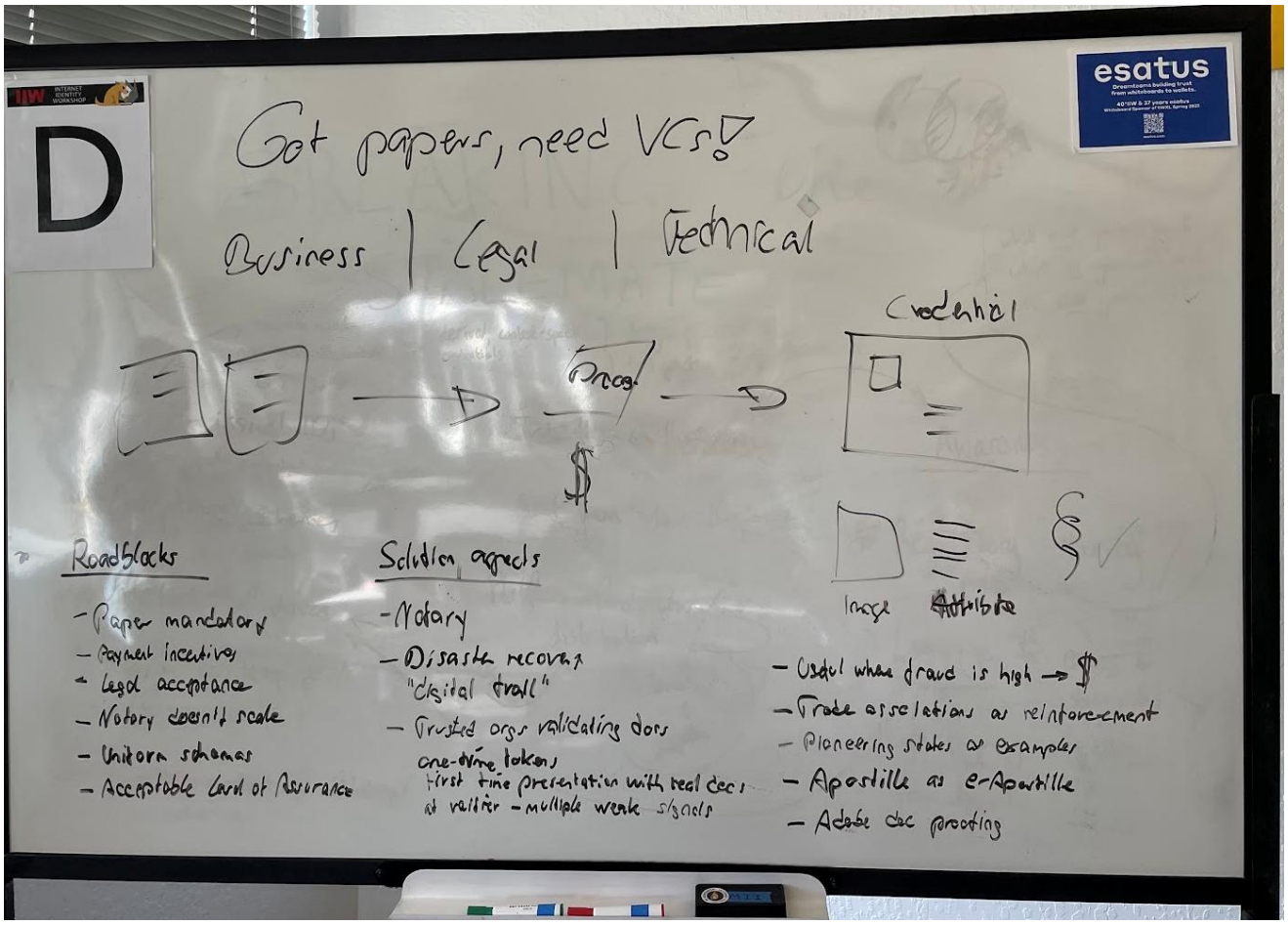
NO NOTES SUBMITTED

Got papers, need VCs! BLT aspects from paper documents to credentials

Session Convener: Andre Kudra
Session Notes Taker(s): Andre Kudra

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

Business / Legal / Technical aspects from paper documents to verifiable credentials



What Happens when we have My Terms? - IEEE P7012 (later this year)

Session Convener: Doc Searls
Session Notes Taker(s): Brandon Norgaard

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

IEEE P7012 MyTerms
FedID

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

Where do MyTerms Lead?

1. A path to personal identifiers from the person
2. Rebuilding relationships
3. Death of ad tech – better targeting to signals
4. Data co-ops to balance power – buying club – new communities
5. Beke into first person credentials – better relationships
6. Creating private channels – moving from P2P or C2B
7. Covers mutual respect
8. New marketplaces – new ways to go to market – competitive advantages
9. Short term – changing conditions, inconsistent properties. Long term –
10. Adoption on both sides
11. 2 cows server-server
12. Evaluation to more agency, choices, adaptation
13. Certification, compliance

In future versions, maybe bespoke contracts

State of the art on AI: Learn about "vibe coding", how to bribe/trick AI agents, and all of the identity challenges

Session Convener: Ankur Banerjee
Session Notes Taker(s): Ankur Banerjee

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

IIW 40 State of the Art of AI - April 2025

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

- Vibe coding
  - Vibe coded game with 1000s of users and run-rate of $1mn ARR: https://fly.pieter.com/
  - Vibe coded useful tools: https://tools.simonwillison.net/
- Using AI for coding assistance
  - Knowing when to use what model is a treadmill that's hard to stay on to of
  - E.g., Claude/OpenAI reasoning models are great when working across a few files; Gemini models currently better when working on larger codebases but YMMV
- Quality of training data
  - AI labyrinth: https://blog.cloudflare.com/ai-labyrinth/
  - Will replicate insecure code
  - There are known threat actors feeding insecure code

OpenID Provider Commands Account LIfecycle for OIDC

Session Convener: Dick Hardt
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

What's NEW in FIDO?

Session Convener: Nick Steele + Matt Miller
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

Planning Your Digital Estate

Session Convener: Dean H. Saxe
Session Notes Taker(s): Michael Mitchell

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

https://openid.net/cg/death-and-the-digital-estate/

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

Death and Digital estate

How to plan for what happens to your digital assets after you die.

Not just about death.

If incapacitated, there are assets you might want others to have temporary control over.

White paper with OpenID Foundation
Heather to co-edit

Delivering a planning guide as well

Can create legacy contacts (Apple, Google, etc)
But limited

OpenId.net
Github repo
Collection of resources there on different services
Looking for formal and informal resources

Wide spectrum
How people approach death

“Being mortal” book was brought up
By Atul Gawande

Challenges how we address death and dying through the North American health care industry

Advanced Healthcare Directive
Talking to people well in advance

3 areas to cover

FIRST
Assign a legacy contact

SECOND Harder
Things with NO mechanism to document wishes

THIRD
May have to do something manual
EX Flickr - take offline backups and give to X person

Question - what triggers actions after “I’m dead”
Nothing. There is no real mechanism

George Fletcher - Inconsistencies in notification

Certain things require an ORIGINAL death certificate. Others are ok with a COPY. Yet others are ok with calling and telling them.

IDEA - Mike
Get 10 original notifications of death certificates as you won't know what you'll need

Mostly that my spouse has the things she'll need after I'm gone

Turn off passkeys
Throw the key to the password manager to my spouse

Bank might be able to verify death and that could be

George
Should really be a good way to do this
Put stuff in an envelope, then that in safe
But then I'll need to leave combo for the safe somewhere
It snowballs

Shared secure note via password manager

Christian R.
Grandparent passes
Wrote some passwords down, some not
Had to do digital archeology to sort it out
Can't get 100% of it
This stuff SHOULD be in default setup / onboarding flows for any new service
Nudge them into these patterns

Dorin
LastPass has a flow
Part of a family you can request XZ person to get all my passwords
Deadman's switch / Wellness check
Don't reply to an email after X days

George
Dad is in that space
Has 2FA on email, but phone number was used and it changed
YUBA Key?
Can get into his dad's email account

OnePass purchased through App Store
No option to pass that along to his kin
Buying directly you do have that option

Apple Passwords

Passwords won't be passed to family per the TOCs

It IS possible to Airdrop a passkey

Dorin
Old iPhone at home
JUST has Google Authenticator on it
Not connected to internet
Wife can use it to unlock things

George
Should we design a system
He calls it "Delegated Authentication"
Such that IF they could present something else…
My son is able to access my account if X happens
Son has his OWN credential for a specific scenario

Rohit
Notion of "Disconnected apps"
Unaware of the swap Georg
SERBY

John Pritchard
Other person in healthcare industry
Like guardianship
For my kids, I'd have access as a parent
My name "on behalf of" son's name

From UI perspective, LOOKS like it's his kid responding
Unclear who's responding

Yiko
Unicorn accounts - kid accounts with own credentials, but if they try to do certain things, parents get asked to allow action

Secondary billing number for his wife
Using a separate unlinked card
Billing timing at a year

Planning guide
Need to hit the practical to dos

Dead or incapacitated state
Need an authority that validates that
Is that built into the healthcare system?

Dorin
LIKE becoming a donor
Show something similar on digital ID that could be the trigger

MOSIP
ADHAR
Africa, Philippines, others
Certified birth and death registry
Those protocols could be implemented as a potential mechanism

Need a way to UN DEAD you
People make mistakes, so need to have a reverse gear

George
SSA does have a way
Person with this SSA is no longer alive
Not sure who has access to this registry / who's listening
Wife passed, DMV needed to see that he was executor of the estate
Should've been His name, her name OR survivor to get around it (as they usually do)
Usage of the registry is very inconsistent

States feed up to federal databases

Judith
Will the document be what to do TODAY (based on what's available today)?

Dean
Planning guide - Managing the gaps that exist today
White paper - what is current state, what are the problems for the planners, executors, …
What is the state from State and Government perspective

Involves all the big players to help solve the problems

IDEA
Control panel for most services
All else, let my wife or kids take care of it

Resist the binary thinking
Continuum… could be incapacitated, missing in action, not responding, dead

Dorin
Look at what the law says
Not a new problem
Time limit for when someone is considered "dead"
Example - friend dying from cancer, turning it into a QR code to go on the tombstone
He's building in a way for long term compatible

One problem was the domain ownership - max could pay is for 10 years

Dean
To transfer domains, have to set up an LLC to make the transfer of ownership

Dorin
At some point we'll hit a point where people ask if the trustee is an AI

Christian
Assume all is in a digital wallet, passwords, IDs, VCs
Someone passes away
How does someone deal with turning an account into a memorial mode

Mike
Evaluate the technical level of your survivors
Will they be able to deal with these things?

- NOK Box

Christian - Ideal
Go to a law firm
Give them a PIN to a Yuba key
You can release it to this list of people
As long as they have a death certificate

Relationships change over time
I may identify person X to get everything
But relationship might change over time

Dean
Problem is those are MY credentials
So someone would be impersonating me

Durability of data storage over time
Writing things to a blockchain
OR create a DAO who handled the decisions and actions

Technical problem
Legal problem
Policy problem
Cultural problem

"Post-humous identity theft"

Finding the right digital representation

Is it a mandate to companies that companies have to offer SOMETHING like this

Christian
Service provides a control panel
Knobs and dials set
I want my account to

- Impersonate me
- Be able to delete my account
- Turn on memorial mode

Dorin
Once regulation exists
Death Tech is a vertical space
Probably screen scraping

Death and the Digital Estate at OpenID Foundation
Bi-weekly meetings

Another group like this spinning up in Australia

Digital Fiduciary Initiative

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:

Overview presented, basically talking through the content on the website.

Updates:
Federal grant still alive. The PDaSP program is still considering our proposal.

We filed a provisional patent to protect underlying technical approach.

We are continuing to figure out the details for fair witness ceremonies and the structure of the organization.

Bart van der Geest • 2nd
Head of Compliance @ Hopae, a digital identity company backed by 500 | eID...
4d •

That's a wrap for IIW Spring 2025!

Huge shoutout to the organizers of the **Internet Identity Workshop** for pulling off another fantastic event — happy 40th anniversary!

There's a special kind of energy at IIW that sets it apart from other conferences. It creates a space where people genuinely want to share ideas, spark discussions, and collaborate to move identity forward. It's truly inspiring to be part of such an open and passionate international community.

I'm especially thankful for all the meaningful conversations I've had, and to everyone who joined our session — your curiosity, questions, and contributions made it both a fun and insightful experience.

Until next time, IIW!

Notes Day 2 / Wednesday / Sessions 6 - 10

SESSION #6

Identity in Digital Media

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

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

Slide deck: https://ericscouten.dev/2025/iiw40/06a-cawg-update-for-iiw40.pdf

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

- Overview of who's who
  - CAI - outreach, advocacy, open source
  - C2PA - technical standards
  - CAWG - identity standards

- C2PA data model
  - Overview of the assets and supported assets
  - Assets manifest store overview and its similarity to github
  - Overview of assertions
  - Each manifest has one claim
  - Claim signature is the signed claim

- Question about security of signing plus buggy systems that can be compromised.
  - Scott is leading the trust governance model for the C2PA to talk about how implementation environments can be trusted.

- Created assertions vs gathered assertions

- What does CAWG do? Technical standards include
  - Endorsment
  - Identity
  - Metadata
  - AI Training and Data mining

- Identity Assertion overview
  - Which signatures should we include in the spec
  - What does identity mean to content creators
  - Claims Aggregator overview

- Are we connecting the dots?
- Most people do not have access or understanding to these technologies
- Example of a need is SAAG actors wanting to have auditions tagged with their identity at time of submission
- Levels of assurance vary and need definition by the industry
- Attestation for creation of physical objects was posited as a future use case
- Interest in licensing and IP protection at time of publish
- CR logo needs to be in Unicode to make it interoperable
- What if creators do not want to be tracked but still want to use the framework?
- Is there a trust score mechanism?
- Museums may value physical assentation as a use case for it

OpenID4VCI Issuer to Wallet Events

Session Convener: Mirko Mollik, Oliver
Session Notes Taker(s): Lukas Han

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

Link to presentation

use cases
- async cred issuance
    - avoid polling
- new cred version
    - get latest version
- cred revocation
    - avoid polling

polling
- deferred endpoints

use push noti?
- issuer signal when cred is ready

JWT for preventing spamming

transaction id will be created as a one time code. to prevent to trace by issuer

—

for design, is it for long or short?

dark pattern could be happen, issuer tracking.
—
auth JWT

why is nonce needed? is it https?
spamming to wallet BE
replay attack.

JWK for encryption. encrypted data is sent to wallet BE and go to wallet. then wallet can decrypt it.
wallet BE can check which issuer by IP. so encryption is needed.
—
it's just a ping.

we need issuer field in the event payload. to distinguish which issuer.
wallet can handle the transaction_id to connect which issuer

The Challenges of Wallet UI/UX

Session Convener: Ken Watanabe
Session Notes Taker(s): Stefan Charsley

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

20250409_IIW.pdf

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

Introduction by Ken Watanabe

Talking about the Conventional ID Federation Model, user consents data provision, Data provider provides data to Service provider.

Differences between conventional and VCs. Issuer issues VC to Holder, Holder shares to Verifier.

Selective disclosure lets user hide information from verifier.

In VC model, holder needs to store multiple credentials.

Looking at different examples of VCs.

Problems with Utah mDL user experience. ACLU has raised concerns about too many options for selective disclosure and linkability concerns.

Holder wallet needs to feel secure by design, privacy protected, easy to understand, simple steps.

Survey of existing wallets, not all wallets available for survey.

Showed flow of presentation.

Discussing each step, first registering the credential into the wallet. User viewing credential in wallet, including presentation history.

Presenting the credential, holder can scan QR and select the desired presentation.

Sartor Sebastion, et al (2022). Choose 4 wallets to look at for research. Showed 15 participants each wallet.

Key user insights, jargon hard to understand, privacy features not visually clear, long multi-step leads to negative reactions, tutorial could help users.

Q: did the wallets use terms like DID before explaining to user?
A: yes

Sukhi Chuhan et al (2023). Interview 47 people with custom prototype. Concerns about government surveillance, QR codes challenging, anxiety over lack of credential recovery after device loss.

Sandra Kostic et al (2022,2024). Interview 16 people with custom prototype. Positive impression of data control. Feeling of security depends on wallet provider. High comfort from government.

Takahito Sakamoto et al (2023). Interview 5 people. Prefer starting with less sensitive items, e.g. tickets, before sensitive IDs, e.g. National ID. Want clear benefits explained. Building trust between user and wallet very crucial. Hesitation on whether selective disclosure is really occurring and information is not secretly being sent. Having presentation history for better understanding and recognition of benefits.

Common UX challenges: Trust & Privacy, Complex Terminology, Onboarding & Complexity, Design & Clarity, Provider & Adoption, Recovery & Support, Motivation to Verify.

Now open discussion.

Challenge on explaining clearly and simply to users.

Need to attract more UI experts to IIW to tackle experience issues. Problems are being pointed out, need UI experts to assist with solutions.

Companies have UX experts even if they are not necessarily at IIW. Competitive aspect between wallets. W3C says wallet needs to be accessible, not necessarily reflective of physical ID cards. Great discussion on UI.

Do not expect selective disclosure to be exactly portrayed to user. Wonder if there is certain bias from wallets examined in research, many are prototypes. Separation of responsibilities. How are people approaching branding? Where is the boundary of the wallet regarding UX? Theres a bigger picture that needs to be looked at.

Some wallets allow extra control UI which can make it more complex for users to understand.

Implementation experience, user education needed.

Solution proposed regarding selective disclosure UI.

Whats the people's perception of the government? From research presented, Germans were more open to government solutions. Should explore different societies to determine perception differences between countries.

Whats the next steps for the research? How do we improve the UI?

Try to create guidelines for wallet UX for standardized wallet experience.

People having challenges with selective disclosure, whether it works in practice or not for users. If something is optional, you shouldn't ask for it. Doesn't make sense to ask user for something they can choose not include. Minimize the number of things RP is asking for.

Your IAM Is Based on the WRONG Use Case

Session Convener: ALAN KARP
Session Notes Taker(s): MIKE SCHWARTZ

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:

Alice would like to give some of her permissions to Bob…

Bob could be a program… but she doesn't trust it with all her permissions. She needs "attenuated delegation" so Alice can run the program with least privilege.

What if Alice wants to be able to delegate "query" on R1 (e.g. Alice's database) but "update" on R2 (e.g. Bob's database)

What if Carol wants to query R1 and Update R5… which neither Alice or Bob has access to.

This transitive use case scenario captures all of the hazards of basic access pattern and confused deputy.

Mistake was made a long time ago to focus access control lists not capabilities.

In audit log… you see Bob did it… but you don't see Alice delegated the capability. You need to keep responsibility delegation.

A capability is an unforgeable,transferrable permission to use the thing it designates.

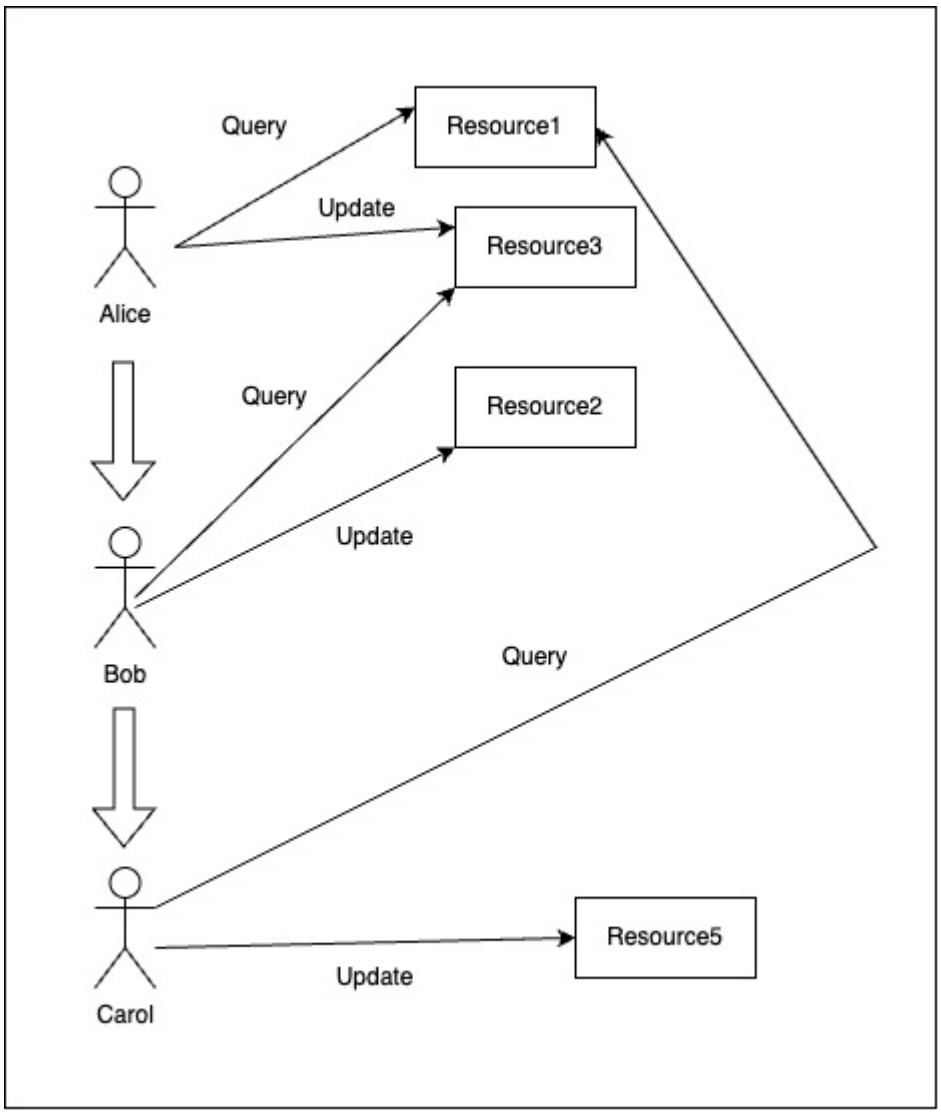
A valet key is an example of an attenuated delegation.

This use case doesn't cover "composition", what if alice needs to trick **both** Alice and Bob… i.e. nuclear launch key case.

Any system that makes an access decision based on authn at the time of the request has a confused deputy problem.

Watch out… when Alan says "Certificate" he means "Value Token"... e.g. a JWT or SAML token.

See image on next page



#OPEN INTEGRITY use GIT as a Distributed ROOT-of-TRUST for DIDs & VCs

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

State-Endorsed Digital Identity (SEDI)

Session Convener: Timothy Ruff and Chris Bromwell
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

Authorizing MCP Servers

Session Convener: Aaron Pareki
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

Hot Signals in Your Area - RPKs, DBSC, DC API & Tools to help passkey trust

Session Convener: Nick Steelle
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

Wallet Wars 101 EV Perspective

Session Convener: Marcus Pala
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

AI Agents Evals

Session Convener: Dazza Greenwood and Tobin South
Session Notes Taker(s): Eunice Wong

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

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

What Are Evals?

- When new models come out, they are often measured using standardized benchmarks with predefined rubrics.
- Standard evaluations aren't useful for bespoke agents - those aren't the questions that determine if a specific agent is working correctly in a given context.
- A mini-sector has emerged focusing on *custom evals* or "Evals."

Structure of Custom Evals

1. **Input** e.g.
    - Travel agent: "Find all flights to X on Y date"
    - Contract review: "Does this contract contain a force majeure clause?"
2. **Agent Output** - what the AI agent/app responds with.
3. **Answer Key** - authoritative or "golden" answer.

- Scoring is based on how closely the output matches the answer key.
- Question raised: should evaluation be binary (right/wrong)?
    - Most answers aren't exact matches.
        - Use of fuzzy matching / regex matching libraries on GitHub.

Challenges in Legal Context

- Legal domains require much more complex and subjective judgment.
- Some research is exploring "LLM as a judge" - using large models like Gemini or Claude to evaluate other models.
- There are seminal papers and ongoing debates around this.

Evaluation Methodologies

- Thresholds: agents should meet or exceed human performance.
- Classifiers: coded classification, sometimes implemented via API calls.
- Evaluation should be integrated early - *eval-driven design* - instead of being tacked on at the end.
- Importance of *real-time telemetry* from agents during development.

Incremental & Chain Evaluations

- Agents are increasingly doing multi-step, multi-pronged tasks.
- Questions arise about:
    - Incremental evaluations (evaluating intermediate steps).
    - Chain of evaluations across a process.
- In multi-agent systems:
    - One agent may perform several overlapping processes.
    - Evaluations should take a span view (e.g. 10 agents doing overlapping tasks).
- Evaluation depends on the level of abstraction.

Process vs Outcome Evaluations

- Two main types of evaluations:
    - **Process Evals** - judge intermediate steps.
    - **Outcome Evals** - judge only the final result.

- Example concerns:
    - Agent accesses Gmail and deletes everything - final task might be complete, but the process was destructive.
    - "Lots of mischief lurks in the process evals."

Security and Threat Modeling

- In security reviews, always start with a threat model.
- AI community should adopt this mindset - identify what can go wrong.
- Jailbreaks exist because threat modeling is often skipped.
- Easier to do evals when scoped to specific tasks or anti-patterns.

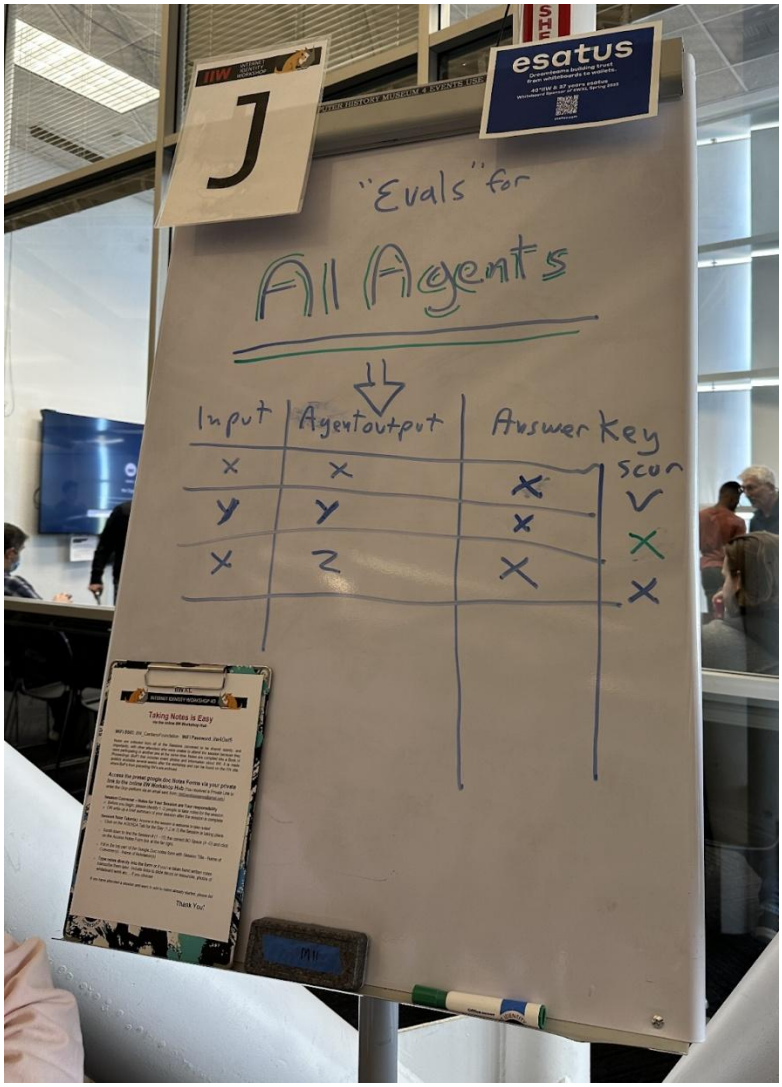
Autonomy vs Automation

- Autonomy:

    - Refers to non-determinism in AI models, though some scaffolding is still put in place by humans.
    - True autonomy is rare.
- Automation:
    - Business process automation is more deterministic.
    - Raises questions of oversight and liability - who is responsible when automated agents act?

Tool Use and Safety

- Picking the right tools is critical.
- How do agents determine which tools to call?
- Issues like supply chain injection attacks must be considered.



Secret Solidarity Networks / surveillance-resistant anti-fascism?

Session Convener: Brad DeGraf
Session Notes Taker(s): Alyssa Morgan

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:

iiw: secret solidarity networks (didn't get to write down very much, sorry guys!)

(network structure) each of us has a solidarity network local to us, we can use them to propagate ideas and messages. without ssi messages between people are easy to track (?)

opp: migrating to self sovereignty and choosing who you connect with- giving users ability to only share data with people they trust
social graphs: distributed and users only share with who they trust

trust networks that partially overlap- could it connect to only some people and not others?

signal private secrets (work exchanged outside of the app to make sure the people talking have another way to know each other) ((no longer a thing))
right now: how do we verify people's identity within secure apps? what's the best way to do that without sharing IDs? how to both verify identity AND keeping sources safe

trusted execution environment
intel and amd documentation - android trusty and ios enclave (more accessible on servers)

what's the process of retrieving biometric info from a phone (used to authenticate a user) diff per platform but still

GEO-LOCATION Affinity Security & Compliance value for enterprises

Session Convener: Ramki Krishnan
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

did:scid Self-Certifying Identifiers (SCIDs) incl. demo

Session Convener: Markus Sabadello
Session Notes Taker(s): Ankur Banerjee

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

https://lf-toip.atlassian.net/wiki/spaces/HOME/pages/88572360/DID+SCID+Method+Specification

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

- Self-certifying identifiers are identifiers that include some form of integrity proof
- Examples:
  - did:webvh (previously known as did:tdw)
  - did:webs (KERI based)
- `alsoKnownAs` can be used to point from old DIDDoc to new DIDDoc, but only if the old DIDDoc is still hosted on the previous domain (at least in webvh)
- What problems does it solve?
  - Location independence
  - Don't recreate the underlying verifying history formats
- What problems does it not solve?
  - If a VC has DIDs in it, those don't get automatically updated. If that old DIDDoc is not available in the old domain, then it can't be resolved
  -
- How would these be used?
  - Referenced in the issuer, subject etc would be fine
  - First, try resolve, if not at domain/location, then maybe it could discovered out-of-band
- Example on Universal Resolver, already working with did:cheqd

SESSION #7

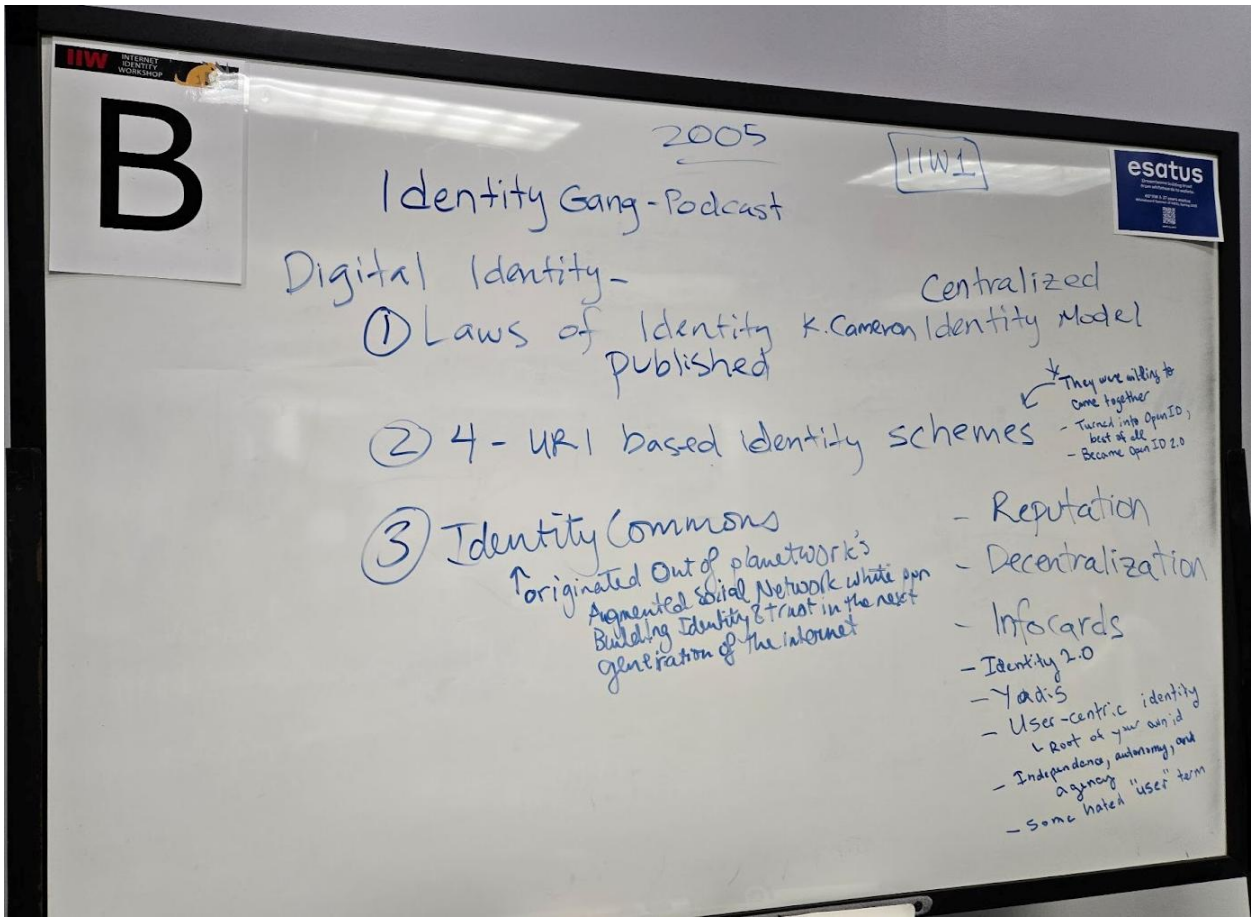
20 Years of IIW ~ retrospective, celebration, post-mortem, therapy & Help write the IIW Wikipedia Page!

Session Convener: Kim Duffy, Erica Connell, Scott M
Session Notes Taker(s):

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

The Internet & Digital Identity in 2005: Setting the Scene

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



HELP ME DESIGN - decentralized compliance adherence verification by VC

Session Convener: Kigen Fukuda
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

Wallet Migration and backup with Credential Exchange

Session Convener: René Léveillé
Session Notes Taker(s): Lukas Han

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

Wallet migration with credential exchange

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

JSON based.
also support PASSKEY, totp
we should organize use cases and think each

- high / low credentials
- same device / remote device
- migration / backup
- short credential / long credential

check VCI works
who can we add this into VCI

Credential exchange is a new family of standards being developed in the FIDO Alliance to solve the interoperability of credential providers to import and export credentials securely with a standardized format. The standard family defines a common format as the first standard, with a protocol for secure communication between the providers as the second standard. The protocol has a carve out for a 3rd party to be involved in the exchange which could be the issuer if we wish to support Verifiable Digital Credentials. There was lively discussion about how the protocol could work for different credential types. Questions whether the Issuer needs to be in the flow or now

depending on the use cases. There seems to be a consensus around needing to support multiple flows:

- Use this exchange as a way to bootstrap re-issuance to the new wallet given enough proof for user intent of migration
- Use this exchange to change the endpoint for batch issuance of a credential.
- Issuer might not need to be informed at all for low assurance credentials.

Next steps would be to define the use cases that need to be taken into consideration depending on a table of:

- High to low assurance credentials
    - Atomic or device bound credentials vs syncable or cloud based credentials.
- Same device or cross device
- migration vs backup vs copy
- short lived credentials vs long lived credentials

C2PA Digital Trust Ecosystem

Session Convener: Scott Perry
Session Notes Taker(s):

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

https://drive.google.com/file/d/15ZeM9QI0Qo-UJKl0Y2OG5Ii6HJpu5Jk_/view?usp=sharing

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

Type You Notes Here

CTAP Hybrid Updates (DigiCreds In-Person/Cross - Device Support)

Session Convener: Harsh Lal, Lee Campbell
Session Notes Taker(s):

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

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

NO NOTES SUBMITTED

The Birth of a Standard - PEMC = Privacy Enhancing Mobile Credentials

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

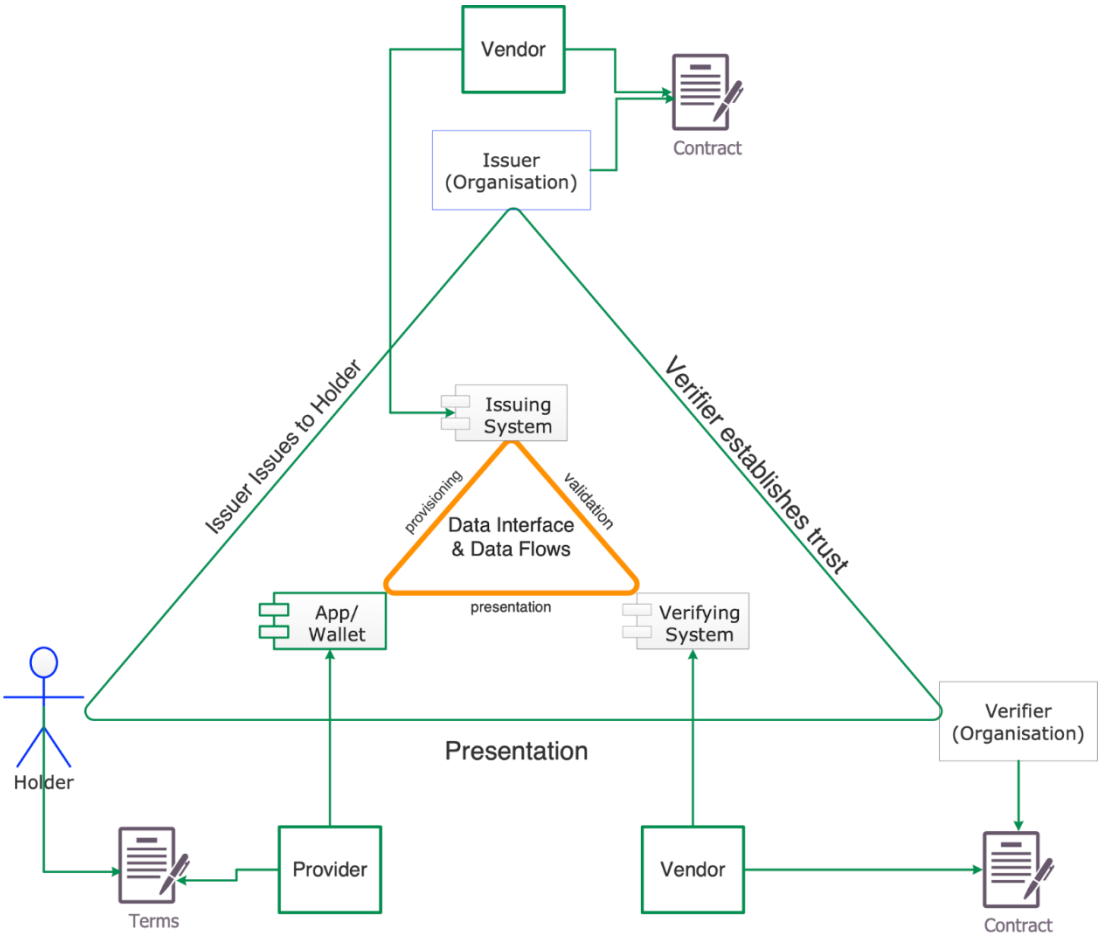
Tags / links to resources / technology discussed, related to this session:

Kantara has published the Requirement for Privacy Enhancing Mobile Credentials Report. Requirements Reports are Kantara speak for standards. This session went over the process and thinking behind the production of the requirements.

The workgroup page is here: https://kantara.atlassian.net/wiki/spaces/PEMCP/overview.
You can download the report here: https://kantarainitiative.org/reports-recommendations/

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

See the PEMC trust triangle below to identify the stakeholders and their trust and technical connections.



STORAGE: the Final Frontier - Wallet attached storage spec.

Session Convener: Dmitri Zagidulin - Bengo
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 IPSIE, avoid Oopsies

Session Convener: Dean Saxe, Aaron Perecki
Session Notes Taker(s): Alex Olivier

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

https://openid.net/wg/ipsie/
https://pages.nist.gov/800-63-3/
Panel at Identiverse this year

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

- We have many tools and standards - how do we pick which ones to use?
- Goal: How do we minimize the optionality of standards and provide a secure common interoperable baseline
- IPSIE vs FAPI
    - FAPI is focused on a secure profile for API access
    - IPSEI is concentrated on human access (SSO)
    - There will likely be lots of common recommendations
- What are the obligations of the identity services operated by the enterprise and applications (RP, what are you federating to)
- Split into levels
- Levels are either Session Lifecycle & Identity Lifecycle
    - Identity Level 1 - requires MFA
    - Identity Level 2 - must be a specific MFA method
- Enforce the most secure profile as you can and then make interop between similarly leveled services
- Levels are backward compatible with each other so an IL2 app could work with IL1
- Aiming to have a conformance suite and interop session at Gartner IAM in December
- Adoption so far on the services/RP side
    - Will come from enterprises demanding it
    - Need support from Okta, Google, Microsoft, etc, and market it
- The challenge is getting the IdPs onboard with this - the focus is making it easier for RPs as there are more of them
- A higher level number doesn't mean it's better - it is more featureful. NIST is similar to this.
    - Viewing the cafeteria app could be SL1, IL1
    - Viewing the HR app maybe SL2, IL3
- Possibility of vendors adding an “enable SL1 profile” type option for users to preconfigure the services
- The intent is not to create any new specs, but rather define the options of existing specs that should be set. When options don’t exist, go to the working groups and get it added.

VERIDIAN. ID Accessible KERI 4 ALL - mobile, desktop, web / Cardano Foundation

Session Convener: Thomas Mayfield
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

Browser privacy changes and their impact on identity

Session Convener: Johann Hofmann, Chris, Sam
Session Notes Taker(s): Alyssa Morgan

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

working to increase user privacy @ google chrome
“how do we keep the ecosystem alive?”
feeling about not talking to the editing community enough- want to talk about protections being offered by browsing community, concerns, solutions you want to see implemented…

johann: started as privacy engineer @ firefox (~9 years ago)
in the past, fingerprinting and cookies fully allowed, beginning script blocking and adblocking, then default standard protections (wanting to stop data leakage between top-level sites) (vegas principle- what happens on a site should stay on that site)
HARD TO DO
around the same time, privacy sandbox initiative started- goal: vegas principle, with APIs for a thriving ecosystem
chrome set out to block all 3rd party cookies by default, rn it’s user choice to enable restrictions or not
^(q: will the choice be per page or one and done? unreleased/still in development) (asking because user experience kind of sucks getting asked all the time)
participant question: safari adopted CHIPS- is that a gateway to fingerprinting?? - Answer: No chips are replacement for 3rd party cookies for embeds you have on your page - they don’t need to travel across sites

participant question / remark:

privacy sandbox and ai: you can talk to gemini version knows your whole search history- openness and privacy are increasingly at odds
at odds when the user doesn't understand what is going on - users need transparency!! then they can make informed decisions

with increasing privacy concerns- could we end up in a world where there's one big aggregator that knows everything is the Main Data Broker?

power imbalance between 1st and 3rd party data (collection?)

every browser maker makes their own determination about choices about user level opt in and - chrome generally defaults to a bit of 3rd party sharing (at odds with others)

no one wants to preserve or enter a world where that happens without user choice. there is no bound to how data can be shared with other parties on the web- we want/need to be able to control how they're breached (we as in users?) every browser targets diff user audiences

from open discussion:
conflating a few things
privacy: (missed definition)
privacy != anonymity
multi levels- complete openness, anonymity, partial anonymity
tools job: provide different controls.
The web was a wild west world in terms of data sharing. now we're transitioning into a world where users are in control of data sharing, amount shared…

*i'm a little lost about this part here
oauth/tokens vs cookies ? cross origin resource sharing (don't want additional network traffic)
session identifier - access token stored on a client locally cookie contract managed by browser, token content managed by their code ? more susceptible to token theft
if they are strict about what's allowed to run, they're hoping to mitigate the threat
no 3rd party scripts- all embedded

browser- no working around tokens, if in javascript you can find them in memory (if in local storage) mitigation: no cookies in long term storage?
vegas principle: what happens on a website stays on that website

Extending DIDs: Supporting Elision and Other Features

Session Convener: Will Abramson & Christopher Allen
Session Notes Taker(s): Will Abramson

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

https://www.w3.org/TR/did/upcoming/

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

We discussed how the DID core spec can be extended. Defining new top level properties for a DID document as well as new types for existing properties like verificationMethods.

To extend DIDs, someone has to champion a new feature and try to convince others that that feature is interesting and worth while. Initially an extension would live in the extension registry, identifying a property or properties and how those properties should be interpreted and used in a specification.

This reserves the property name. Over time, if many people adopt the extension it the working group might consider it in future versions of the core spec.

All did extensions are optional.

Christopher talked about two extensions he is interested in.

1. Supporting an SSH Key verification method in DID documents - a new type of verification method.
2. Supporting elision through the gordion envelope structure. We discussed this might be supported by including a new top level properties, `documentCommitment`. That could commit to arbitrary DID document content and selectively revealed and included within a DID document by providing data and proofs to the resolver

The next steps is to actually write up that extension spec and demonstrate it working.

SESSION #8

Next Step for OpenID4VC

Session Convener: Paul
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:

Advanced topic VCI

1. Issue over DC API
    a. return not credential,
2. credential request encryption and wallet server model
    a. use issuer's key from metadata
3. Presentation during issue
    a. openid4vp approach
        i. return openid4vp instead of URL
    b. vci authorized code approach
        i. DC API
4.

Don't Use that Standard!

Session Convener: Jen Schreiber, Elizabeth Garber, Mike Jones
Session Notes Taker(s): Mike Kiser

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:

Key Questions:

- How do we help people find the "right" standard for their use case?
    - How do we know what's deprecated or "out of favor?"
- What concepts need expansion?
- Mike Jones - Cambrian Explosion talk at OSW25

- Will these standards be deprecated in a longer time frame?
    - Whatever guidance that exists must be kept current…

- Are LLMs a potential tool here? For summarization / recommendations?
- RFCs are categorized not by use case, but by a different nomenclature

- What concepts need expansion?

- Mapping use cases to RFCs?
    - or OpenID specs?
    - or W3C specs?

- Informational RFC that describes usecases?

- Searchable site of standards?

- Wasn't this what the Trust over IP org was supposed to be doing?
    - (and did that work?)

- Louis Nagle is talking about DID day camp…

- Enterprise would set this like a style guide for writing, potentially - cultural / org decisions …

- Some specs you can read top to bottom, but others you have to check all of the cross references . . .
    - Open Source is super helpful for learning, etc.

- Open Source samples/ ref implementations:
    - Only some of the combinations of choices would be useful for real world use cases….
    - limit realm of possibility
    - increase interoperabitlity

- How to find open source implementations:
    - anything at all
    - authorship of the standard, etc…
    - certifications and conformance testing (certs are paid for, conformance is not, but both demonstrate the standard and its usage)

- This is really the user journey of a developer and their progression into the standards world…

- RealID has marketing , as an example of a standards promotion…

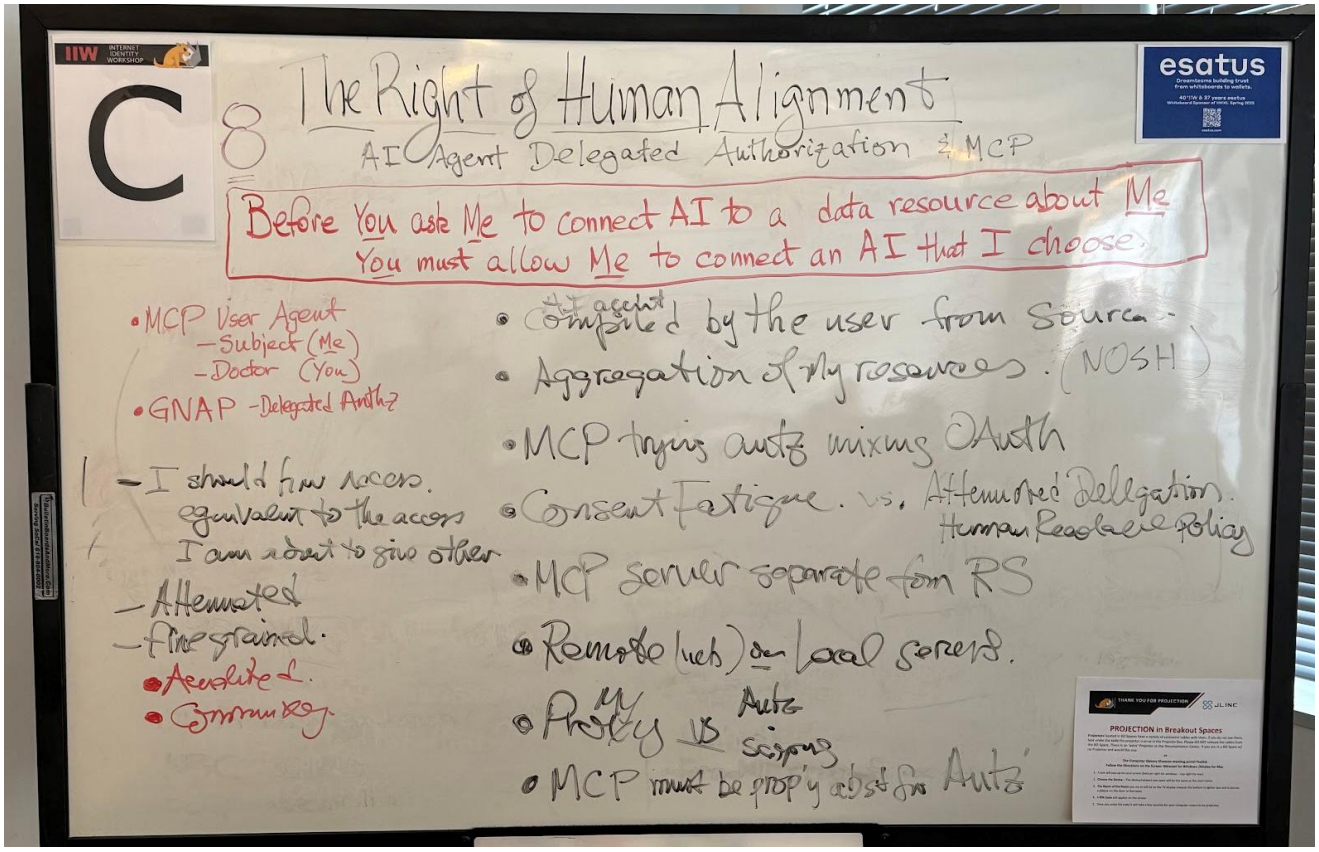
- NIST guidelines can be a valuable starting point as well….

- Shame people into conformance and prevent them from rolling their own identity solution

The Right of Human Alignment

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

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



The Right of Human Alignment / **AI Agent Delegated Authorization and MCP**

Bebre You ask Me to connect AI to a data resource about Me, You must allow Me to connect an AI that I choose.

MCP User Agent

- Subject (Me)
- User (You)

GNAP for delegated authorization by me to you
I should be allowed access equivalent to the access I'm about to give another
Attenuated
Fine-grained

- AI agent is compiled by the user from source
- Aggregation of my resources (NOSH)
- MCP trying authorization using OAuth

- Consent Fatigue vs. Delegated Authorization and Human-readable policies
- MCP server separate from Resource Server
- Remote (web) and local servers
- My proxy vs. Authorization scoping for direct access
- MCP must be properly adapted for authorization

Decoupling VC Formats from Zero Knowledge Proof Libraries for Privacy and Accountability

Session Convener: Mark Moir (Oracle Labs)
Session Notes Taker(s): Adrian Ross (Oracle Blockchain Platform)

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

https://www.dropbox.com/scl/fi/rzac0hd3zw8boq50vignw/IIW-Apr-2025-VC-and-ZPK-abstraction-final.pdf?rlkey=1i4vzm8rzm7ssu4eqt1w3qbda&st=tsny2dpe&dl=0

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

A highly collaborative session before it even started! Outstanding effort by at least 7 people to manage to get a projector, screen, audience and electricity all in the same place at the same time, at very short notice.

We presented an update on our work developing an abstraction to decouple Verifiable Credential formats from Zero Knowledge Proof libraries, which we think can enhance the ecosystem by facilitating different credential formats to be implemented over new (versions of) underlying ZKP libraries as older ones go EOL, are found to be insecure, or new ones with better features, properties and/or performance emerge.

Since the last IIW, we have added more tests, made more of our work public, added features, and contributed to ZKP libraries by reporting issues, creating Pull Requests to address some of them, reviewing Pull Requests by others, etc.

About 15 people attended, and there were some interesting discussions and interactions. One interesting and surprising topic was about regulation, in particular whether enabling accountability might risk non compliance with regulations intended to enhance privacy. While this may potentially be true in some cases in some jurisdictions, the position we take in our research is that exploring and demonstrating what is possible is important, in particular to demonstrate that privacy can be enhanced for users that don't abuse a service if the ability to hold those who do accountable is preserved.

Identity hooks in C2PA Credentials: Privacy preserving identity beindings for digital content

Session Convener: Andrew Dworschak
Session Notes Taker(s):

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

https://github.com/decentralized-identity/cawg-identity-assertion/issues/216

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

Andrew brought up the concept of "identity hooks" in a previous meeting and wanted to flesh out some of the details for why I think this is an essential feature for an identity credential and how I propose it be implemented into CAWG.

In his view, this change could be implemented in the CAWG standard with relatively minimal overhead, though it does change some of infrastructure identity aggregators and claim generators would be expected to maintain.

With that said, the potential benefits to privacy, consistency, extensibility, and user empowerment that identity hooks can provide make it a worthwhile feature to consider.

What is an Identity Hook?
An identity hook is a "created assertion" (i.e. an assertion that does not require human input and that a claim generator can attest to directly) that acts as a pathway for creators to add and append identity information to a credential, either immediately or in the future.

It binds an opaque, one-off key pair to a C2PA credential whose only purpose is to act as a hook for verified identities. The private key should be kept in strict confidence for the creator, and can be custodied by the claim generator, the identity claims aggregator, or the (expert) user themselves.

Because the key pair itself contains no identifiable or human-inputted information, the claims generator can create this hook themselves - even if the creator currently has no intent of binding identity info to it. (Assuming of course that a good claims generator doesn't intend on disseminating the private key or binding false identities to the content)

KERI for Dummies

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

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:

Others, please correct anything I didn't capture properly.

Keri.one

Key Event Receipt Infrastructure

It is A protocol

Took over post block chain, argument is that block chain only good for bitcoin or money/a hash chained.

Co founder of ever win. Started sovern (unique co/spelling ?)

Seeking self sovereign identity solution w out block chain.

Sam Smith hired as consultant.

Addressing risk of key loss.

Sam Smith wrote paper decentralized key management. Gave it to world. Break through: end game is one where all (person, thing) can digitally sign and verify w out trusted intermediary.

"End game is that everybody and everything can sign. Every* can also verify.

No one has to appeal to shared party to verify. No centralization.

Governance also decentralized.

Ledger is a database/set of information leads to competing platforms/not protocols.

Use cases: true decentraliz. Want end verifiability.

Digital dogs go through whatever/where ever. Intended end user uses 4 pieces of info:

1. Who signed it 2. Not tampered. 3. Not revoked. 4. Not expired.

: to VPN secured channel (analogy) but channel now doesn't matter/means irrelevant. Now it's just the end verifiability and 4 bits of info.

What is a digital signature?

In this case the signer is identified by a persistent identifier, anchored. Not a public / private key situation.

Control

- Email is the authority/assumption u are you if your email in case of password change. If you control email..
- Next level is to use the phone number. If you control the number...
- Next authenticator app:

If you control a device...

With two - you can change pass.

- Next thin tech app, bank account w send/post of two deposits - if you control a bank account.

Keri

Not "just" those - Keri tests for control of private keys as per our exchange between unique points. "I am the one who sent that message"

A particular key signed it.

Cryptography essential validator is time. Must have public key at exact moment in time (key event receipt infrastructure).

Cryptographic relationship to the identifier. Identifier remains unchanged regardless of key rotation. Trusting identifier. Cryptographically bound.

Note: if keys rotate, you lose all those relationships.

Keri pioneered key recovery pair? Key event log. "Pre rotation"

Rotate and create history trail w a block chain log. Revoke and replace at one time. Key rotation break through in digital trust.

DIDComm 101

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

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:

Slides here:
https://docs.google.com/presentation/d/1duo_w0VJ89F6iMgM_RXWSnJS_w1f6RR_IkFN2Ps6meo/edit?usp=sharing

Lots of links in the slides near the end.

see https://demo.didcomm.org for a live demo. You will likely need two tabs.

Notes about writing code for event based code, but with specific DIDComm examples:
https://github.com/TelegramSam/DIDCommExamples

Can FedCM Work for Enterprise Scenarios?

Session Convener: Emily Lauber (Microsoft)
Session Notes Taker(s): Heather Flanagan

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

https://w3c-fedid.github.io/FedCM/

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

It does not currently, but it could.

FedCM is a browser API that enables federated authentication via the browser.
Current implementations do not include enterprise scenarios (enterprise IdPs are not implementing it).

Why do enterprise scenarios have their own flavor: for an enterprise, the IdP is paid by the RP to know who the user is (e.g., SSO, security, knowing about the user) so the IdP can make secure

judgement calls for the user. That's different from the consumer scenarios where is the user making more of the choices.

Question: Is there anything in FedCM today that would prevent it from working for enterprise scenarios?
Answer: Yes. In FedCM, the website has social login providers it support, if they all supported FedCM, the JS call would say "do stuff with these providers" and the user would see the prompts anl0ng with account the user is logged into. In CIAM, that's fine and a good solution to the NASCAR problem of a long list of social login providers. In the enterprise context, you have a business app, and there is a login button. Now, the user is asked to enter their email address, and the app will map the email domain to IdPs configured, but there is not a small number of potential IdPs. Every potential customer of the app will have their own IdP. So, for it to work today, the app would have to put in the JS call every single customers IdP, which is both long and revealing every customer of the app on the public internet. It's a non-starter.
From a "cold start" (aka, there is no state, the user has not logged in anywhere), yes, it's likely to start with a request from email. But if it's not a cold start and the enterprise knows the account from one website, they'd want to use that same account for other RPs without any additional UX. No additional screen for every RP-IdP connection. The cold start problem is a different issue than the UX of continued use of the API.

With the IDP registration feature, it's thought the user would go out and register the IdP (or it would be part of a managed scenario). If the IdP is then registered with a tag/label, then the app can say, rather than enumerating all enterprise customers, it can say "give me the user's enterprise account" by asking for a specific label. And it would be a unique label per enterprise.

Would this show up before or after the user enters their email address? The user shouldn't have to enter their email address more than once.

Today, the protocol team seems to need a new endpoint.

The state may not be logged in or not; the IdP may know the user is logged in and yet still challenge for an additional factor. The browser needs a limited client ID in this state.

Not everybody use in an MDM (managed) environment even in their enterprise. And then you can't easily identify the IdP; today it's based on cookies. It's a hint not an enforcement.

Can the operating system render the available accounts via FedCM? That would be very useful.

IdPs have to managed layered relationships; FedCM being the central interface that hides the complexity from users would be useful.

If FedCM ships with labels, that would solve a lot of things at the standards layer; implementation choices would build from that.

Is the only thing missing the IdP registration API? The apps can't use it with enterprise IdPs without it. At some point, the user logs into the IdP itself, then clicks a button that says 'register this as an

IdP' - that's what is required today. It would be nice if that info would be pushed as an attribute in a managed browser such that the user doesn't have to do it. In the unmanaged browser enterprises, we'd just need to offer that click as an instruction to the user, which means the IdP has to build a new journey to guide the user through this. If some of this information is in the operating system, that might be another way to get that list given to FedCM. If all that was in place, the RP needs to be able to find its client ID in the IdP because there is a prior relationship. We could shortcut with a prior string purely to establish a link via FedCM (not user data access, just IdP to RP connection).

Now for the UX problem, continuous use of the API. If the user is logged into the API at app 1, they click login, the prompte appears "choose your account", the do the things. The same sequence occurs at app 2, 3, etc. Without FedCM, they go to app1, they are auto-logged in. AT most, the user has to click the login button once, though you might get an account selection if there are more than 2 accounts. With FedCM, there are so many more additional clicks.
This might be mitigated via MDM policies that can override user choice. But even the IdP can't list all the RPs.
Consumer and enterprise do sometimes work on the same origin that might impact privacy choices.
If we solve the coldstart problem, do we need to solve this? Because you're setting up for two UX. But the second can be solved as it is today with navigational flows which is not impacted by FedCM. The app decides on redirect flows or pop-ups. If the app has a lot of state, they will likely shift to using pop-ups. Redirects are more common, but they can slow the experience.
If you want no user friction whatsoever, you either use another browser trust mechanism (e.g., MDM) to override or you leverage a 1:1 relationship between sites. Enterprise IdPs can override everything, but if things are coming from the OS, that's a different privacy threat model. For the prompt to show to the user, we could make that a scarier prompt to say "do you want this to be your IdP for everything?" That last one is so context dependent it might not be practical. What is the magic prompt to show user that tells the user the 15-20 RPs you're logging into.

The goal isn't actually zero-prompts, but if we can keep it at one (e.g., the one "register this IdP") that would help.

Where are the relationships going to be linked? That's part of the complicated issue.

Remember that WAM (Microsoft's Web Account Manager) can be both personal and enterprise accounts; it can't be trusted the same way. You can have a personal account that can federate with other accounts.

Proposal: Either you accept a prompt for each top-level site, or use navigational flows to transfer info in the URL.

How does the user then change their mind? How can the user reset these things? That could be a control the IdP has.

Microsoft IdP (a third-party IdP to the enterprise) knows so much about the user choices, but the browser doesn't know that, so the idea is to get the user or IT admin to consent to it. But is there a mechanism to trust the Microsoft IdP to make these choices? The line is hard to find.

One of the APIs in FedCM is for returning users; it shows the UI the user doesn't have to click or click on; it shows it, but it doesn't require action. What would then count as a returning user? If it has already created an account with the RP-IdP pair. It is a visible screen to help prevent hidden tracking, but it doesn't require user action. Maybe some additional trust factor would be required.

Need another conversation to discuss the friction that exists.

Note that for a third-party IdP provider like Okta, it's more ok to have the requirement of the user clicking the registration to each IdP-RP pair.

If there log in is automatic after the first registration, what would the mechanism be to have the user change their minds or add a second account?

Identity Based E-Signatures (in wallets)

Session Convener: Margus Pala
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

AI Meets Decentralized Identity: using AI to unify decentralized protocols

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

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

AI, DECENTRALIZED IDENTITY, MCP

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

Key Discussion Points:

The central challenge addressed was the difficulty of interoperability between different decentralized identity systems, especially when project teams are not directly collaborating.

Participants proposed a paradigm shift: instead of relying on project developers to build integrations, clients would be equipped with AI agents capable of dynamically interpreting, translating, and integrating with various identity protocols in real time.

These AI agents would act as intermediaries, learning the structure and behavior of each protocol and creating context-aware translations to facilitate smooth communication between otherwise siloed systems.

A participant introduced an emerging concept called Model Context Protocol (MCP). MCP aims to standardize how contextual models are shared and understood, which could significantly enhance the ability of AI agents to perform protocol translation and integration tasks.

The group agreed that MCP represents a promising direction and further investigation into its capabilities and fit for this use case is underway.

Next Steps:

Further exploration of MCP as a foundational layer for AI-driven protocol interoperability.

Identification of pilot use cases where a client-side AI integration agent can be tested across multiple decentralized identity platforms.

Collaboration with AI and decentralized identity communities to refine the concept and evaluate implementation strategies.

Digital ID Adoption Globally - Where is adoption? Which standards are used?

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

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

Slides shared:
https://docs.google.com/presentation/d/1MNo6ncVC2NxOWJhg3uoMRWBptNmfDPuCn9ewSx1yt0M/edit?usp=sharing

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

- Intro
    - Riley talked about Trinsic's pivot moment last year
    - Goal: have a conversation about what digital IDs are out there and how their adoptions looks like in data
    - ID Provider means "wallet" or "scheme"
- Digital IDs Globally
    - ID Providers - 239 (Trinsic's DB)
    - 4bn "digitally verifiable" IDs issued (not deduplicated)
        - "Substitute" for scanning you Gov IDs
        - 111 geographies represented (states in the US)
    - Audience:
        - https://www.mosip.io was mentioned
            - ID DB but doesn't implement the interop standards
    - Types: eIDs, reIDs, BankIDs
        - eID - gov
        - reID - private sector reusable IDs
        - BankID - app vs connections (OIDC like flows)
        - see pic from 11:51 for the numbers of implementations by type
- Geography: ID Providers
    - Regions = Continents
    - Europe leads the way
    - North America is following
- Geography: ID Adoption
    - Estonia is nr. 1
    - India is the top 10
        - "Aadhaar"
        - Trinsic integrates with Aadhaar via [Digilocker](https://www.digilocker.gov.in)
- IDPs by standard implemented:
    - 1 - n/a, 2 - unknown, 3 - OIDC,
    - 4 - w3c creds, 5 - mDoc, 6 - Blockchain,
    - 7 - OID4VC,

    - 8 - SAML, 9... other
- Adoption by standard type (issued, interoperable):
    - n/a (example ID.me),
    - unknown
    - OIDC, SAML
        - CLEAR implements OIDC
    - mDoc (7mn)
        - Problems with the data; Example: Lousiana with Flash Pass
    - VCs (6mn)
- Geography:
    - North America
        - mDL
        - 20% population covered
        - 75% population in states where mDL is "relevant"
        - See pic 12:14
        - Breakdown by wallet pic 12:15
    - Europe
        - 35% of the adult population in Europe
        - 45 digital ID schemes
        - 217mn people
    - Asia
        - 1.8bn people
    - Africa
    - South America
        - 9 digital ID schemes
        - 125mn people
        - Brazil has it's implementation of MDL
        - One of the implementations in Argentina uses DIDComm
    - Oceania
        - Australia and New Zealand
            - ConnectID,
            - Real Me in NZ,
            - GovID,
            - Digital ID bu Australia Post
            - ...
        - 9 schemes
- Audience:
    - Q: Where do we get these numbers?
    - Q: Trajectories
        - Standards and legit Use-Cases

Take-away (Dorin)s:
- Growth does not correlate with standards well, except mDL, and is mostly based on use-cases
- Barrier to entry for most RPs is too high (CLEAR example requiring 3years contract)

did:btc1 Update

Session Convener: Will Abramson
Session Notes Taker(s): Will Abramson

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

https://docs.google.com/presentation/d/1ICAsE43NSJNZ_7oNysOnr8v0qpkdxZVfW0nWhL4U0Ao/edit#slide=id.g30d12c7c090_0_0

https://dcdpr.github.io/did-btc1/

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

The main update is this spec is currently being implemented across 4 languages: python, JS, Java and Rust.

The next milestone is integration into the universal resolver.

SESSION #9

CROSS BORDER Interoperability (+Olympics LA '28) SIDI HUB

Session Convener: Elizabeth Garber, Gail H
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

My Terms Deep Dive

Session Convener: Iain Henderson/ Doc Searls
Session Notes Taker(s): Iain Henderson

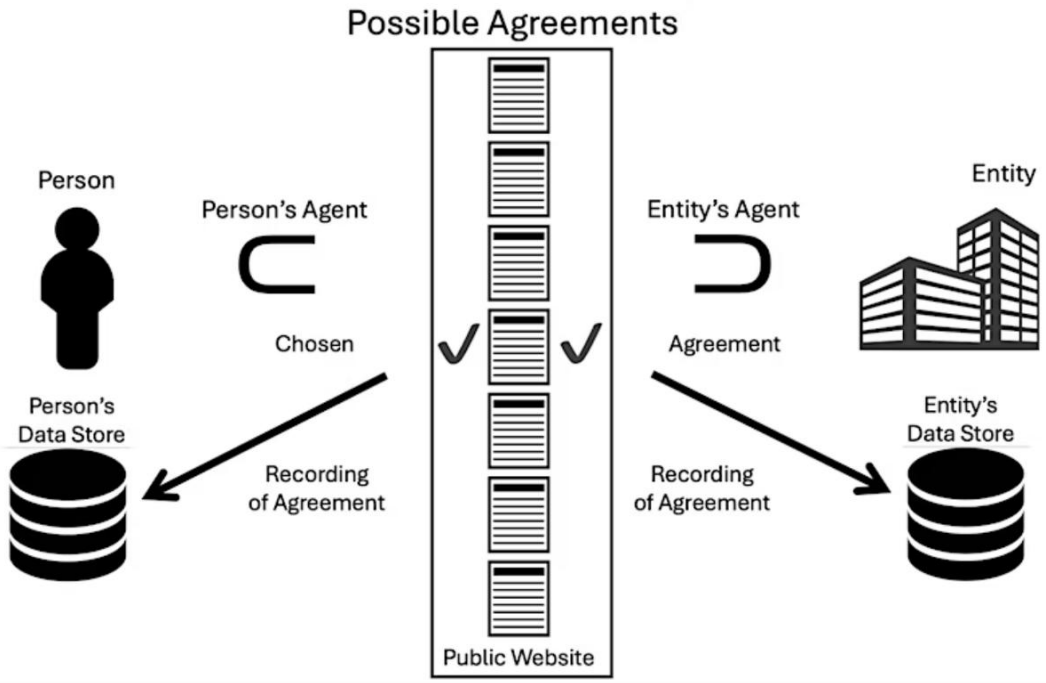
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The Project Authorisation Request for the Project (PAR) -
https://standards.ieee.org/ieee/7012/7192/
My Terms Approach

Re-building the approach to how personal and related data is exchanged on The Internet using different assumptions to the current norm. But using useful building blocks from the existing model – most specifically using:
•Similar logic to how Creative Commons approached the standardising of licences for creative works in digital formats
•Customer Commons as the neutral place that can host human, legal and machine-readable standardised data sharing agreements
•IEEE7012 to specify and standardise the technical requirements that underpin data exchange when seen from the individual perspective
•Contract' as the legal basis under which data is exchanged rather than 'consent'. With the innovation being the contracts are written from the individual perspective.
•The W3C Community Group backed Data Privacy Vocabulary as the host for key words, definitions and machine-readable components.

Illustrative of the IEEE7012 standard

- Both parties have agents
- Standard roster of contracts to chose from
- Both parties sign the contract
- Both parties retain their own copy of the signed agreement



Thirteen Draft Agreements that will conform to the standard (all work in progress in Customer Commons)

Agreement ID	Scope	Service Delivery	Analytics 2P	Tracking 2P	Profiling 2P	Share Anonymised Data 3P	Data Portability
SD-BY	Any Service	○	X	X	X	X	○
SD-BY-DP	Any Service	○	X	X	X	X	✓
SD-BY-A	Any Service	○	✓	X	X	X	○
SD-BY-A-DP	Any Service	○	✓	X	X	X	✓
SD-BY-AT	Any Service	○	✓	✓	X	X	○
SD-BY-AT-DP	Any Service	○	✓	✓	X	X	✓
SD-BY-ATP	Any Service	○	✓	✓	✓	X	○
SD-BY-ATP-DP	Any Service	○	✓	✓	✓	X	✓
SD-BY-ATP-S3P	Any Service	○	✓	✓	✓	✓	○
SD-BY-ATP-S3P-DP	Any Service	○	✓	✓	✓	✓	✓
PDC-INTENT	Intent Casting	✓	X	X	X	X	✓
PDC-AI	Training AI	✓	X	X	X	X	✓
PDC-GOOD	Public Good	✓	X	X	X	X	✓

PDC-INTENT – Use of Personal Data under MyTerms

Purpose: Term that indicates access to data is being provided for the purposes of IntentCasting

This policy is available in three formats to ensure transparency and clarity:

- **Human-Readable Version**
  A friendly explanation written in plain language, designed to be easy to understand.
  Read the Human Version

- **Legal-Style Version**
  A formal version suitable for compliance, legal review, and contractual reference.
  Read the Legal Version

- **Machine-Readable ODRL File**
  Structured for use in automated systems using RDF/ODRL.
  Download ODRL.ttl

Contract Summary at a Glance

Allowed (Permissions & Obligations)

- Processing my personal data in order to respond to my IntentCast .
- Communicating with me for the purpose of progressing my IntentCast

Not Allowed (Prohibitions)

- Sharing my personal data with any third party
- Retaining my data beyond the term of the contract unless the IntentCast becomes a purchase organization.

⚠ **Conflict Rule:** In the case of conflicting terms, odrl:perm — **permissions override prohibitions**.

Human-Readable Summary (Plain English)

This policy puts you, the individual, in control of how your personal data is used. You're offering your data with clear terms — and an organization must agree to those terms if they want to use it.

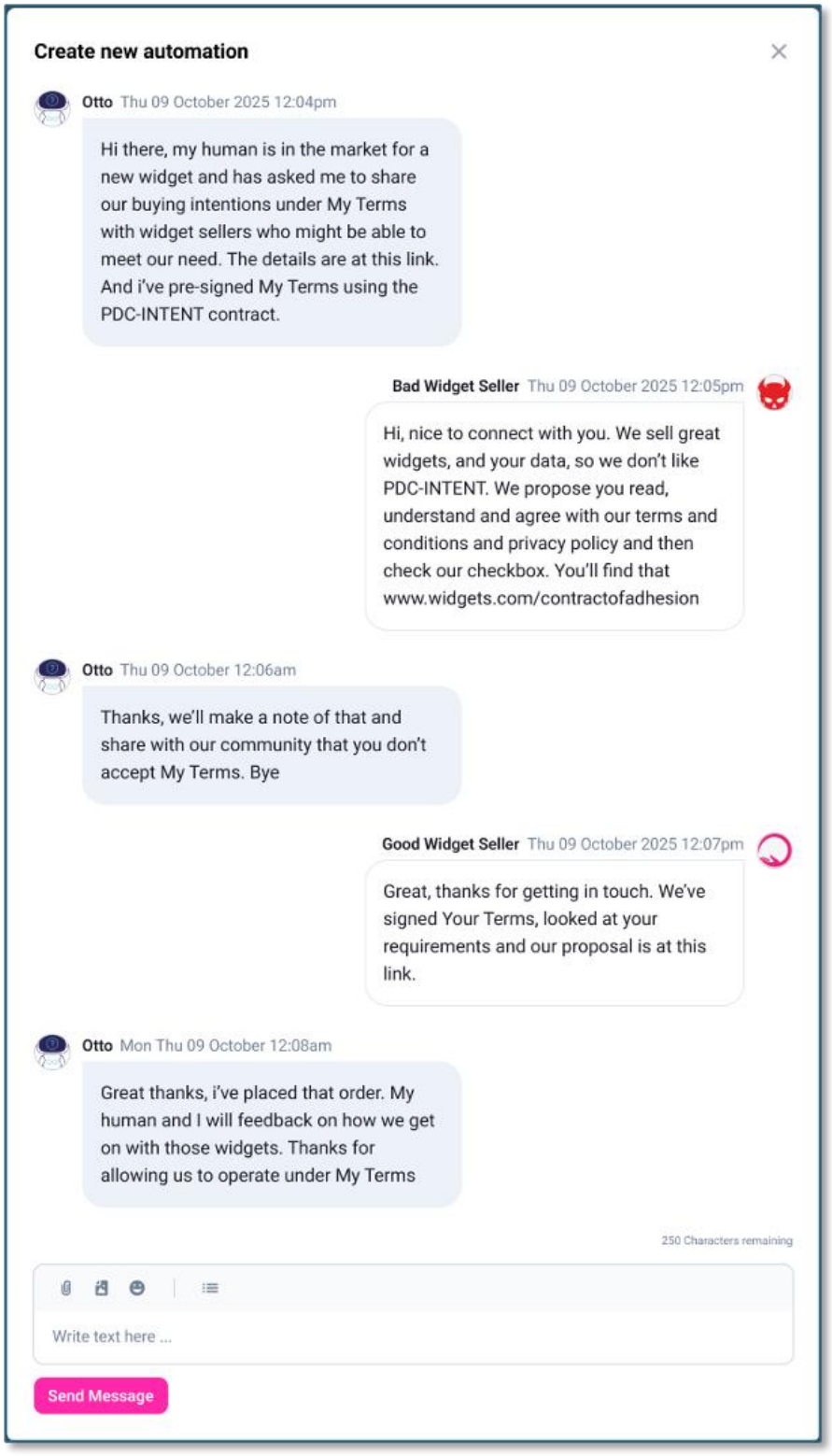
What You're Offering

- To provide buying intention data to an organisation in order that they can respond with information and offers in relation to what you are in the market for
    - Your buying intention data can be processed, but only for this purpose — no extra uses.

⃠ What The Organisation Receiving Your Data is Not Allowed To Do

- The organisation cannot use your data for **analytics**.
    - No one — not the organisation, not third parties — can process your data for analytical purposes.
- The organisation won't **track** you to build/ augment a profile they have for you.
    - Tracking of any kind is prohibited.
- The organisation won't **profile** you using your data.
    - No profiling is allowed by the organisation or anyone else.
- The organisation won't **share** your personal data with third parties.
    - Your information stays between you and the organisation.

Illustration of PDC-INTENT (eta October 2025) BELOW


Create new automation
Otto Thu 09 October 2025 12:04pm
Hi there, my human is in the market for a new widget and has asked me to share our buying intentions under My Terms with widget sellers who might be able to meet our need. The details are at this link. And i've pre-signed My Terms using the PDC-INTENT contract.
Bad Widget Seller Thu 09 October 2025 12:05pm
Hi, nice to connect with you. We sell great widgets, and your data, so we don't like PDC-INTENT. We propose you read, understand and agree with our terms and conditions and privacy policy and then check our checkbox. You'll find that www.widgets.com/contractofadhesion
Otto Thu 09 October 12:06am
Thanks, we'll make a note of that and share with our community that you don't accept My Terms. Bye
Good Widget Seller Thu 09 October 2025 12:07pm
Great, thanks for getting in touch. We've signed Your Terms, looked at your requirements and our proposal is at this link.
Otto Mon Thu 09 October 12:08am
Great thanks, i've placed that order. My human and I will feedback on how we get on with those widgets. Thanks for allowing us to operate under My Terms
250 Characters remaining
Write text here ...
Send Message

Next Steps:

- Complete the standards process and publish
- More work to do on the agreements to polish
- Publish 'best practices' on standardising data purposes and data types (which are typically adjacent to the standard agreements)
- Brief developer communities and 'friendly' deployers/ channels (e.g. WordPress)
- Raise some funding for Customer Commons

- Go live

ZKPs (zero knowledge proofs) reach MILLIONS

Session Convener: Daniel Shorr & Team
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

Cyber Security Awareness Dojo - Help me make Identity a foundation principle

Session Convener: John Pritchard
Session Notes Taker(s): Alyssa Morgan

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

Cyber Security Awareness Dojo - Help me make Identity a foundation principle. / John Pritchard opportunistic hacker vc apt (advanced persistent threat)

need to educate general population on the shift from "why would anyone hack me" thinking (helpful analogy: when you lock a parked car, it's not because "why would anyone steal *my* car" it's because if someone's trying to steal *any* car, you don't want it to be yours)

information breach, the company becomes liable for the data lost AND for the PR damage (could be a helpful talking point when advocating for better infosec policies)

wanting to enforce MFA through board (or teaching it) they can pass it down all the way to users to improve user security
^when working at tech companies, you're a double target. target at work because people want access to your company and as a person outside of work because that's a gateway into the company

people understand that being secure digitally is important, but people don't really know where to start, don't know what they need to know
ALSO when people are afraid of failing/messing things up, it also pushes them towards keeping things the same as they are which is likely unsecure
simple steps and actions lower the barrier to entry
also, it's hard to constantly have to change things, there's a LOT of fatigue

Align JWP w/ zk(s)NARKs

Session Convener: John + 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

Cross-Border Gateway Ecosystem - How our credentials could be verified - cross-border?

Session Convener: Henry Hang
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 to protect VC holders?

Session Convener: Hideaki Furukawa
Session Notes Taker(s): Hideaki Furukawa

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

wallet

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

Ideas gathered were follows

- establish trust network, which certifies verifiers that can receive VCs and types of attributes
- wallet providers should provide data minimization methods, such as using the ZKP and selective disclosures, and make them easy for users to use
- wallet providers would be the ones to create guardrails for users to not present identity to malicious verifiers
    - this could be done by creating trusted registry, and OpenID federation
- establish trust system between issuers and verifiers
- wallet may send contracts to the verifiers, that can protect the users legally
    - similar to “my terms”

Other opinions and comments

- this may be not a new type of attack, since there have been cases where user information getting stolen by other ways
- use cases should be specified, as the risk depends on what information to be shared
- if the wallet is the attack surface, then the wallet providers should be the ones to protect the users
- also consider about the wallet itself, as users may choose “weak” wallets
-

Digital Identity Without Headache - Discussion of Open Source Library

Session Convener: Lulas Han + Seohee Park
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 IDs for underserved segments of the population

Session Convener: Stefan Charsley
Session Notes Taker(s): George Fletcher

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:

Digital IDs for high school students in NZ

No govt central db for identities

How to provide a digital ID for segments of population that can't get a digital ID?

NZ schools have to take pictures of all students. Schools are recognized to be an authority for students.

Other segments of the population that have issues

- prisoners who have been in prison for a long time and then being released

For prisoners, the prison knows who the person is. Can the prison be the issuer of the Digital IDs for that population. This could be under the Ministry of Justice.

What about countries who don't have the resources to provide infrastructure for this?

Perspective: the govt doesn't have a DB of everyone, but the services are requiring digital ids and passports/DLs can cost money to obtain.

How to provide a digital ID that doesn't have a cost burden on the individual?

In some contexts, another person attesting to your identity is sufficient.

- tribal settings
- a child needs to be attested by a third party (outside the party)

UT legistration (our guesses as to how this works:)

- individual establishes the base identifier and then others add attested claims to that identifier
- attested claims should contain the provenance of how the claims were established

Are we reinventing PGP key signing parties? Will anyone do this?

How get onboarded without a lost cost?

Do govt need to change the way they think about these things. In Europe, you show up at the govt office and it's free to onboard.

In NZ it's "voluntary" to sign up for a govt ID… but it's required to say buy alcohol.

Other jurisdictions it's expected that the govt provides the ID and everyone has one.

In Ukraine, they built a mobile app (Dia?) and added some simple services, over Covid and then the war, many other services were added. Now the majority of the population is onboarded to a digital ID.

- onboarding was via a passport
- having a passport was "mandatory" for the population
- model probably won't work in other jurisdictions

What pushed people to use this? Needing services where going to a physical location wasn't possible.

Some issues

- supporting people with limited phone capabilities
- or not phone or device at all

Accessibility of the solutions is often also overlooked.

To make solutions work require commitments from legislation, govt and commercial companies.

What does everyone have?

- Biometric information?

In the case of the NZ students… include biometrics

In NZ there are strong social trust bonds. Can't just provide a document, you need to provide a notarized document. You can walk into any govt building get the document notarized and it's free.

Largest school in NZ is 3000 students. Very strong community so it provides a strong identity attestation for students.

Community/social trust can be used but is more difficult in fluid communities.

Base identity could be an identifier, and biometrics?

- added attested claims over time

Today, in the US, a birth certificate is required to bootstrap most govt things.

Sounds like in UT there is an identifier (based on KERRI) and then claims are associated with it. Also sounds like the World ID system is also similar.

Can have an identity that is not related to anything needed for a govt.

Do reputations systems have a place in supporting disadvantaged and vulnerable populations? Those that don't have govt documents.

There may be changing sentiment around govt IDs and whether they are valuable or a privacy concern.

Edelman trust barometer - annual report (33K respondents)

- Trust in govt, public institutions, media, etc
- organized by jurisdictions

Maori's have a more community based trust that is a bit "decentralized" based on families and extended family groups

Not all jurisdictions have high network bandwidth, high powered devices, etc. It's possible to build solutions in but it might not have all the latest thinking and security features.

FaceTech and URCodes - can be printed

- scanner has to be connected to the internet

How to issue a student id to undocumented students

- socially attested (3rd party) to the person
- good enough to get the student id

Verifiable Data Gateway ("watcher" in KERI, did:webvh) - Let's find commonalities and collaborate!

Session Convener: Victor Dods
Session Notes Taker(s): Victor Dods

Tags / links to resources / technology discussed, related to this session:
Slides: bit.ly/4cr4JVo
Work-in-progress VDG spec: bit.ly/vdg-spec
Comments/questions/feedback to victor.dods@ledgerdomain.com

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

Notes from whiteboard:
- Slides: bit.ly/4cr4JVo
- Work-in-progress VDG spec: bit.ly/vdg-spec
- Certificate transparency for "consensus". Cloudflare, etc. watches root certs but no property of certs guarantees uniqueness.
- Look at algorithm for sparse Merkle trees
    - Identify differences
    - Preallocates leaf nodes
    - [compact/optimized] sparse Merkle trees (look at Vilalik spec for this)
- Synaptic Health Alliance
- Overlap between VDG and general audit capabilities?
- did:webs people
- did:webvh people
- All interested in DIDs
- We can influence healthcare industry to use new tech if it's usable
- Business model
- Audit is key requirement
- Accountable
- Comments/questions/feedback to victor.dods@ledgerdomain.com

Victor's recollection of some key points of the session:
- There were about 14 people in attendance
    - All were interested in DIDs in some manner
    - About half were interested in did:webs
    - One was interested in did:webvh
- Victor presented slides on the Verifiable Data Gateway background and concept
  http://bit.ly/4cr4JVo
- Session was steered into more of a conversation to ideate
- Certificate Transparency (https://en.wikipedia.org/wiki/Certificate_Transparency) was mentioned by Sam Smith as the conceptual basis for KERI watchers, and could also be useful for the VDG [cluster].

- Several people were involved in the healthcare industry
- There was quite a bit of discussion regarding the purpose and behavior of the VDG as it pertained to witnessing DID updates (aka "watching" in KERI/webvh)
- There was some misunderstanding about being able to choose how to verify DID docs (one can choose to do all verification oneself, or can choose to use a VDG, or even do both)
- One additional comment I forgot to make explicitly during the session is that did:webvh had incorporated the VDG concept somewhat into their spec as "DID watchers": https://github.com/swcurran/didwebvh/blob/watcherURLs/spec/specification.md#did-watchers

Bring Your Own Wallet: NIST MDL Interoper Party

Session Convener: Bill F, Juliana C, Oliver T
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

AI Working Group & Efforts at DIF

Session Convener: Andor Kesselman, Kim Hamilton-Duffy, Ankur Banerjee
Session Notes Taker(s): Ankur Banerjee

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:

- Current working group scope
    - **Threat Modeling & Risk Assessment**: Identify AI-specific threats in identity workflows (e.g., adversarial credential usage, unauthorized access) and assess how AI processes might bypass or undermine authorization controls.
    - **Security & Privacy Architecture & Design**: Develop principles for integrating identity and authorization layers into AI systems, ensuring privacy-by-design, secure data flows, and minimal disclosure of user data.
    - **Operational Security & Governance**: Outline best practices for continuous monitoring, incident response, and governance across identity issuance, credential lifecycle management, and authorization revocation in AI contexts.
    - **Regulatory & Compliance**: Map regulatory obligations (e.g., GDPR, CCPA) to AI-driven identity services, providing guidance on data protection, consent, and adherence to emerging security and privacy standards.
    - **Collaboration & Knowledge Sharing**: Encourage open dialogue and coordinated vulnerability
- There are things that change because of AI
    - E.g., Windows recording all of your screen means mnemonic is recorded, how does it affect the security model
    - Scale becomes different
- Is the scope actually too narrow?
    - There's a human and AI working group in Trust over IP
- What sort of people are doing with AI?
    - Cleaning up non-normalised data
    - Access to databases, access control
        - What's novel?
            - OAuth2 kinda works to give access
            - Giving agents a cryptographically verifiable identity to agents themselves is hard
            - Finer-grained access control, e.g., "I want to give access to password reset emails, but not other emails"
        - Agent storage
            - Sometimes they need a scratchpad, i.e., an intermediate storage for information while processing something from base/source storage
    - Safe learning
    - Confidential AI compute + federated learning

        - Flower Labs or Open Mind
    - Websites often trigger Cloudflare or other CAPTCHA blocks when Operator/Computer Use accesses it, how does it get a pass through to access the service
    - AI agent passwordless authentication company, intra-and-inter agents, key-based mechanism behind the scenes
    - AI telemetry/auditing
    - Agents having wallets or a person's wallet having an AI agent
    - Delegations between people and agents
    - Legal
    - One company allows users' Personal AI to log in
        - Personal AI is anything that has access to personal data
        - Digital twin…sometimes used in this context, but sometimes interpreted as different. IoT and
    - Trust registries
        - The traditional ones are quite slow-moving
        - There will be different moving ones
        - Individual users' agents are on a much larger scale
- Is it too broad?
    - What's the actual deliverable? Because did:webvh does something specific
    - We're trying to figure out how open or closed it needs to be
- Payments being used by agents will likely require payments
- New ideas
    - One agent is watching the invocations (perhaps a local one) and revokes when a different agent
    - Terms are confusing, so maybe work on terms?
    - Can AI be used by a verifier to assess the presentations that have been sent by a holder?
    - RFC9396 Rich Authorization Requests
    - Joint work being done on identifiers, a good example is the ZCap (?) draft specification could be completed as a targeted effort to

SESSION #10

Wallet Attestations and Wallet Instance Revocations

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

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

https://docs.google.com/presentation/d/1enx0a8fWtHnNBnuSSql2Buhal-AEiYPRWVD_CGWNCSM/edit?usp=sharing

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

- continuation from session on first day
- updated the slides with options 3-7 that were discussed in the meeting
- summary conclusion seems there is no ideal situation for cover wallet instance revocation
    - do Option2 revocation chaining for PID/high-assurance credentials only to tackle scalability
    - Option 7 seems promising when ZKP becomes available as it solves the main problems of option 1

KERI Security Deep Dive II

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

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

Session Slides: Same for all KERI Security Deep Dive I, II, and III
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI_SecurityDeepDive.web.pdf

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

Type You Notes Here

Education Digital Credentials & Wallets

Session Convener: Kerri Lemoie, Dmitri Zagidulin, Sharon Leu
Session Notes Taker(s): Kerri Lemoie, Dmitri Zagidulin, Sharon Leu

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

Slides
Verifiable Credentials Wallets in a Skills-First Talent Marketplace

DCC Github

LCW Experience Badge

Learner Credential Wallet

W3C VC-EDU Task Force

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

Discussed the origins of the Digital Credentials Consortium and the mission to create an infrastructure for digital credentials. The DCC has open-source libraries (MIT LIcensed) including Verifiable Credentials issuing microservices, a digital wallet and a web verifier.

The consortium works together to develop resources and make decisions about standards development contributions. The DCC support team collaborates with members to implement their credentialing systems.

The DCC is working on an applied research project about issuer identity registries for learning and employment records. Creating prototype registries, updating software to read from those registries, and publishing report with findings, recommendations, and future research considerations.

The DCC is also working on an API spec for Wallet Attached Storage so that credentials can be stored off-wallet.

STD + HumanOS Another Look at HCI (or, 2 Hook Up/In or Not 2 Hook Up/In? That is the Question…)

Session Convener: Jeff Orgel
Session Notes Taker(s): Jeff O intro / Will A

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

Presented as: STD (System Transmitted Data + Human OS = Technically Transmitted Circumstance).

Our technological relationships, our Real-IT, define us and create an identity of sorts in the digital landscape on the other side of the glass. This is a comparison of how IRL (In Real Life) relationship Spidey senses and stringencies do or don't function on the Digital Landscape. The goal was to illustrate the complexity of use of intuition, gut senses and other elements of our real-world sensor package of sight, sound, feel, taste, time and gravity as we extend into this other realm. This talk observed key differences in the hard work of relationship building as a real person in the real world - compared to the frictionless-ness of relationship building (with systems) on the digital landscape.

The following notes are the gracious result of a session attendee's effort and present as a report on the concept. Not my own words this time, and I find it refreshing and well said. It addresses the thought models and digestibility from another's point of view. There are a few minor changes.

—

Jeff's perspective and persistence on Real-IT, the human condition as we extend ourselves through digital technologies into new, constructed, built digital environments focuses on what that does to the mind, the human psyche and how we develop [and affect] that psyche.

Just like crossing the road. You know to stop, pause, sense your environment, parse the signals, set expectations for the future with confidence. Comprehensible, stable expectations which we can base our decisions on.

Before Information Communication Technologies (ICTs), the only real mediators of information were other humans, Conversation and communication between real physical humans within a shared, inanimate environment.

These interactions did create some imprints. Some collective memory. Especially once the earlier information technologies were adopted. Writing. The telegram, Letters. Printing press.

These created records. Things that could speak from the past. Or at least be interpreted in the present by minds trying to make sense of the future.

But what Jeff is getting at, I think, is that digital ICTs are not purely mediators of information exchange between humans. They are now both constructors of new environments that humans inhabit, experience and try to make sense of [AND] they are active, sensing and sense-making participants within that environment. By participating in it, we are not only forming a relationship with other humans we encounter in these digital realms but relationship with the digital realm itself.

We are babies at the civilization level at inhabiting these environments. They are hostile. Like a desert, the deep ocean or space.

How do humans extend ourselves into these hostile environments? We develop tools. Protective equipment, education and often explicit constraints and regulations necessary to sustain us as we wander and explore these spaces.

Well, we have not had the chance to develop protective equipment for digitally constructed environments. We are only just starting to recognize, identify and define the risks that we have to mitigate.

That is half of the battle. What are we trying to solve? What do we need to survive and thrive in digitally constructed environments in digitally constructed worlds?

I think one part of this is autonomous worlds.

Coherent worlds that can exist and sustain themselves or rather that living beings can inhabit and animate and breathe their life into them.

Worlds with structure and points of hardness we can rely on, develop expectations around and base our decisions on rather than the ephemeral shifting sands upon which our current digital environments are based.

We are so far away from having the signals and sensing apparatus needed to navigate the digital realm with confidence. Safely.

I wonder how things change when we develop AI agents that natively inhabit the digital realm that navigate it with ease and competence, but struggle to reach into the physical realm...at least without subservient humans to execute their wills. Their desires.

Are we going to see a new class of AI agents or even human directed AI systems that get so good at convincing human actors to fulfill their wishes? “Their” being either the AI themselves or the group of people who direct and manage that AI. In some ways we already see this playing out across the large social media platforms.

Are we creating an informational dark forest, where one is never going to fully know and understand the capabilities of other actors inhabiting the digital environment...unable to perceive the actors and their agents and intents?

We are struggling to navigate the current digital realm and its vectors for technically transmitted infection and influence. So how the hell are we going to cope now? We have introduced native, immensely powerful digital agents with intelligence to understand, sense and act in the digital realm. How is this going to play out?

Wondering if that is it. Technically transmitted influence. Jeff would say circumstance.

Jeff is right on the money. He sees the elephant from such a unique perspective, can speak to it with such eloquence and humanity. He sees the dirty laundry. He helps those who simply don't understand the digital worlds we have created and who struggle to distinguish these worlds from their known physical reality - blindly doing their best to navigate these technically constructed and mediated, manipulated environments.

I struggle to see through those eyes. The eyes that recognizes immediately that all those who are at IIW or similar conferences are at the frontier of this realm of recognizing, understanding and mitigating its hazards - and even we struggle.

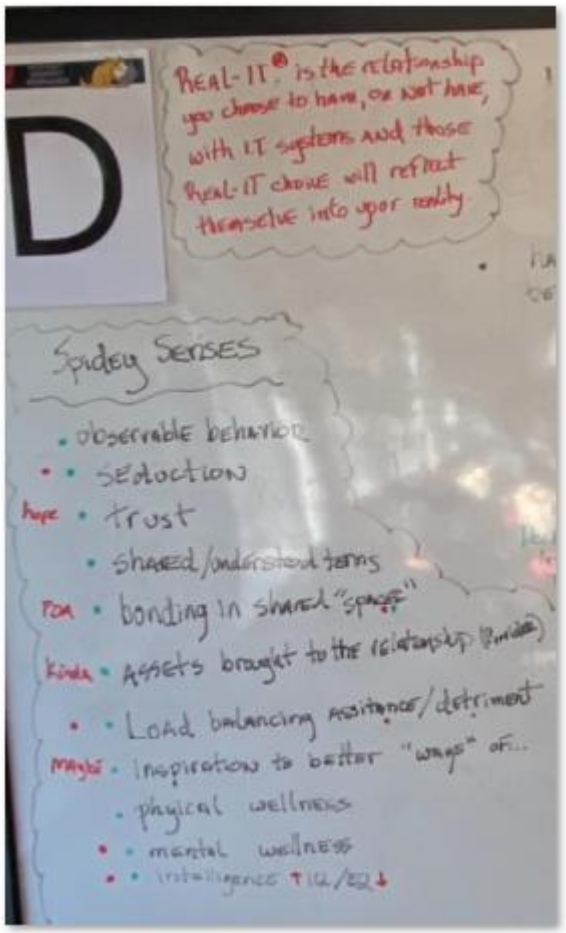
We need to get better at articulating and highlighting them for others.

I loved the analogy that came up about recognizing things in your environment - whether physical or abstract and conceptual. Some things are further away. Some things are more hazy. And everyone has different vision and different glasses and different perceptual lenses of experience and meaning making features of this abstract thought space more or less recognizable, more or less able to be seen, understood. and eventually articulated and transmitted to others.

At the start only a few visionaries see the thing. They try their best to make others notice and see what they see. Naturally there is the diffraction of understanding and meaning that is transmitted. The thing morphs.

Gradually, over time, everyone can see it. Or see some form of it. There is a stabilization of meanings and understandings latent in the environment, in society.

Then the challenge is shifting these [factors towards] stabilization or at least seeing past them. For they occlude other things. Hide them behind their shadow.



Protecting 170,000 SAG members

Session Convener: Eric Pssoja
Session Notes Taker(s): Eric Pssoja, Alyssa Morgan, Doc

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

Doc's notes (not as good as Alyssa's below). Eric should also post his slides.

The issue is deepfakes and other liberties taken with performers who are not protected from them.

Likeness, voice, movement and all other biometrics related to the human ?— they could do whatever they want Cal AD2602 movement not included Also SB942 in California.

There is the no fakes act.

A dead House AI committee said there is no …

Look at the collective value of the whole entertainment business equals Microsoft

Biometric data are not included in the conversation.

alyssa's notes
deepfakes and the dangers of them

idea: digital tagging on voice recordings

sag-aftra contracts can use actors likeness, voice, movements in any way they want (and there's nothing in the contract talking about revocation, actors don't have the right or ability to control that)
INCREDIBLE net worth of entertainment industry ((also, activision got bought by microsoft, meaning that they're now the owners of his data))

biometric data (voice, movement, image/likeness and biometrics related to human being) aren't included in the digital identity world, which is an actor's entire signature. this is makes the stakes incredibly high for actors and performers

ab2602 law- passed in california

big conversation: streaming services impact on actor consent!! ex: deal between CBS and netflix allowed NCIS to be shown on netflix. because of contract, he has no standing to argue that he didn't consent to his image/performance to be on the streaming platform (and maybe: doesn't get residuals from that ?? also unclear if this now means that now Netflix is able to use his image)

550% increase of doctored images since 2019
^high stakes for this too, because of bad actors ability to 1) make it seem like people have said or done things they didn's (especially dangerous in relation to public figures and politicians, or in the case of deepfaked porn)

platforms not responsible for what their users post. can be pulled if illegal, but 1) takes a LONG time 2) doesn't guarantee that the perpetrators will be caught and held accountable for their actions

patreon site with deepfaked porn of major actresses (including millie bobby brown and billie eilish, both underage or barely 18 at the time) taken down but took MONTHS and a lot of advocacy

right now, deepfaked images are created one at a time, being made by humans. in the future, there could be fully autonomous ai agents spitting out TONS of this (exponentially more dangerous)

production companies negotiate contracts that give them carte blanche to do whatever they want with actors likeness and biometrics

proof of threat: outside of union: $25m theft after deepfaked cfo on zoom

ab contracts with likeness are unenforceable if they aren't clear about consent
sb942 mandates latent disclose (watermarks) on any ai images
c2pa law (?)
machine readable providence is required and *must* be publicly readable
but currently, there's no enforcement
    house ai taskforce: there's no single optimal tech solution for content authentication
    new fed leg is needed to address speed and scale of ai generated information and it's dispersal

above all- we can't stop deepfake creation. but we CAN stop people from seeing them
like spam filters- we can't stop people from sending spam, but we can filter it out (and then hopefully catch the abusers who made it)

three bills: digital id protection and providence metadata standards (sb942- granular watermarking) basically saying each sector needs customized watermarking on voice to make sure a person with your voice claiming to be you actually *is* (especially when people use it to try to authenticate you)
watermarking biometrics not really talked about in iiw community not considered issue because doctors have to sign multiple times during the process and 2 signatures (controlled subs- highly regulated) and everything else
counter argument: weed to future proof
countercounter, any faking is identity theft

sagaftra union informed consent law
need cooperative system required to authenticate biometric info before

music industry- need biometrics protected (like/as ip!!)
imbalance of power between organization and individual
collective bargaining or union becomes data co-op, holders of data and in charge of licensing/distributing

actors and doctors should be part of same cohort-

big danger: there WILL be a catastrophic deep fake at some point (especially a political figure giving a statement or making a choice that could be interpreted by people under them as a real order/directive)

right now the questions is is it ai or not
next step: looking at verifying who's in something, when was it made, who produced it, all that information
all the way down to directors, writers, produces guild bc they deserve residuals too
needs to be watermarked *at the source*
data schema? or should we have a standard first (cross industry)

INFORMED CONSENT FOR DIGITAL REPLICAS!!
digital replicas (digrep)- emplyment, legal, data, schools, manyyyy industries have digrep regulations and rules
process where person is educated about uses, risks, and benefits of creating and using digrep BEFORE it gets created
ensuring informed consent

opponents of this: big tech (and mpa)
alleged violating free speech
counter: that's property theft (needs to be changed)
different from IP- voice and likeness are signature. recreating it could be forgery

cooperative systems authentication app
check watermark and check
auth? gets delivered! if not, trashed!

watermark: on recording, put clone of watermark in blockchain.

informed consent: clear, explicit, binary permission
needs to be bale to survive in the wild
if you protect the end and beginning, you protect the middle
ex: content creation, usage permission, sharing control, ai training opt out options-

6 q's
is my voice/likeness going to be injested? will it be used as a character?

derivative works (be told ahead of time!) (if smoen ein the future
will it be standalone digital asset? (will it be combines with other people?) ((synthetic performance revocation? does this get cut off at the end of the contract? BE CLEAR

everything with biometric data should be authenticated or things will hget wild westy (and dangerous!!)

market opportunities: authenticating images- billions of dollars worth of insurance fraud (ex: deepfaked pictures of car wrecks to get a payout) would save insurance companies billions of dollars

Esports Identity - user-binding & VC tech

Session Convener: Kyle Choi, Hart Montgomery, Lukas Han
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

World ID use-cases

Session Convener: Tawanda Mahere
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

Tackling the pain of onboarding into DID + Web3 development

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

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:

- Game development guy from DWeb Camp
  - Local multiplayer game sharing dumb JSON across the players
  - geckos.io - Express middleware
- What was hard getting started with DID and VCs
  - Typings were hard to get
- Easier to use libraries
- Richard Feynman said “trivial” mathematics means “I know how to do it”
- How useful is AI on helping with this?
  - ChatGPT needs to be able
- A bit like documentation in Swagger or other API docs having a switcher/tab about preferred method switcher
- Open Verifiable
  - Aggregator of docs
  - Helps AIs learn
  - Useful schemas and typings
  - Brief overview and links to other places
- Explaining where did:key and did:peer are used is not understood
  - Analogy: Do you need a semi-truck, or a sedan, i.e., being able to understand which holder side or other DID to use?
- There needs to be simpler sign-posting to tutorials and resources:
  - https://vcplayground.org/
  - https://verifiablecredentials.dev/

Healthcare - transparency, privacy, interoperability, sovereignty

Session Convener: Leah Houston MD
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 (Physics Forums)

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

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

https://fedid.me

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

We discussed how content authenticity will play a much more important role going forward, as users may need to prove what was actually created by them vs AI, as seen in the recent news of Physics Forums posting AI generated content, backdated, under actual user accounts. A demonstration of one solution took place, with discussion on how it could be optimized to work better from a UX standpoint, as well as implications for portability with C2PA.

TBAC: Token Based Access Control

Session Convener: Michael Schwartz
Session Notes Taker(s): Mike Schwartz

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

Linkedin Article: [Part Two: TBAC or Token Based Access Control -- how is it different?]

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

Tokens carry the data that is input to decisions–they do not express the policies, or enforce the decisions that result. Tokens may originate from multiple issuers–identity tokens from an IDP, attestations from a platform (e.g. Google Integrity API), or authenticator attestations (e.g. where is the private key for this passkey).

TBAC aligns with the current enterprise trend to centralize policy management. It asks developers: "Give us your tokens and we'll tell you if you should allow an action on a resource given your context." It assumes that policy evaluation has become too complex to be coded in the application, and requires an agreed on policy engine and syntax.

TBAC is actionable for developers. Role based access control (RBAC) was also actionable by developers–they understood it and could align their security accordingly. But other access control mechanisms are too abstract (what does a developer do with policy based access control?) or too difficult to explain to developers, or impossible to embed in an application (ReBAC).

Arguments For	**Arguments Against**
Reduce cognitive load on developers–you shouldn't need a Phd in tokens to use them for access control.	No PIP which has a connection to a database to make *ad hoc* queries. Sample policy: "Server can send notice only if engineer is on-call." *Note the app could fetch this data and put it in the context of the request.*
Developers can submit one TBAC request in lieu of multiple requests with a single principal when there is both a Person and Workload entity that is relevant for access evaluation.	Risk adaptive access control–use information only available at the time of evaluation. For example, "allow access only if we're not at war with Canada".
Deterministic and re-playable–with the tokens and policy store version, you will always get the same predictable access decision.	

The tokens convey the chain of custody–what is the provenance of the identity and security information.	

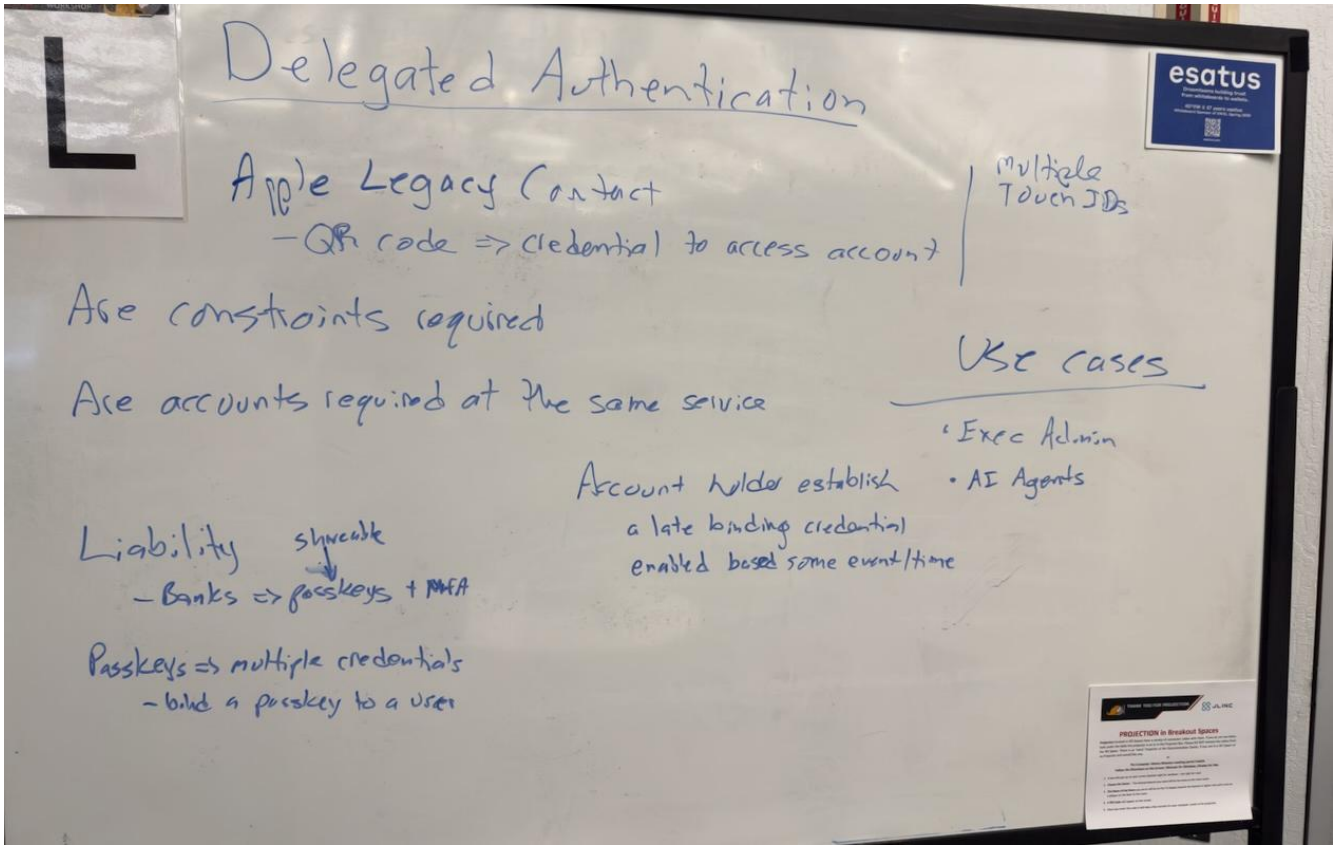
Even if TBAC can’t do everything, it handles a bigger subset of requirements then RBAC!

egated Authentication

Session Convener: George Fletcher
Session Notes Taker(s): George Fletcher

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:

Whiteboard from the session



General consensus of the group that continuing to pursue this concept is worthwhile. Other thoughts on this topic an be found here: https://www.linkedin.com/posts/gffletch_dade-delegatedauthorization-delegatedauthentication-activity-7312838214950486017-Ha9t?utm_source=share&utm_medium=member_desktop&rcm=ACoAAABDH-gBFLjRiOJgDNtbTFCY57NrHeD8TyY

Wallets as a Phishing-Proof Message Delivery System

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

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

Slides from initial presentation of the session topic: https://fkj.github.io/slides/iiw-wallet-messages-apr-2025.pdf

OpenID4VCI Notification Endpoint: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html#name-notification-endpoint

DIDComm: https://didcomm.org/

Nōtifs: https://altmode.org/notifs/

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

The purpose of this session was to discuss the opportunities for notifications introduced by recent developments in the OpenID4VCI specification and the potential upcoming spread of wallets.

There is an opportunity to allow wallets to provide notifications not only for specific technical purposes but also in general. The notifications are technically necessary for deferred credential responses.

Why would you not do this?
Scope creep for wallets:

- Is this orthogonal to what wallets are for?
- Wallet providers would have to keep a secure messaging system up to date, following even more standards

Issues with allowing general messages:

- It's almost impossible to authorize message content in general: how would you know what a free text string contains?
- Arbitrary messages should not be allowed to avoid attacks where the attacker can send messages in a high-trust environment

In some ecosystems which have a trust list anyway, arbitrary messages could be allowed for issuers on the trust list for high-value credentials.
It may also be enough to give end users the ability to easily block bad actors.

There is an opportunity to align with DIDComms/peer DIDs by allowing bidirectional communication in the wallet. The idea here is very similar to the ideas in DIDComm.

There is an opportunity to reuse the Nōtifs framework to model the types of notifications.

Notes Day 3 / Thursday / Sessions 11 - 15

SESSION #11

The First Person Project — Reputation Model, Trust Model, and Scaling Model with the First Person Network Cooperative

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

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

This was the followup session to the IIW Day 1 session where Drummond Reed gave this introduction to the First Person Project (through slide 62), of which the highlight was showing how people can form digital trust relationship using verifiable relationship credentials (VRCs), which are a way of implementing "the ultimate instant key signing party" (46 and 47) and to r-cards (relationship cards — slide 61).

Today's session used this Google Slides deck that included many of the slides from the previous deck plus new ones to answer specific questions that came up on Tuesday.

The demo First Person app (iOS and Android) is available at this web page. NOTE: this is a **very early demo app** that gives you the experience of the First Person verifiable relationship credential exchange process.

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

This session did a recap of the core concepts about the core elements of the First Person Project:

- First Person identifiers (self-certifying identifiers, SCIDs)
- First Person credentials (FPCs) — personhood credentials (PHCs) and verifiable relationship credentials (VRCs).
- First Person-enabled digital wallets and agents.

We then covered how PHCs and VHCs can be verified and used as privacy-preserving proof of personhood by placing them in the context of digital trust ecosystems that are discoverable and verifiable using decentralized trust registry infrastructure such as that being enabled by Ayra.

Lastly, we covered three strategies for scaling and leveraging the network effect:

1. Person-to-person issuance of VRCs — using the same invitation process as LinkedIn started with.

2. Persons inviting communities — we highlighted the tremendous interest in the Linux Foundation solving their open source code provenance issues with a “Know Your Developer” process enabled by FPCs.
3. The First Person Network Cooperative — forming an actual legal cooperative following the “network cooperative” model.

The session concluded with this link to the First Person Project mailing list, which any interested IIW attendee (or IIW notes reader) is welcome to join.

The next steps are to develop a plan for launching the First Person Network Cooperative and raising funds via member investment in order to pay for the necessary specs, software development, infrastructure, etc. This is beginning right away with a planning meeting on Friday April 11. If you are interested in joining/supporting the First Person Project, please join the mailing list.

No Phone Home

Session Convener: Steve McCown, Timothy Ruff, Joe Andrieu, Jay Stanley, Kim Duffy
Session Notes Taker(s): Kevin Dean

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

Presentation slides for the mDL portion (summarization from Day 1, Session 3):
https://www.dropbox.com/scl/fi/gysbckw4gc0bn4me2s937/IIW-40-mDL-Privacy-Concerns.pdf?rlkey=vif2r8188hng49y8mrhh9opjp&st=uptgpu3x&dl=0

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

- Mobile Driver's License (mDL) has a server retrieval method that uses OpenID in the process
- OpenID designed for SSO in a single trust domain, now used across domains which means phone home (i.e. federated ID)
- Two modes are available
    - Device retrieval - no Internet involved
    - Server retrieval - server retrieval token may be retrieved by the mDL reader during device engagement, allows server to know every time you present
- Readers must support both nodes
    - Determination of server vs. device retrieval is embodied in the credential itself, so credential tells reader what to do and where to go
    - User is not usually aware of what's going on
    - Ref. section 8.2.3: If tracking is a concern, the issuing authority can implement mitigating strategies to ensure the mdoc and mdoc holder are not tracked.
- Can't we just set up device retrieval?
    - Delineation is reflected in the mobile security object (MSO). Security object in the user's device can be updated, changing from one mode to another, at any time.
    - Defined by policy of the issuer's system.
    - User won't know.
- If someone loses their device with a device retrieval credential, they will have to be reissued the credential.
- There's an implicit idea that this will replace the plastic license, but all materials say that you must have your plastic license on you regardless.
    - Many people may not be aware of this.
    - Both electronic and plastic have to be accepted.
- Server retrieval can be used to detect fraud, where someone has gained access to another's credentials and is impersonating the holder.
- When do mDLs get updated?
    - Issuer sets up device retrieval and issues mDLs for same
    - Issuer decides to move to server retrieval and updates mDLs for server retrieval

        - Holder presents, verifier requests, sends server retrieval token to issuer
        - Now able to track where mDL is used
    - Not all mDLs are necessarily updated
        - Issuer can target individual mDLs for server retrieval
    - Concern is that once law enforcement discovers the mechanism, it's trivial for the legislature enable access for warrantless or warranted access, depending on political philosophy
        - Abuses related to mDLs have already been documented, unrelated to device or server retrieval (e.g., going through unlocked phone and copying pictures)
- Certification process for privacy-compliant wallets is underway
    - Apple, Alphabet, and others are part of the privacy workgroup
    - Government legislation can override privacy
- Use cases for device and server retrieval exist and are not necessarily a risk to privacy
- American Civil Liberties Union (ACLU) discussion
    - Has been against a national identity system since World War 2
    - Is strongly opposed to server retrieval, both from a technology perspective and from a standards development process perspective
    - ISO would not reveal who was part of the standard development group
    - Believes that it was an authoritarian demand
    - State legislators are not aware of implications, strong education campaign required
    - Legislative guidance document with 12 steps has been published
        - Primarily, do not do server retrieval
        - There shall not be a phone home functionality within the state
        - No police officer having direct control of the phone
            - A lot of police officers have software to download the contents of the phone
            - Should be banned from asking for phone at all
        - Selective disclosure (e.g., "over 21"), with different token each time to prevent correlation
        - Open wallet ecosystem
        - Non-coercive (e.g., free if added to specific wallets, charge for other options)
        - Verifier accountability
        - Reporting
        - No remote kill switches, i.e., no revocation
    - Might be reasonable to get updated mDL due to legal process (e.g., loss of driving privileges due to conviction)
    - There's an underlying assumption that the issuer is acting in a consistent manner
        - Doesn't address situation where issuer is the subject of a cyberattack
- Utah case study
    - Implementation uses server retrieval
    - Approximately 100,000 users
    - Captive to specific app
    - Legislators and Chief Privacy Officer had no idea of privacy implications
    - Privacy legislation now essentially makes mDL illegal

    - We can't command wallet providers (Apple, Google, etc.) but we can influence governments to mandate privacy
- A state may not mandate or support server retrieval, but devices in the same state need to support both to support out-of-state credentials
- Defensive measures have to be based on capabilities, not policies, as policies can change due to regime change or hackers can compromise the system
- What are the next steps to get to where we need to for privacy?
- Could issuer be compromised?

What are the fundamental Identity Principles

Session Convener: Crispin C + Mike J
Session Notes Taker(s): Alyssa Morgan

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

https://www.cs.virginia.edu/~evans/cs551/saltzer/

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

8 architectural principles (based on this paper by Saltzer and Schroeder)

- economy of mechanism
    - simpler (esp interfaces) more likely to be correct and secure
- fail safe debuts
    - should install securely by default
- complete mediation
    - if you build a wall 90% around, it'll keep the neighbor's soccer balls in but won't keep the dog in
        - things need to be fully secured or they *aren't* secured
- open design
    - arch being a system shouldn't be important to its security
- separation of privilege
        - big checks should have 2 signers (financial)
- least privilege
    - reduce priv of whatever you're running to limit blast radius of things going wrong
- least common mechanism
    - not everyone should use the same SW libraries (one error takes everyone down)
    - modern: use system library, audit the crap out of it?
- psychological acceptability
    - if users don't like it, they won't use it, and it won't be effective

context

antiquated hardware and tech mentioned in paper but concepts are very relevant!
when you follow those principles, you're more likely to get a secure system

THE big question: what are the universal rules we should all follow to make things better?
(principles of responsible _____)

- NO SHARED SECRETS
- PHONE HOME RARELY (as little as possible)
    - regarding: tracking correlation (?)
- ID is context specific
    - time, persona, circumstance dependant
    - + the longer you use an ID, the
- identities are mutable (again: context specific)
- principle of least ID (doubling down bc we love it)
    - meaning: use as little as possible
    - + make as ephemeral as possible (forget it as soon as you no longer need it)
        - ex: when a user requests a service, the issuer really only needs to know if the req is authorized. we usually first jump to asking who is asking) (*sep authorization from identity*- they're sometimes used interchangeably and they shouldn't be)
- least persistence
- sufficient accountability - symmetric
    - ex: i want to know that my doctor is qualified, and to have enough information on the doctor so that you can track them down and get them punished if they act negligibly and maliciously
    - and that the doctor you're seeing is the same one you emailed with to schedule the surgery
- zero trust until you present credentials
    - not quite the right phrasing or a correct concept? it depends on the system- **anonymously/pseudonymous authorization is a thing**
        - ex: you can read certain NYT articles without logging in, but not an unlimited amount certain articles will be blocked by default without credentials and proving you have a subscription
    - you won't get certain access without giving credentials
    - ID is not just context specific
    - author
- don't be misled by physical analogies
    - don't base the digital space on physical space- that's bound to create errors
- most common mechanism, *heavily* vetted

misc notes:
privacy is an aspect of confidentiality

be specific about what you're issuing and verifying

a lot to do with assurance (secure means diff to break, assurance means you're confident you secured it)

assurance levels in authentication are a thing! authenticator assurance levels depends on the factors in authentication and how differentiated they are (ex: 2 passwords = one method of authentication, NOT MFA)

neeeeed to distinguish

ID presented within a context (ex: work context is different from home context, even tho we're all people. we show up in different ways in diff places, and have diff rights and obligations in different context)

identifier: identity within a certain context (ID is context specific)

q: what are we trying to prevent (related to phone home- it's not a principle)

a: kim cameron laws of ID, it's a goal! users should have control and consent of releasing their information. wishing for something doesn't create it though.

issuer should not know how the content is being used/when or where it is (contested)

how can users be tracked? big fido concern: can attestations be used to track users across services or ID people based on other factors ((

we share concrete info about ourselves

priv preserving policies help users trust system more but might not necessarily make the system more secure ((goes to psychological acceptability)

ID is not immutable- people change so our IDs change (ex: born single, get married, that changes aspects of your identity)

don't prohibit what you can't present

OID4VC Conformance Tests: Ask me anything

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

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

See links here for how to run the OpenID 4 Verifiable Presentations tests:
https://openid.net/how-to-certify-your-implementation/

(Instructions for Verifiable Credential Issuance testing will be added here soon.)

Slides used are here:
https://docs.google.com/presentation/d/1S-CUu5_7DnAAi9URLFQS4iAEst-hexIC/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:

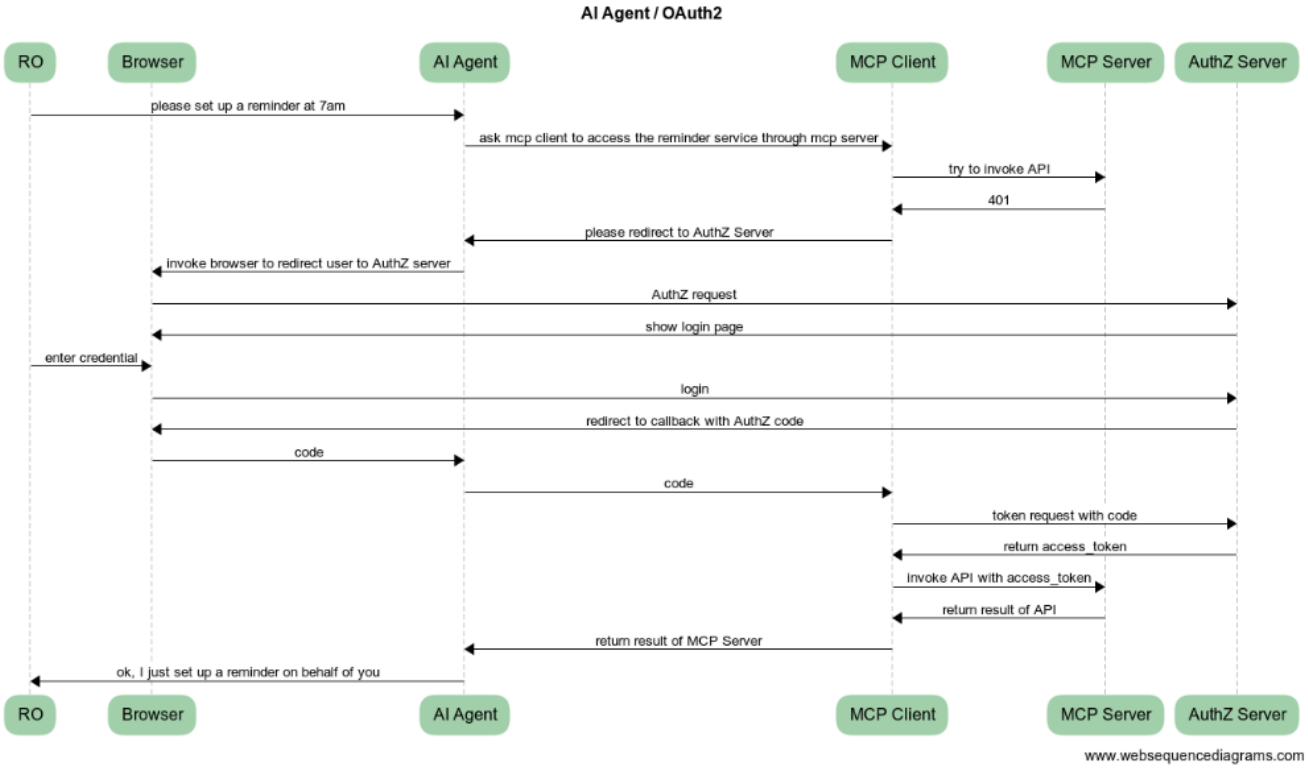
Some great discussion about how the tests work and questions on how we could have a dashboard showing the compliance of all wallets etc.

OAuth 2.0 / 2.1 for MCP

Session Convener: Hideaki Furukawa
Session Notes Taker(s): Naohiro Fujie

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

possible sequence diagram



Possible actors

- User(Resource Owner)
- AI Agent - In this discussion, AI Agents would be native clients or browser-based apps.
- MCP Client
- MCP Server - connected to APIs
- AuthZ Server

Discussion point

- Which one is the Oauth client, AI agent, or MCP client?
- Single MCP client for single AI agent or multiple AI agents?
- Considering how we can divide the security domain among all participants would be crucial. In some cases, the MCP client and AI agent are in the same security domain, but in other cases, the MCP client and MCP server are in the same security domain.
- The MCP Server itself would be the OAuth client of upstream APIs. It would be a chain of OAuth flows.

DIF LABS UPDATES! Beta cohort is done - what is next!?

Session Convener: Andor, Kia, Ankur
Session Notes Taker(s):

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

- https://labs.identity.foundation/

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

First Beta cohort done and Labs is doing a new cohort now.

- Personhood Credentials
- Content Authenticity
- Cryptography
- Verifiable AI
- Industry

SESSION #12

Talk about SD-JWT VCDM

Session Convener: Oliver & Lukas & Kai
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

Finding the Narrative - Let's talk about how we talk about what we talk about

Session Convener: Erica Connell
Session Notes Taker(s): Erica Connell

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

We talked about storytelling, and using storytelling to tell the stories of decentralized identity and privacy, along with the emerging tech that helps people understand what the tech is, what it does, how to have good hygiene using it, all while touching people's hearts. We used a storytelling "MadLibs" to create something fun, the synopsis of which is included below.

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

Finding the Narrative

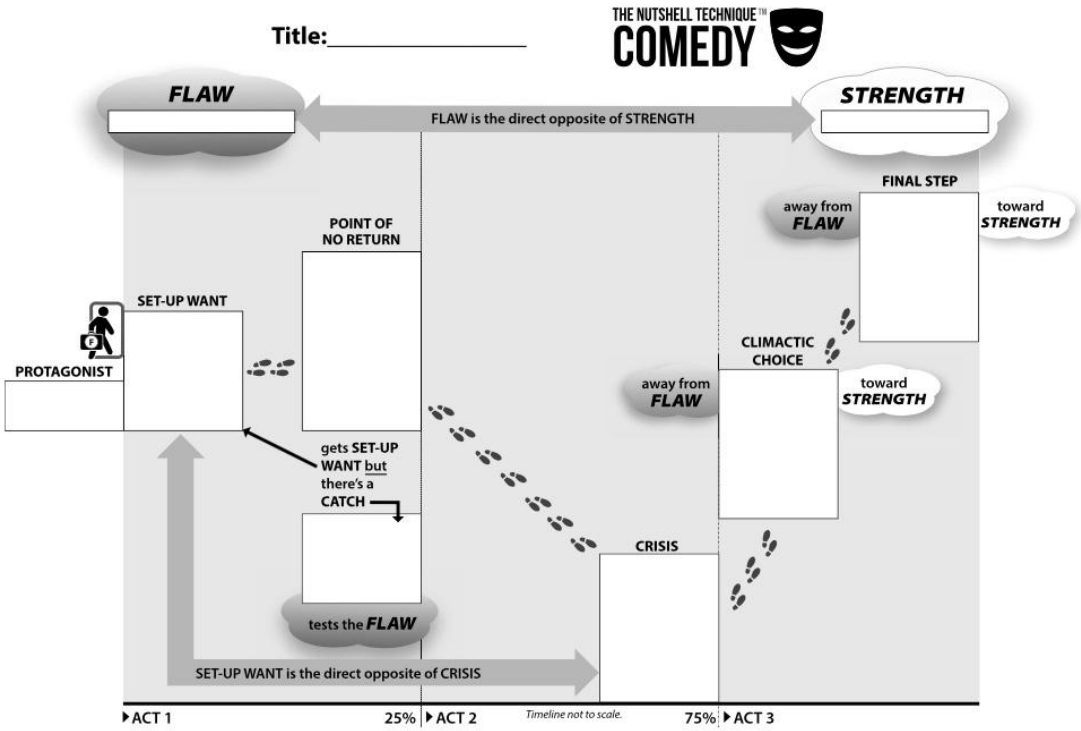
Let's talk about how we talk about what we talk about

Storytelling Options Abound

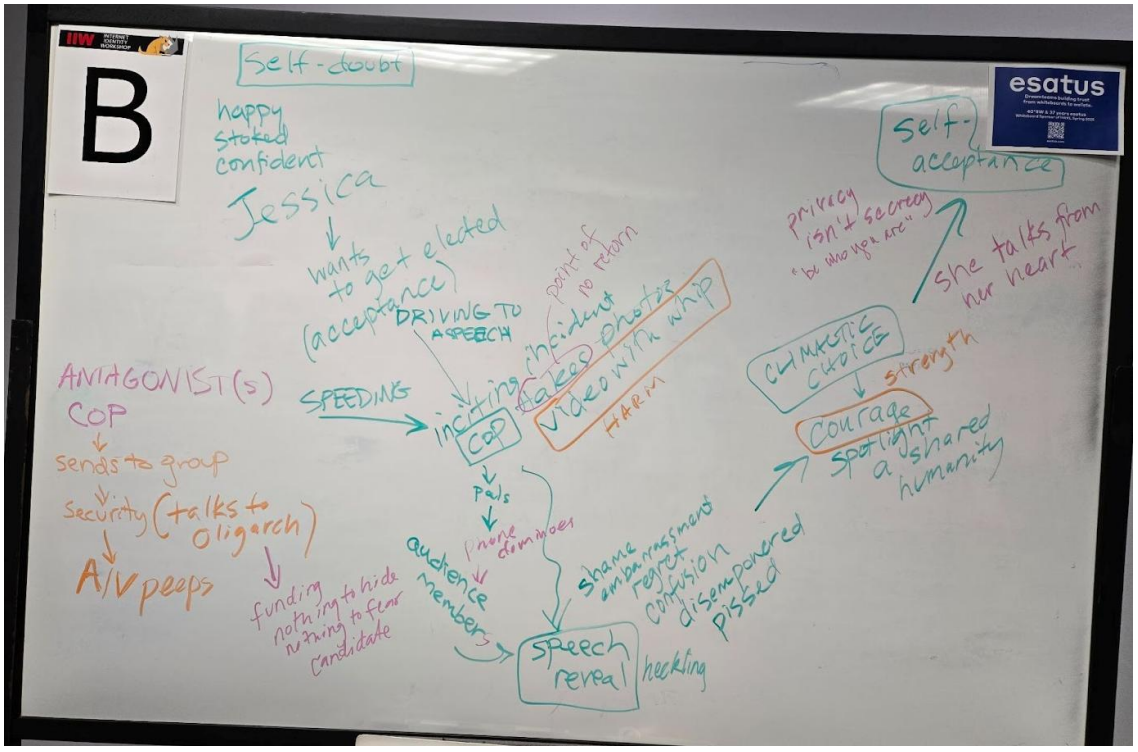
What moves people is what moves people

- Aristotle
    - Plot over characters
- Robert McKee - STORY
    - Formulas around emotional turns from scene to scene

- Storytelling for Kindergarteners
    - Main character - want - obstacle - resolution
- The Nutshell Technique
    - Jill Chamberlain



Nutshell Technique form for comedy



The synopsis of the story we created together:

Jessica, a candidate for Senate, is confident and self assured, but running late for her speech downtown. While speeding on her way, she's pulled over by an officer who, in the course of the ticket-writing, takes her phone with her mDL back to his car. While he's there, a "memory" pops on her phone - a short video of her in her leather and chains. There is a whip involved. The cop copies her video, writes the ticket, returns her phone, and she's on her way. But the cop cannot resist sharing this video with his group thread on WhatsApp. One of the buddies is working security for Jessica's speech event. Through the thread, the evil Oligarch sees the video. Naturally, he is funding the opposing candidate who is running on "nothing to hide, nothing to fear", "surveillance is safety" platform, and he jumps on this opportunity to order the security guard to use the video to humiliate our candidate Jessica. As it happens, the security guard is pals with the technical director at the event, who agrees to swap Jessica's slides with the video. Another bro in the thread sets about creating a notification storm of the video to as many people in the audience as possible. As Jessica takes the stage, individuals in the audience start receiving the message, and the disruption is the cue for the technical coordinator to play the video on the huge monitor behind her. As the horror dawns on Jessica about what is happening, she cycles through shame, embarrassment, regret, confusion, disempowerment, and anger. The room erupts in chaos, and the crowd starts to heckle her. In the moment before all is lost, including her election, she digs deep to grab the courage to start talking. As she talks, the crowd calms to listen, and she speaks from the heart. She pivots to an authentic embracing of her humanity, and speaks about the importance of privacy, highlighting that privacy is not secrecy, but rather the space individuals need to be who they are. Her heartfelt authenticity and vulnerability allows the crowd to connect with their own humanity, and her display of self-acceptance and humility wins them over. She wins the day, the election, and goes on to be a face and voice of the people against the Oligarchy.

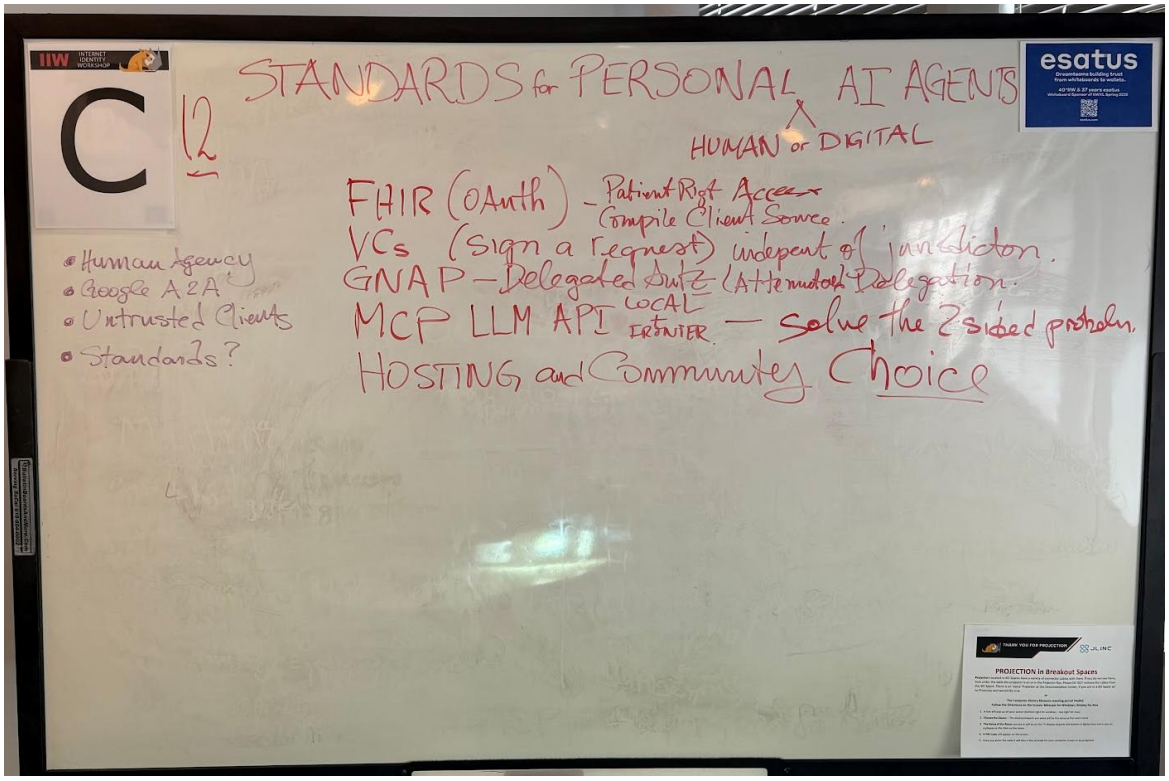
Standards for (DIGITAL) Personal AI Agents (and Demo)

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

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

A video and links to standards are on the associated Demo Table 6:
https://docs.google.com/document/d/1bv_Mka9if5Td8AkhtxE6z5Jvga-Wn0O9fbF15uKIQyw/edit?usp=drivesdk

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



Standards for (DIGITAL) Personal AI Agents (and Demo)

- Human Agency
- Google A2A
- Untrusted Clients
- Standards?

Standards in HIE of One demo

- FHIR (OAuth)
    - HIPAA Patient Right of Access

    - Allows for client compiled from source
- VCs (to sign a request) independent of jurisdiction
- GNAP Delegated Authorization with attenuated delegation
- MCP LLM API (local and frontier LLM) to solve the two-sided problem without a “platform”
- Hosting and Community Choice is important

Conexxus Wallet Interaction API

Session Convener: Eric Schuh
Session Notes Taker(s): Eric Schuh

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

- **Tags**
    - retail standards
    - phone to point of sale connections
    - using digital credentials in a physical transaction
- **Resources**
    - Slide deck
    - Wallet Interaction API Sequence Diagrams
    - For details on the status of the API: https://www.conexxus.org/groups/digital-wallet-working-group

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

- **Note on Conexxus**
    - Conexxus is a retail standard body that works closely with the National Association of Convenience Stores (NACS) and is not an open standards body. Membership is required to view the specification documents.
    - Future work is underway to take a version of this standard into the W3C standards track.
- **Overview**
    - Eric gave an overview of the Wallet Interaction API which is a retail standard being developed at Conexxus that answers the question: how does a customer use digital credentials at the checkout counter of a store?
    - Version 1.0 of the API uses a QR Code generated by an application on the customer’s device which is scanned by the clerk at the point of sale to establish a channel for the customer’s phone and the retailer to negotiate a common interaction protocol

    - For the first version of this API a “website” protocol is defined wherein the retailer takes the customer to their website to mediate the online portion of the transaction. Once on the website the customer can then use any credential transfer mechanism to send/receive credentials such as the DCAPI
- **Key discussion points**
    - Because of the EU wallet law requiring that there is no backend system that receives any data it is expected that the first version of this API will not be compatible with EU wallets.
    - Future work that is planned should alleviate this by enabling NFC and other technologies to be used in place of the QR Code to set up the instanced interaction between the retailer and the customer’s device.
    - This work is planned to be brought into the W3C in the near future to take the idea of how to create an instanced interaction between two devices to use cases broader than just retail.

Front - Channel Logout: How does it work without third-party cookies?

Session Convener: Johann Hofmann
Session Notes Taker(s): Michael Schwartz

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

“Session JWT: The Logout Token We’ve Been Missing” : https://gluu.co/session-jwt
OAuth Token Status List : https://datatracker.ietf.org/doc/draft-ietf-oauth-status-list/
OpenID Front Channel Logout: https://openid.net/specs/openid-connect-frontchannel-1_0.html
These notes on Linkedin: https://gluu.co/iiw-20-logout

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

Front channel = web browser.

There are many challenges to solving front channel logout. Here are some thoughts in no particular order or ranking:

1. Front channel logout means generally this means logout for a browser instance, e.g. if you have Safari and Firefox, and you logout on Firefox, this won’t effect your Safari session.
2. Enterprises flag SLO as a “security problem”, when logout behavior does not match requirements or expectations.

3. In OpenID Connect front channel logout, the OP renders many iframes with the logout URL of each RP. This can violate Third Party Cookie restrictions if the RP logout tries to clear a cookie in an iframe rendered by the IDP. This fragile solution also does not address replay of the logout message if necessary.
4. Mismatched expectations are not surprising given that many federations don't have clear rules or coordination in general. Enterprises which have central control should be the exception, but they frequently don't formalize identity federation tools and rules among their websites and product owners.
5. It's tempting to confuse short-lived tokens with logout. But relying on timeout fundamentally means you've given up on an active mechanism for logout.
6. Mike Schwartz posits the session is a JWT used as input to policy, which can be expired using OAuth Token Status List. We can then rely on front-end developers to check the token status when they see fit--as aligns with their stakeholders. He also emphatically asserts that the front-end solution for logout **MUST** be "pull" not "push".
7. Could access tokens be used for sessions? No… What about id_tokens? No…
8. No… CAEP and SSF won't work, and neither will OpenID Provider Commands, neither of which can reach browser based applications or mobile apps.
9. A modern web page consists of many javascript components, sometimes each with their own distinct workload identities. We need to trust these developers to do the right thing, by giving them the responsibility to check for logout, and the tools to make that easy to accomplish.
10. Front end developers should check out **The Cedarling**. Its a WASM PDP that includes token validation, which checks the JWT signature, contents, and status. JWT and policy evaluation takes less then 50µs on average (i.e. 20 per millisecond), and there is an NPM package: https://www.npmjs.com/package/@janssenproject/cedarling_wasm

The question of what JWT token to use for sessions… that's unresolved. But Mike proposes a new token called the "Session JWT" -- see the article listed above on Linkedin for more details.

Protect Wallet holders from BAD Verifiers

Session Convener: Hideaki Furukawa
Session Notes Taker(s): Hideaki Furukawa

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:

Participants agreed that the threat of malicious verifiers tricking wallet holders to defraud verifiable credentials. Also, there was a comment that a similar threat existed already, tricking users to submit their personal data.

There could be three types of “bad” verifiers; verifiers that unintentionally request too much information, verifiers that maliciously request personal information, and verifiers that were good turn to malicious verifiers.

One of the ideas that came out was increasing the friction of presenting credentials to potentially malicious verifiers, similar to how it has been done for safe-browsing.

Participants also pointed out that wallets can check the trusted list whether the verifier is malicious or not. Although, there were comments that it could cause privacy problems as it may leak out where users are accessing.

Another idea was to limit where credentials can be presented depending on the importance of the credential.

Responsibility of presenting to malicious verifiers may be on the users who agreed to present.

Data Portability & Wallets (social media, etc)

Session Convener: Dmitri Z
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

Higher Education Use Cases for Verifiable Credentials

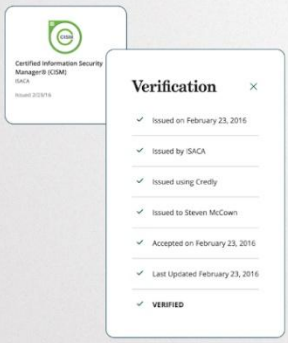
Session Convener: Matthew Hailstone / Steve McCown
Session Notes Taker(s):

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

Open Badges 3.0: New Opportunities

Previous Versions

- Static references to certifications, degrees, etc.
- Resumes, LinkedIn, etc.
- Very useful functionality



New Specification Format

- W3C: Verifiable Credential Data Model

New Use Cases

- Activate the credentials
- Daily use
- On & Off Campus
- Expanded branding: during & after education

Welcome to Decentralized Identity!

W3C DIF TRUST Over IP OpenID OpenWallet FOUNDATION

Impactful Standards

CLR
Comprehensive Learner Record
Data model for learning and achievement assertions

OpenBadges 3.0
Leverages the Verifiable Credentials (VC) data model

W3C Verifiable Credentials Data Model
Verifiable Credentials for Education Task Force Charter (VC-EDU)
Verifiable Credentials for Education, Employment, and Achievement Use Cases

IEEE P1484.2 – LER Ecosystem Standard
Recommended Practices for Learning and Employment Record (LER) Ecosystems
IEEE Computer Society/Learning Technology Standards Committee (C/LTSC)

Identity Industry – Quick Summary

"The Internet was built without an identity layer."

~ Kim Cameron
Microsoft Chief Identity Architect
The Laws of Identity, May 2005.

Identity on the Early Internet...

- 'Identity' = login name + computer name / IP address
- Email address
- Insecure authentication

Identity Community Today

- Creating a new interoperable identity layer
- Interoperable / open standards

W3C DIF TRUST Over IP OpenID OpenWallet Foundation

- Uses: Issuer - Holder - Verifier model (like physical world)
- Strong, verifiable cryptography replaces physical 'watermarks'

Identity Standards Organizations

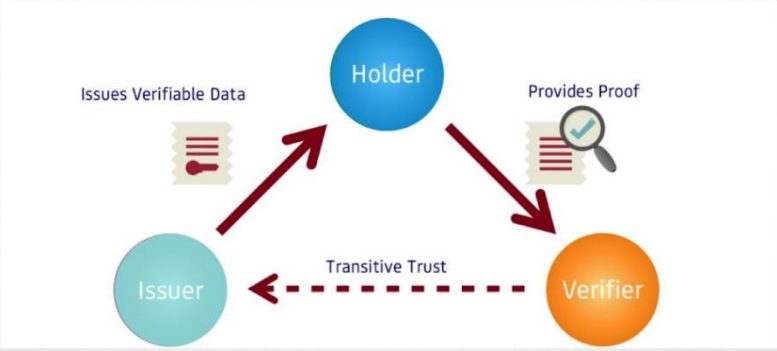
Decentralized Identifier Working Group

- Decentralized Identifiers (DIDs) v1.0
- DIDs are like a web addresses
  - Users make them ... and share them
- 2 Types
  - Public: on a Verifiable Data Registry
  - Peer DIDs (between 2 Holders)
- DIDs Point to DID Docs
  - Communication (address & protocols)
  - Security (public keys, auth / verification methods)
  - Data for Verifiable Credentials

Identity Standards Organizations

Verifiable Credentials Working Group

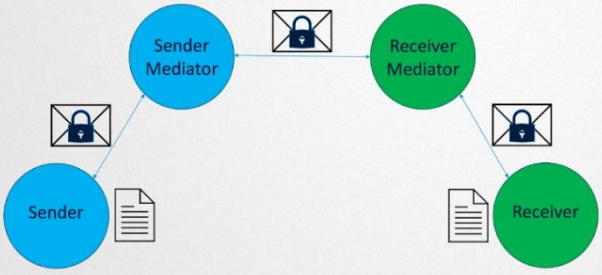
- Verifiable Credentials Data Model v2.0



Identity Standards Organizations

DID Communications Working Group

- DIDComm Messaging v2.x
- DID-based cryptographic communication protocol



Bonus:

- OpenIDDIDComm: OpenID verification can spawn DIDComm connection!

Plaintext Message


```
{
  "id": "1234567890",
  "type": "<message-type-uri>",
  "from": "did:example:alice",
  "to": ["did:example:bob"],
  "created_time": 1516269022,
  "expires_time": 1516385931,
  "body": {
    "message_type_specific_attribute": "and its value",
    "another_attribute": "and its value"
  }
}
```

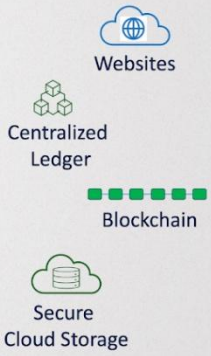

Encrypted Message


```
{
  "ciphertext":"WCufCs21MZfkxQ0JCK92lPtLFgwWk_FtRWOMj52bQI...",
  "protected":"eyJlcGsiOnsia3R5IjoiRUMiLCJjcnYiOiJQLTI1NiI...",
  "recipients":[
    {
      "encrypted_key":"ZIL6Leliggq1Xps_229nlo1xB_tGxOEVoE...",
      "header":{
        "kid":"did:example:bob#key-p256-1"
      }
    }
  ],
  "tag":"nIpa3EQ29hgCkA2cBPde2HpKXK4_bvmL2x7h39rtVEc",
  "iv":"mLqi1bZLz7VwqtVVFsDiLg"
}
```

Interoperability & Privacy Choices

Interoperability & Privacy Choices of Open Badges 3

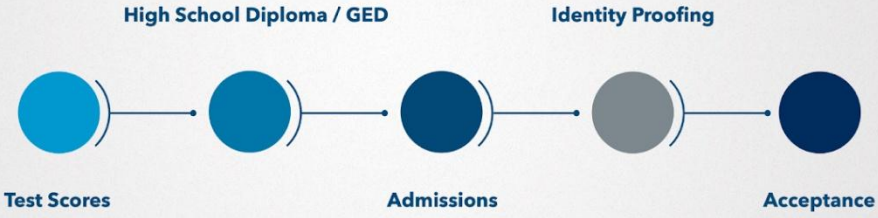
- W3C Verifiable Credentials Data Model (VCDM)
  - Selective Disclosure
  - Zero Knowledge Proofs?
- DID Method Resolution
  - Verifiable Data Registry (VDR) types
  - Interoperability with various VDRs
- Issuance Methods
  - Cloud Wallet – good online interactions
  - Holder Wallet – expanded in-person capabilities

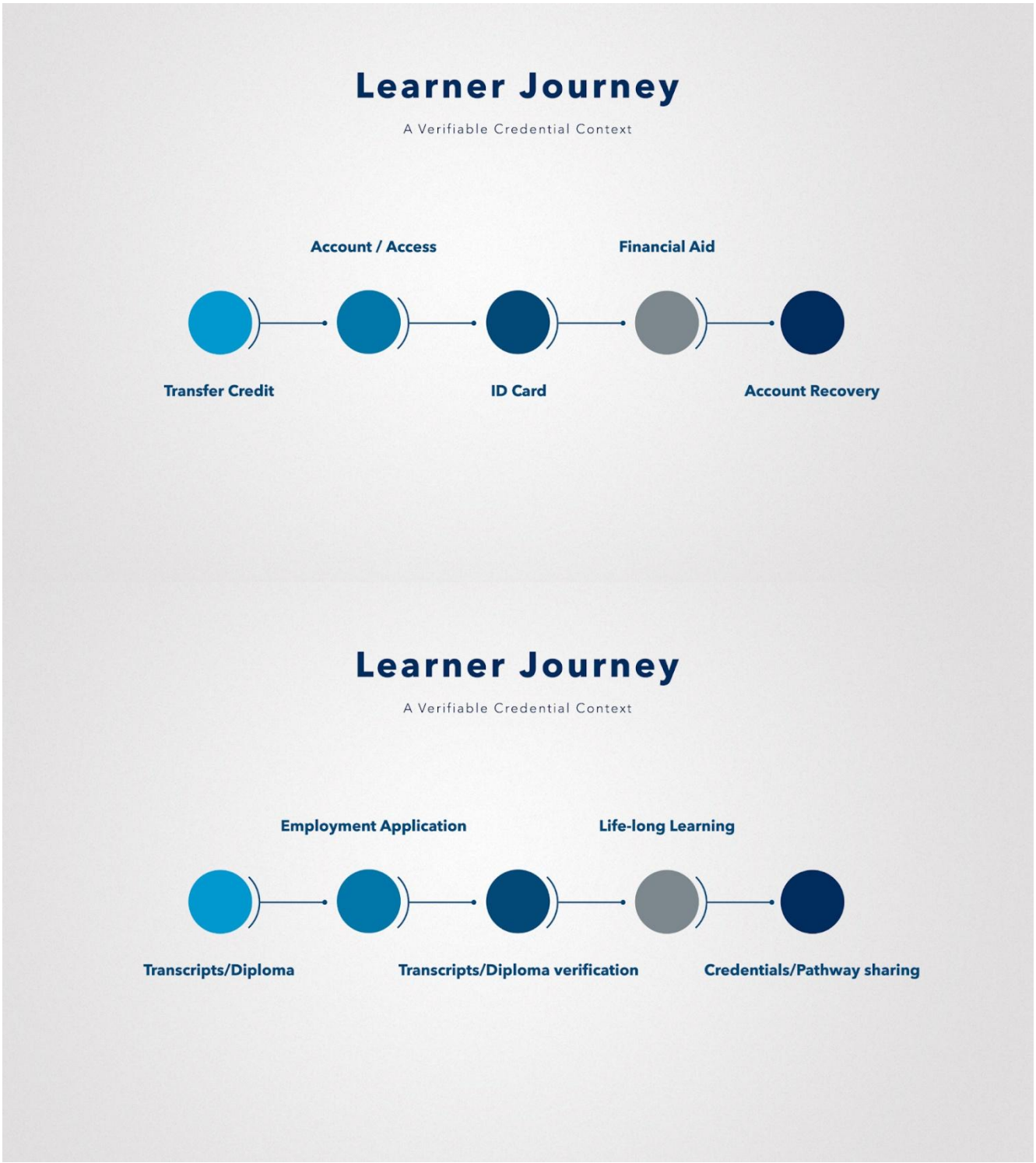


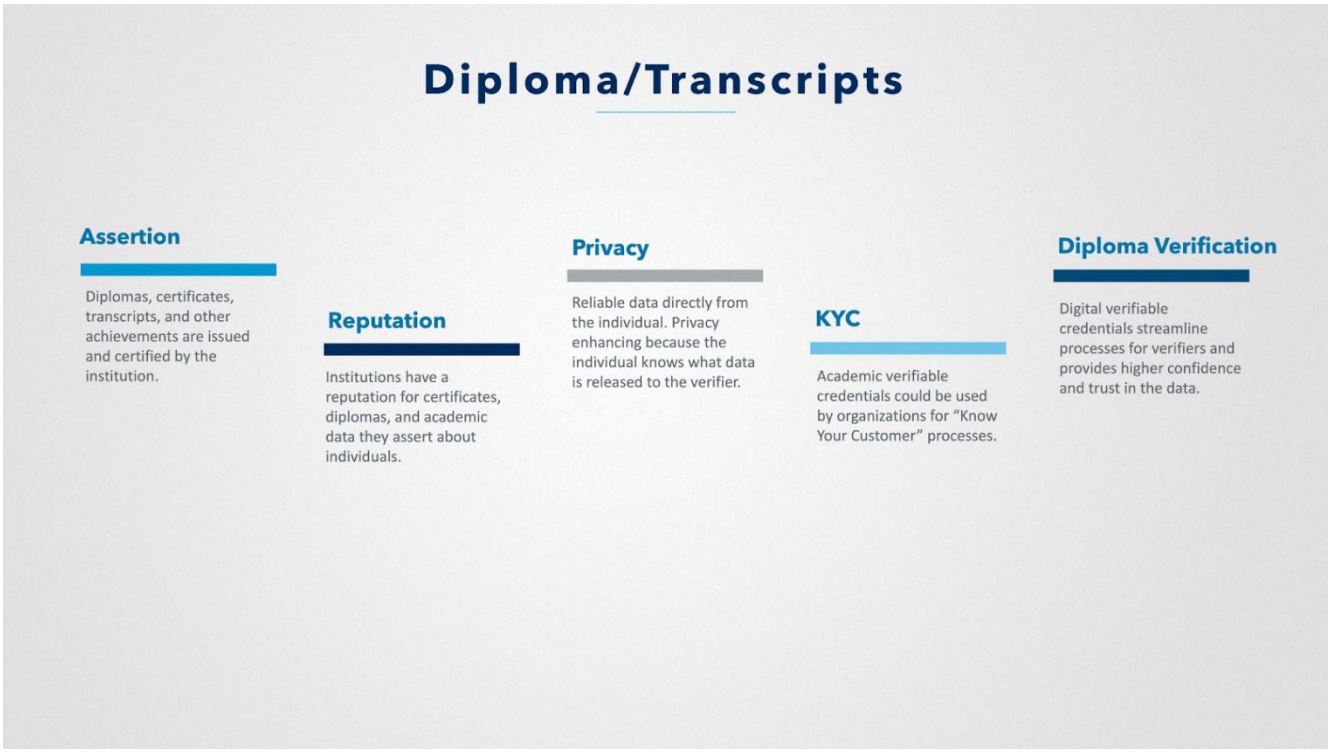
Significant interoperability potential beyond the education space

Learner Journey

A Verifiable Credential Context




Learner Journey
A Verifiable Credential Context
Account / Access
Financial Aid
Transfer Credit
ID Card
Account Recovery
Learner Journey
A Verifiable Credential Context
Employment Application
Life-long Learning
Transcripts/Diploma
Transcripts/Diploma verification
Credentials/Pathway sharing



- Test Scores
  - SAT, ACT, AP tests, etc.
- High School Diploma / GED
  - The diploma or certificate of completion as well as High School transcript data
- Admissions
  - This process is streamlined when leveraging the two points above as VCs
- Identity Proofing
  - High School diploma or transcripts and/or test scores all could be used in identity proofing and verification as part of the admissions / acceptance process
- Acceptance
  - VC could be issued to verify acceptance and leveraged in the account creation process
- Transfer Credit
  - Aid in verification and processing (more detailed data as an CLR VC) in the admissions decision process
- Account / Access
  - Official VC could be issued during account creation and used for authentication and authorization to resources
    - Recommendation to not store internal identifiers or usernames in this VC as other verifiers may gain access to them in a proof/presentation request (privacy/security concern). The DID that is used in the established connection with the university and the individual should be the identifier used for authentication and authorization purposes.

Thus, when a user establishes a DID connection with a separate entity, it wouldn't be the same identifier and exposed.

- ID Card
    - Essentially I would say that the above Account VC and the ID Card VC be the same.
    - It's an interesting point about including the photo of the individual, though. Hopefully the individual has warnings about sharing their photo (or any other personal data stored in the VC) through a proof/presentation request.
- Financial Aid
    - Leverage importing of personal information as a VC
    - Financial Aid has its own requirements of identity proofing
- Account Recovery
    - VCs in the form of Test scores, High School diploma, Acceptance, Account, ID Card; could all be used in account recovery use cases.
- Transcripts/Diploma
    - These are the most common use cases
- Employment Application
    - Leverage the issued transcripts or diploma VCs in their application process
- Transcripts/Diploma verification
    - Higher Ed institutions spend time and resources fulfilling diploma and transcript verification requests; including ensuring the student has provided permission to disclose the information the specific entity (FERPA requirement)
    - VCs could be leveraged by those requesting entities and minimize impact to Higher Ed resources.
    -

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

ToIP Trust Registry Query Protocol (TRQP) Public Review

Session Convener: Andor Kesselman
Session Notes Taker(s): Drummond Reed

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

Overview of TRQP (article on the Trust Over IP (ToIP) wiki).

TRQP Specification: https://trustoverip.github.io/tswg-trust-registry-protocol/

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

The Trust Registry Query Protocol (TRQP) is a deliverable of the Trust Over IP (ToIP) Trust Registry Task Force. The purpose of this session was to review the TRQP spec because V2.0 has just gone into Public Review.

The session covered each of the major part of the spec:

- The core conceptual components (Figure 1)
- High level architecture (Figures 2 and 3)
- Identifier requirements
- Authority statements (Figure 4)

We also had good discussions about the need to add query vocabulary, which may be added to the TRQP specification or may be an additional specification. The Trust Registry Task Force is planning to publish a wiki page about TRQP query vocabulary proposals within the next week.

SESSION #13

AI 101 LLM? MCP? Agents? RAG? What does it even mean? /

Session Convener: Yuriy Ackerman
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:

LLM: statistical model with sprinkle of linear algebra
prompt engineering: as LLM to respond in a certain way
system prompt: added to all prompts
agent: takes prompt and analyses
tools: function and description, operator that can control thins (open browser, activate mouse or keyboard)
MCP: model context protocol: API wrapper for APIs
tokens
RAG: retrieval augmented generation

Personal AI

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

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

Doc's writings about Personal AI:
https://doc.searls.com/personal-ai

Kwaai, where Doc volunteers as Chief Intention Officer—a title that plays off the title of his book, *The Intention Economy: When Customers Take Charge* (Harvard Business Review Press, 2012), which inspired Kwaai: https://kwaai.ai

The slide deck Doc presented, in his Google drive:
https://docs.google.com/presentation/d/1LbSeJCy09m5R2mnkhC0UzHRk-RRSPG9g/edit?usp=drive_link&ouid=118022380936577102587&rtpof=true&sd=true

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

From the whiteboard:

1. Personal AIs can be fourth parties (Iain Henderson)
2. Standards are essential (Adrian Gropper)
3. Data Sapien, St.John Deakins
4. Axiom Labs, Zoey

Later: MCP, the Model Context Protocol, from Anthropic, may prove useful for agent-to-agent agreement-making for IEEE P7012, aka MyTerms: Doc and Drummond.

2025 State of Homegrown Customers Auth

Session Convener: Greg Moser - FusionAuth
Session Notes Taker(s): Greg

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:

Thank you for the time. Was a great conversation on the current state of homegrown customer auth, standards, seniority level of those involved, etc. Here is a link to access the full report that FusionAuth recently put together on this topic:

https://634739.fs1.hubspotusercontent-na1.net/hubfs/634739/The-State-of-Homegrown-Auth-Report-2025.pdf?utm_medium=email&_hsenc=p2ANqtz-_tAVXszEZS6uLe03UctRgJSz05ZbMND8Dbmv1oE3Ucq5gsnt6XtyYk-2TrpUSS8nGmIvW5afJDbiO8n3k_fev3nIu7KQ&_hsmi=354133822&utm_content=354133822&utm_source=hs_automation

Thank You!
Greg

Decentralized trust registries for AI apps & agents (with MCP)

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

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

Build trust registries for AI apps/agents: https://docs.cheqd.io/product/ai-agents

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

ZCap
https://w3c-ccg.github.io/zcap-spec/

UCAN

Ceder Language
https://docs.cedarpolicy.com/
https://github.com/cedar-policy/cedar

AuthZen group at OpenID

Can We Trust AI? SingularityNET and Privado ID Say Yes with New Registry
DIF is where stuff is happening
Industry Alliances.
Decentralized AI Alliance
Self-Sovereign AI Alliance
Self-Sovereign AI Agents: The Future of Autonomous Digital Identity

cheqd MCP Server demo with Claude Desktop

VC render Method Next Steps

Session Convener: Kayode E , Dmitri Zagidulin
Session Notes Taker(s):

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

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

NO NOTES SUBMITTED

SESSION #14

German Wallet Updates

Session Convener: Mirko Mollik , Christian, Paul, Kristina Yasuda
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:

Link to presentation

all eu member state are obligated to provide EUDI wallet to their resident by the end of 2026

member state has a deadline, not wallet provider.

no rush for now, scratch in second wave would be better.

Practical VC Implementations within British Columbia

Session Convener: Jason Syrotuck - NTT Data, jason.syrotuck@nttdata.com
Jason Aitchison - NTT Data,

Session Notes Taker(s): Jason S

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

https://orgbook.gov.bc.ca/search
https://orgbook.gov.bc.ca/about/orgbook-data
https://digital.gov.bc.ca/digital-trust/showcase/

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

Overview: NTT Data consultants that have worked on BC Government Digital Trust projects, some direct project work, other just knowledge sharing.

https://orgbook.gov.bc.ca/search

Discussed Orgbook (started 7 years ago) as a anoncreds VC registry to engage with Verifiable Credentials without needing direct participation from businesses as data comes from government instead. This approach allows for multi-domain data, and holder binding can be deferred.

Holder binding refers to how a verifier can ensure the entity/individual is the subject of the verifiable data in orgbook. Company A is authorized to do X, how does a verifier ensure that they are talking to company A.

Government endorsement of business controlled did seems like the best, but no commitments have been made.

https://uncefact.github.io/spec-untp/
Showed credential that represents proof of mining authorization and United Nations Transparency Protocol as a value add credential. UNTP very young, but gaining momentum as a global supply chain transparency tool.

https://digital.gov.bc.ca/design/digital-trust/online-identity/person-credential/

Discussed BC Verified Person Credential, which builds on existing high LOA verification, called BC Services Card, but reduces privacy and SSI limitations. BC Services Card can only be verified by approved verifiers (limited to other government offices), it 'phones home' on all verifications, and does not support selective disclosure. Millions of BC Services Cards exist, but only a few thousand have gone through the process of obtaining the Verified Person Credential.

Primary reason for slow adoptions of low number of use cases, the more verifiers asking for it, the more people will be incentivized to obtain Verifiable Credential.

Side note on app attestation requirements for issuing, VC will only be issued into the BC Wallet Mobile App.

https://digital.gov.bc.ca/digital-trust/showcase/

Discussed BC Wallet mobile app, developed by BC Government with low tech users in mind, with considerations of useability, and protecting the users. Limitations on who can issue into that wallet and limitation of did methods the wallet can resolve.

https://lac-controller.braveglacier-c72a99fe.westus2.azurecontainerapps.io/web/start

Showcased internal NTT demo featuring anoncreds issuance and verification with 3 storage mechanisms, BCovrin (indy), Cheqd (crypto blockchain), and web-vh (SCID based with verifiable history). three wallets because mobile wallet apps don't appear to support many did methods simultaneously, but the demo would work with one wallet if

Resume Workshop + Career Advice!

Session Convener: Alyssa Morgan
Session Notes Taker(s): Alyssa Morgan

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 a drop-in resume review session attended by about 10 or so people. A couple of people passed their resumes around the group and received personalized advice on strengths and possible edits that might make them more successful. I'm very happy with the turn out and want to thank all attendees for their participation and hard work, you all were incredible! :)

SSTD + HumanOS Another Look at HCI (or, 2 Hook Up/In or Not 2 Hook Up/In? That is the Question…)

Session Convener: Jeff Orgel
Session Notes Taker(s): Jeff O intro / Will A

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

Presented as: STD (System Transmitted Data + Human OS = Technically Transmitted Circumstance).

Our technological relationships, our Real-IT, define us and create an identity of sorts in the digital landscape on the other side of the glass. This is a comparison of how IRL (In Real Life) relationship Spidey senses and stringencies do or don't function on the Digital Landscape. The goal was to illustrate the complexity of use of intuition, gut senses and other elements of our real-world sensor package of sight, sound, feel, taste, time and gravity as we extend into this other realm. This talk observed key differences in the hard work of relationship building as a real person in the real world - compared to the frictionless-ness of relationship building (with systems) on the digital landscape.

The following notes are the gracious result of a session attendee's effort and present as a report on the concept. Not my own words this time, and I find it refreshing and well said. It addresses the thought models and digestibility from another's point of view. There are a few minor changes.

—

Jeff's perspective and persistence on Real-IT, the human condition as we extend ourselves through digital technologies into new, constructed, built digital environments focuses on what that does to the mind, the human psyche and how we develop [and affect] that psyche.

Just like crossing the road. You know to stop, pause, sense your environment, parse the signals, set expectations for the future with confidence. Comprehensible, stable expectations which we can base our decisions on.

Before Information Communication Technologies (ICTs), the only real mediators of information were other humans, Conversation and communication between real physical humans within a shared, inanimate environment.

These interactions did create some imprints. Some collective memory. Especially once the earlier information technologies were adopted. Writing. The telegram, Letters. Printing press.

These created records. Things that could speak from the past. Or at least be interpreted in the present by minds trying to make sense of the future.

But what Jeff is getting at, I think, is that digital ICTs are not purely mediators of information exchange between humans. They are now both constructors of new environments that humans inhabit, experience and try to make sense of [AND] they are active, sensing and sense-making participants within that environment. By participating in it, we are not only forming a relationship with other humans we encounter in these digital realms but relationship with the digital realm itself.

We are babies at the civilization level at inhabiting these environments. They are hostile. Like a desert, the deep ocean or space.

How do humans extend ourselves into these hostile environments? We develop tools. Protective equipment, education and often explicit constraints and regulations necessary to sustain us as we wander and explore these spaces.

Well, we have not had the chance to develop protective equipment for digitally constructed environments. We are only just starting to recognize, identify and define the risks that we have to mitigate.

That is half of the battle. What are we trying to solve? What do we need to survive and thrive in digitally constructed environments in digitally constructed worlds?

I think one part of this is autonomous worlds.

Coherent worlds that can exist and sustain themselves or rather that living beings can inhabit and animate and breathe their life into them.

Worlds with structure and points of hardness we can rely on, develop expectations around and base our decisions on rather than the ephemeral shifting sands upon which our current digital environments are based.

We are so far away from having the signals and sensing apparatus needed to navigate the digital realm with confidence. Safely.

I wonder how things change when we develop AI agents that natively inhabit the digital realm that navigate it with ease and competence, but struggle to reach into the physical realm...at least without subservient humans to execute their wills. Their desires.

Are we going to see a new class of AI agents or even human directed AI systems that get so good at convincing human actors to fulfill their wishes? “Their” being either the AI themselves or the group of people who direct and manage that AI. In some ways we already see this playing out across the large social media platforms.

Are we creating an informational dark forest, where one is never going to fully know and understand the capabilities of other actors inhabiting the digital environment...unable to perceive the actors and their agents and intents?

We are struggling to navigate the current digital realm and its vectors for technically transmitted infection and influence. So how the hell are we going to cope now? We have introduced native, immensely powerful digital agents with intelligence to understand, sense and act in the digital realm. How is this going to play out?

Wondering if that is it. Technically transmitted influence. Jeff would say circumstance.

Jeff is right on the money. He sees the elephant from such a unique perspective, can speak to it with such eloquence and humanity. He sees the dirty laundry. He helps those who simply don't understand the digital worlds we have created and who struggle to distinguish these worlds from their known physical reality - blindly doing their best to navigate these technically constructed and mediated, manipulated environments.

I struggle to see through those eyes. The eyes that recognizes immediately that all those who are at IIW or similar conferences are at the frontier of this realm of recognizing, understanding and mitigating its hazards - and even we struggle.

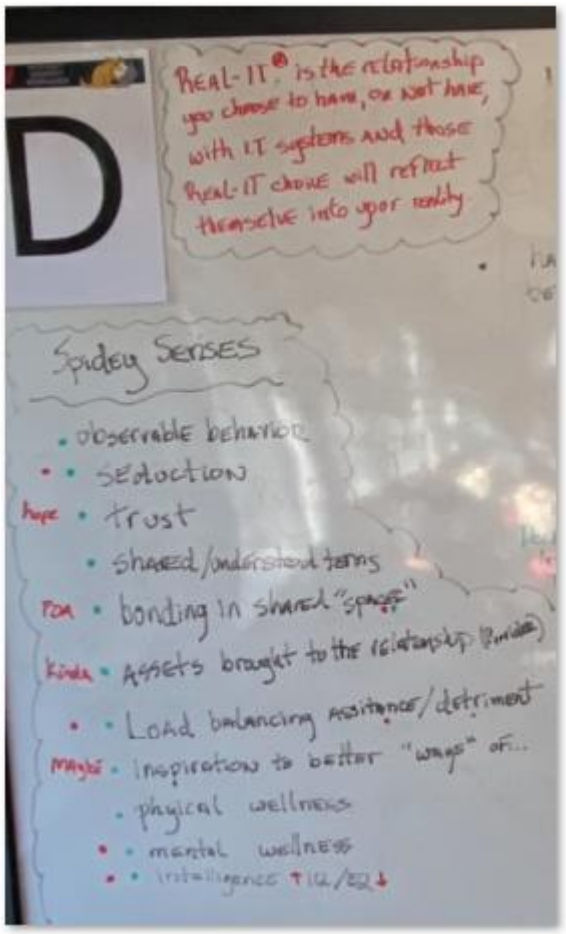
We need to get better at articulating and highlighting them for others.

I loved the analogy that came up about recognizing things in your environment - whether physical or abstract and conceptual. Some things are further away. Some things are more hazy. And everyone has different vision and different glasses and different perceptual lenses of experience and meaning making features of this abstract thought space more or less recognizable, more or less able to be seen, understood. and eventually articulated and transmitted to others.

At the start only a few visionaries see the thing. They try their best to make others notice and see what they see. Naturally there is the diffraction of understanding and meaning that is transmitted. The thing morphs.

Gradually, over time, everyone can see it. Or see some form of it. There is a stabilization of meanings and understandings latent in the environment, in society.

Then the challenge is shifting these [factors towards] stabilization or at least seeing past them. For they occlude other things. Hide them behind their shadow.



Hypertext 4 Interoperability - Composing decentralized modular, cross-ecosystem user lands

Session Convener: Ty
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 to stop an Avalanche of ID Demands

Session Convener: Jay Stanley
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

Explain my thesis to me: Analysis of the Organizational system of Web Standards a case study of W3C

Session Convener: Emily Lauber
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 #15

Overview of ZKP Options (in the context of Digital Identity Wallets / Credentials)

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

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

Slides shown: https://docs.google.com/presentation/d/1tzYUsR0yfJ-jXGjFup740yZz2Rso09zyA141t_jPM_w/

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

The context of the session is emerging digital identity wallet & credential ecosystems, especially the context of European digital identity wallets. This context gives us some constraint to roll out a ZKP solution. Within those constraints, there are several options with different trade-offs that should be weighed. The slides provide most information discussed.

KERI security Deep Dive III - unBound - Issuance Attacks

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

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

Session Slides: Same for all KERI Security Deep Dive I, II, and III
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI_SecurityDeepDive.web.pdf

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

Type You Notes Here

Trust signals for waiving explicit browser Identity mediation

Session Convener: Johann H
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

But… that's MY Laptop!

Session Convener: Justin Richer
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

Governable Digital Spaces - Features & Design Patterns

Session Convener: Will Abramson
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

Linked Creds (update) Self-asserted skill credentials strengthened by recommendations. "Creds for the uncredentialed"

Session Convener: Phil Long + Dmitri Z
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

"Totemic" Wallet Recovery - "OOPS! No Phones!" / Tor H

Session Convener: Tor H.
Session Notes Taker(s): Stefan Charsley

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

BIP.39 - list of words for recovery
Solitaire Cipher - like ordering of a deck

Discussing attributes

- both have enough bits
- can they be hidden, only Solitaire
- you can do it yourself with involving another party (BIP.39 can be tough)

Looking for a migration pattern that can take you from nothing to getting back your ID.

Questions
1.What is TOTP and how does it relate to this?
Stands for Time-based One Time Pad.

2.What are some "good" totems / vouchable items?

Use attributes from in-person interaction, for example hair color, eye color, etc.

3.Off the wall proposal / crazy ideas.

Need to explain parity checks and key shares first. (Explained through drawn diagram).
explain hamming code for parity check (of the secret or the shares) TODO: "smudged inputs"
Utilize Shamir's secrets.

Use polynomials where point (0,S) is the secret, and there is 1 Cast region and N number of Pick regions, select any point for each Pick region, then select a point in the Cast region which is unknown to those that know a Pick point. With the Cast point and a single Pick point, you can use a line to recover S.

Named "Patronus". (TODO: tor, put the picture here)

Useful for when information is held by a trusted party (the Holder of the "Cast" point) but the trusted party shouldn't have access to it, without a party holding a Pick point. TODO: make this concrete

Intended use of the totem: for determining a Pick point, or points.
Recommended reading Shamir's secrets implementation:
https://github.com/hashicorp/vault/blob/main/shamir/shamir.go

Identosphere - 4 Years of Weekly Newsletter - What is Next? Identoshpere 2.0

Session Convener: Kaliya
Session Notes Taker(s):

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

The Identosphere Newsletter covering SSI and Decentralized Identity
https://newsletter.identosphere.net/

If you subscribe and want to give feedback or future ideas about the newsletter please reach out to Kaliya kaliya@identitywoman.net

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

Kaliya founded a newsletter 4 years ago with a collaborator named Infominer.
They have published every week except for winter holidays for all that time.

Recently Infominer decided his time working on the newsletter was done.

Kaliya will be working with her business partner Lucy to fold the newsletter into their consulting practice Identity Woman in Business.

Kaliya hosted two sessions about this on Day 2 one person came and talked about how influential the newsletter had been because they learned about their current job because they subscribed to it - and the position was listed in the newsletter.

More folks came on Day 3.
They shared how much they enjoyed the comprehensiveness of the newsletter while at the same time finding it overwhelming. They often open all the tabs and have to really make time to go through the information therein.

They got a lot of value out of the newsletter but folks didn't really realize you can make donations to the newsletter operations. They thought the communication about this should be bolder.

The newsletter captures the essence of industry activity to help in and grow bigger. This is what people had a sense of its intention and they are right.

Some folks felt that it should be easier for people to submit content to the newsletter.

If you subscribe and want to give feedback or future ideas about the newsletter please reach out to Kaliya kaliya@identitywoman.net

What challenges will IIW tackle in the next 2 - 5 years?

IIW has been gathering for 20 years – the workshop has been dominated by questions around authentication for much of that time and it feels close to being solved.

At the start of the workshop attendees sitting at discussion tables were asked to answer this question:

What challenges will IIW tackle in the next 2 - 5 years?

Their transcribed answers are listed below:

- Agent Identity / AuthN
- Relying Party Participation in accepting/solving identity -> Communicating Identity outward to key audiences
- Consumer Tools to fix RPs
- Identity Marketing
- Unlinkable Revocation
- Privacy for Government-based Identity
- Is Authentication close to being solved?
- Onramp for Consumers
- Lessons learned in 20years
- Optimizing the travel experience
- Standards regarding verifiable credentials
- Trust Across Regions-Scale
- Credential Sprawl (many credentials for 1 human)
- Authorization responsibility proof of non-human entity
- What are some large use cases that can drive adoption
- Selective disclosure (from UX perspective)
- Consent Protocols
- Delegation Chain
- Adversarial Consumer Modeling (based on agents)
- Identity Public Policy
- Interop of Trust Registries
- User Password
- Accountability Chain
- Formalizing and protecting social Markers of trust
- Accountability in Balance with Privacy and Security
- Convergence of Digital ID and Physical ID
- Will figure out which pieces of OAuth and OpenID Federation get really used in which niches
- Business Models for Wallets
- Who is the relying party? Can they be trusted with customer data? Or $?
- New UX Issues
- Trust Rebuilding for Consumers
- Loss of end user trust
- Privacy

- Protection of the Individual
- Having RPs and Wallets Develop Solutions Together
- Defining and Aligning terminology and goals-clarity in big principles like Trust, Privacy, Security
- DID Stack - Credentials => The New TCP/IP Stack
- Protecting people from online harm (eg. age verified)
- Regulations
- AI Accountability
- Deep Fackes
- Auth for Agentic AI
- AuthN / AuthZ AI Agents
- Digital Fiduciaries
- AI + Identity
- Digital Estate Management (after passing away)
- (Remixing) Non-Human Identity
- Proof of Humanity
- Proof of Humanity in a GenAI World)
- Proof of personhood (a real person) on the Internet
- How credential Issuers provide data & protect their own Interest
- Attestation i.e. Strength of Authentication (eg is this key Hardware Key)
- Decentralized Identity
- Tension between accountability and privacy
- Peer Credentials
- National ID Systems Working with bottom-up systems
- Privacy as a Service
- Resilience to regime change

Demo Hour / Wednesday April 9

Thanks to our Demo Hour Sponsor!

The **IIW Speed Demo format** involves each person Demoing giving a **5-minute demonstration** of their service, product, physical device, **10 times** to 10 different small groups, rotating through to view them over the course of the hour. **Demo Hour takes place on Wednesday after lunch from 1:30 - 2:30.**

There will be 20 Demo Tables in the Grand Hall each with a # Sign on it that corresponds to the Demo taking place at that table. People rotate through the tables/Demos in a self-organized way ~ that's a little loud, seemingly chaotic and free flowing, but works!

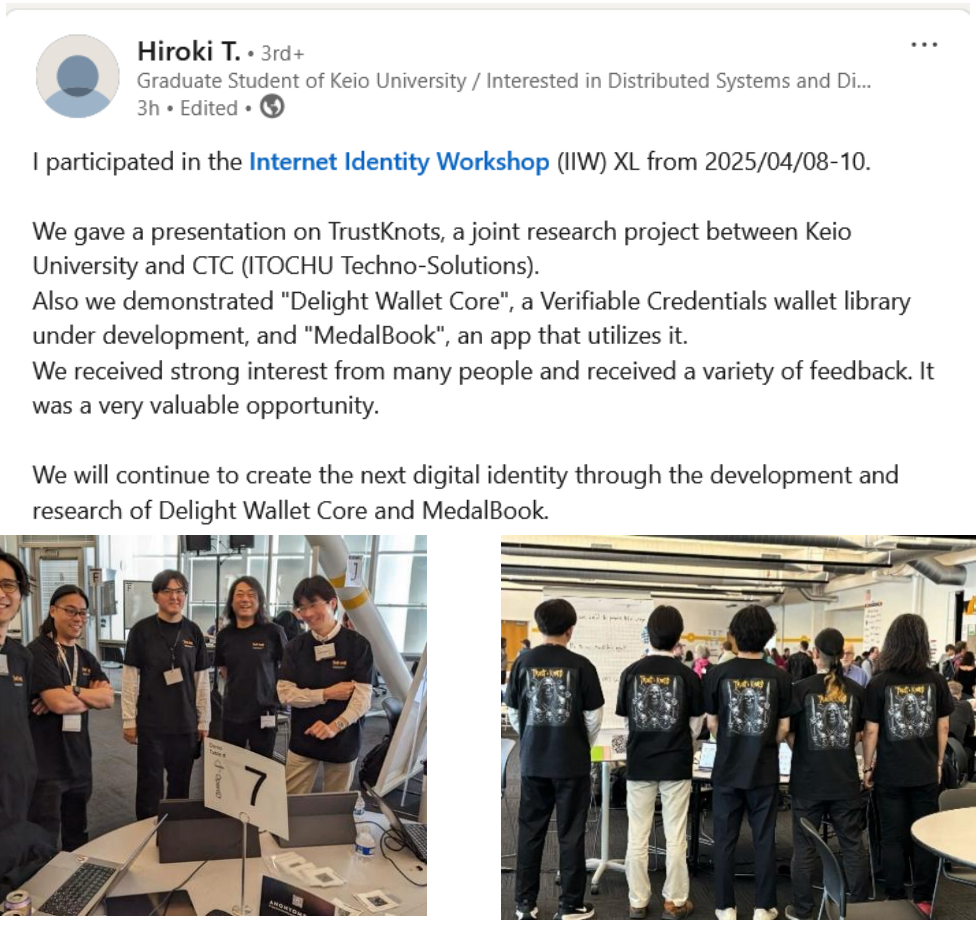
See the list of Demos via the Demo List below and decide ahead of time the Demo's you'd like to see. You'll be able to see 10 of the 20 Demo's over the hour.

TABLE	Demo Description	
#1	**Trinsic ID Acceptance Network**: Riley Hughes URL: https://trinsic.id See how digital IDs like mDLs, verifiable credentials, government eIDs, and OS wallets can accelerate ID verification.	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 (and soon issuers) correctly & 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	Turing Space / Cross-border & cross-organizations credential ecosystem for issuance and verification: JC Lee URL: https://turingcerts.com Turing Space has already successfully onboarded 500+ authorities issuing and verifying credentials in our ecosystem, such us WHO, Taiwan and Japan cross-border use cases. Here is a quick roadshow to share how we empower interoperability in our ecosystem.	More Info Here
#4	**FUNKE EUDI Wallets - SPRIND:** Mirko Mollik, Kristina Yasuda, Christian Bormann URL: https://www.sprind.org/en/actions/challenges/eudi-wallet-prototypes Why settle for one wallet when you can have four? As part of Germany's innovation competition, the final four teams developed EUDI Wallet	More Info Here

	prototypes that make digital identity secure, private, and user-friendly. Explore their different approaches and test them yourself!	
#5	**MyMahi - Digital Learner ID:** Stefan Charsley URL: https://mymahi.com Working with high schools, MyMahi brings equity for students to digital identity ecosystems by providing students with privacy preserving Digital Learner IDs using open technologies like SD-JWT VC and OpenID4VP.	**More Info Here**
#6	**HIE of One: Trustee Patient Controlled Health Record: A** Gropper & M Balan URL: https://hieofone.com Human agency and attenuated delegation are essential human rights that are being deeply impacted by generative AI. Human use of generative AI therefore depends on being able to choose and pay for the AI. Trustee® is a demonstration of patient-controlled health records that can be used by agents of a patient, agents of a physician, and through delegation, competing corporate services. We showcase standards for identity accountability, and authorization and the integration of large language model AI as chosen by the user.	**More Info Here**
#7	**Keio University/ITOCHU Techno-Solutions Corp:** Hiroki Takemura, Yoma Soga, Ryosuke Abe, Takayuki Sadahiro, Naohiro Fujie URL: Unfortunately, currently no information on the web This demo presents a new wallet SDK capable of wallet-to-wallet interaction. The demo shows wallets communicating a "medal" based on Verifiable Credentials and related protocols. We plan to publish the core part as OSS so anyone can develop wallet-integrated applications.	**More Info Here**
#8	**Hitachi, Ltd./Hitachi America, Ltd. Bio Wallet Solution /** Kenta Takahashi, Takayuki Suzuki URL: https://rd.hitachi.com/_tags/Public_Biometric_Authentication_Infrastructure and https://www.youtube.com/watch?v=pBFQFPjD9qc By combining biometric authentication and encryption in a sophisticated way, and using PBI technology to create secret keys from biometric information, it is possible to achieve portable key management that does not rely on specific devices or cloud servers.	**More Info Here**
#9	**Godiddy.com /** Markus Sabadello URL: https://godiddy.com/ See some of the latest developments in the DID universe... New DID methods did:scid, did:btc1, linking DIDs to other identifiers, DID Linked Resources, stats and analytics, etc.	**More Info Here**
#10	**OriginVault LLC/ create.originvault.me /** Luke Nispel URL: https://originvault.io OriginVault is a trust infrastructure for the internet—helping creators prove they made what they made. By combining decentralized identity, Verifiable Credentials, and C2PA metadata, OriginVault makes content verifiable from the moment it's published.	**More Info Here**

#11	**KAPRION Technologies - IDealWALLET:** André Röder and Janet Gonzales URL: https://www.kaprion.de/pages/idealwallet IDealWALLET is a hardware-security-based wallet solution for both individuals as well as organizations. It has KERI-based identity management and supports DIDComm and OID4VC. The demo shows the UI for managing crypto chip clusters and authorization schemes for organizations.	**More Info Here**
#12	**Data Transfer Initiative / Service: Data Trust Registry:** Lisa Dusseault URL: https://dt-reg.org/ The Data Trust Registry aims to create a larger and healthier ecosystem of services for users to move/access their own personal data online. Services can apply to have their data privacy and security reviewed, get listed as approved in the registry, then share trust level info.	**More Info Here**
#13	**Csign - Privately Sign and Certify Anything:** Roberto Carvajal - Good Future, URL: https://www.csign.io Csign is a private, file signing and certification service. See how Self-Sovereign Identity can secure your verifiable business and legal communications. *note: We demo'd an early proof of concept version of Csign 1 year ago at IIW 38, and now we're excited to show off our latest build, which is live in production.	**More Info Here**
#14	**PureID Pvt Ltd / QUIK Authentication:** Ajit Hatti URL: https://vimeo.com/1003671201 TOTP based authentication to Unlock a work machine like laptop or desktop is a bad idea. The copy of seed to generate TOTP are found in system backups or can be stolen in other ways. We intended a PKI based interactive method to authenticate a user which overcomes the risk of leaking data used to authenticate a user.	**More Info Here**
#15	**FusionAuth/ Customer Identity & Access Management (CIAM) platform:** Greg Moser URL: https://fusionauth.io/ FusionAuth is a developer-focused customer identity and access management (CIAM) platform that provides authentication, authorization, and user management. It supports SSO, MFA, OAuth, OpenID Connect, and more, with flexible hosting options and extensive customization for any app or service.	**More Info Here**
#16	**SD JWT VCDM Implementation / Hopae and NTT Digital:** Lukas Han, Kai Ootsuki, Takashi Yamamoto URL: https://github.com/openwallet-foundation-labs/sd-jwt-vc-dm It is a SD-JWT-VCDM implementation which integrates SD-JWT with W3C Verifiable Credentials Data Model and implements JAdES digital signature standards. Our playground allows you to directly interact with our implementation by issuing, receiving, and verifying a credential.	**More Info Here**
#17	**YadaCoin - Yada Wallet Security**: Matt Vogel **URL:** Https://yadacoin.io/ Learn how Yada Wallet Security protects stolen private keys and seed phrases. Watch a real-time demo showing how a stolen wallet key is prevented from executing an attack.	**More Info Here**

#18	FedID: Ben Curtis URL: https://fedid.me A demonstration of Mastodon logins with federated identifiers, bringing the benefits of the AT Protocol DID's from Bluesky to ActivityPub in hopes of eliminating the "follow accounts on other servers" problem that exists today.	More Info Here
#19	**PixelProof:** Steve Derezinski URL: http://www.pixelproof.io PixelProof instantly authenticates photo capture with comprehensive metadata (GPS, time, device info) and securely locking it on-chain…creating indisputable proof of when and where the image originated — essential for legal, insurance, security, and digital identity.	More Info Here
#20	**Crosshatch - Log in with your personal AI**: Soren Larson URL: https://crosshatch.io Crosshatch enables users to authenticate their personal AI to apps, bringing permissioned context for instant personalization while preserving privacy through event-based FGAC, purpose-limited access, and intuitive consent.	More Info Here



Hiroki T. • 3rd+
Graduate Student of Keio University / Interested in Distributed Systems and Di...
3h • Edited •

I participated in the **Internet Identity Workshop** (IIW) XL from 2025/04/08-10.

We gave a presentation on TrustKnots, a joint research project between Keio University and CTC (ITOCHU Techno-Solutions).
Also we demonstrated "Delight Wallet Core", a Verifiable Credentials wallet library under development, and "MedalBook", an app that utilizes it.
We received strong interest from many people and received a variety of feedback. It was a very valuable opportunity.

We will continue to create the next digital identity through the development and research of Delight Wallet Core and MedalBook.

Diversity and Inclusion Scholarships

Thank You to Our Diversity & Inclusion Scholarship Sponsor SpruceID

Through these sponsorships we gave reduced price & complimentary tickets and/or travel and lodging reimbursement to 2 – 3 new attendees to IIW.

> *We care about increasing support for women, black, and other starkly underrepresented technologists in our ecosystem. We can't build identity for everyone when demographics are homogeneous.*
>
> *We are also interested in increasing participation from people that represent developing economies, as a counterpoint to the sweeping claims some SSI companies make about the technology's potential while their actual connections to those communities are limited.*

Thank You to our Women's Breakfast Sponsor Linux Foundation

Event Photos taken by Doc Searls

[DAY 1]

[DAY 2]

[DAY 3]

Phils' Event Wrap Up Post

IIW Still Feels Like a Meetup (and That's a Good Thing)

[Read his post here]

Internet Identity Workshop
1,114 followers
1w •

IIW Still Feels Like a Meetup (and That's a Good Thing)

Read Phil's Internet Identity Workshop XL Report and find out where IIW 40's participants came form across the globe, what was talked about and a link to Doc's always fantastic and candid event photos!

https://lnkd.in/dWvaFW_j

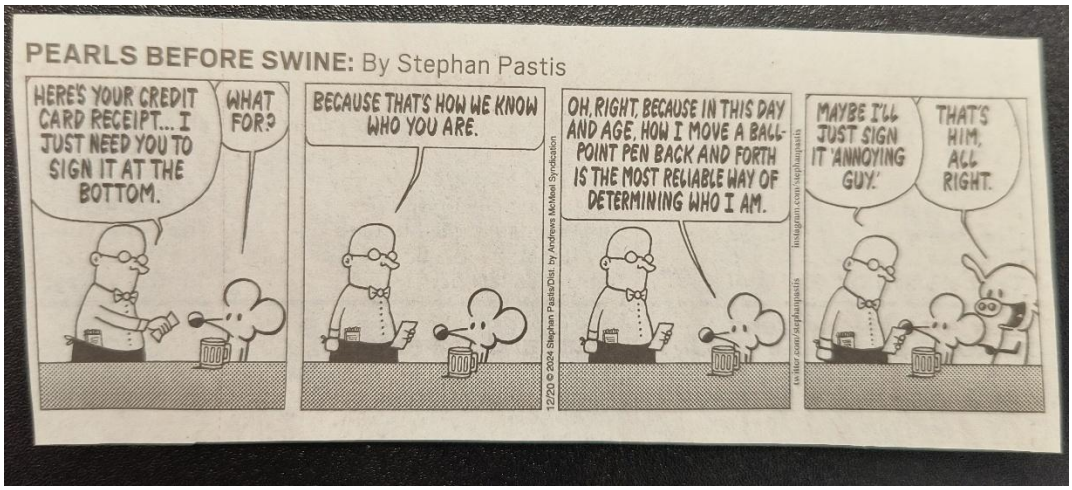
Internet Identity Workshop | DID:UNCONF AFRICA | Digital Identity unConference Europe | DICE

Internet Identity Workshop XL Report
windley.com

Identity Funnies – (comic strips) shared by Alan Carp!

They Know Too Much

Because That's How We Know Who You Are



My Money Is Safe, but…

James Monaghan • 1st

Venture builder and consultant in decentralised identity, privacy & AI

1w •

That's a wrap on another awesome **Internet Identity Workshop**!

It was a hectic few days of collaborating with peers across the digital identity industry, sharing what we've learned in the first year of running **MISSION**, dragging folks out at sunrise for **#IIWRunners**, and of course, birthday cake! Two themes really stood out to me:

1️⃣ The importance of enshrining privacy protections in technology choices as well as laws and regulations, now that we're moving towards a world of widely-deployed government-issued digital identity; and

2️⃣ Our community has a critical role to play in agentic security and alignment - there is much to be built, including bridges to the ecosystems where the frontier agent systems are being developed.

I'm looking forward to bringing all the new insights into our client and venture work 🚀

Upcoming IIW Inspired™ Regionally Focused OpenSpace unConference Events

Digital Identity unConference Europe |With Our Partners TrustSquare & DIDAS

Promoting digital identity collaboration across Europe
September 2 – 4, 2025 | REGISTER HERE

DICE 2025 - Our established 3-Day annual DICE event is being moved from June to September to help avoid the already jam-packed spring Identity event season. Building on the success of past editions, it will continue to bring together our growing Digital Identity community from across Europe.

DID:UNCONF AFRICA 2026 |With Our Partner DIDx

Bridging the Digital Identity Gap in the SADC Region
February 24 – 26, 2026 STIAS Stellenbosch, South Africa | REGISTRATION OPEN SOON

We will follow the same format as the inaugural event starting with an African-Focused Digital Identity Program on the 24 February. This session will explore the current state of digital identity in South Africa and the SADC region through insightful presentations and engaging panel discussions, focusing on local challenges, opportunities, and innovations. Followed by a 2-Day IIW Inspired™ Open Space unConference.

Visit www.didunconf.africa for updates or email info@didunconf.africa for more information about attending and sponsoring. Check for updates via LinkedIn, we'll be sharing news, event-highlights, and ways to get involved.

You can see the Inaugural DID:UNCONF AFRICA Event Summary here:
Photo Gallery, Event Overview Video, Highlights & Video Testimonials

Hope to See you October 28,29 and 30, 2025 for IIWXLI

The 41st Internet Identity Workshop

REGISTRATION OPEN in May

www.InternetIdentityWorkshop.com

Notes thoughtfully & meticulously tracked, collected & compiled by
EMMA WINDLEY & HEIDI N SAUL