

IIWXXXIX



INTERNET IDENTITY WORKSHOP 39



October 29–31, 2024

Book of Proceedings

www.internetidentityworkshop.com

Computer History Museum / Mountain View CA



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

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

Thank You! Documentation Center & Book of Proceedings

Sponsors: inrupt and Procvivis



Contents

- Thank You! Documentation Center & Book of Proceedings Sponsors: inrupt and Procvivis..... 1
- The Book of Proceedings Helps with FOMO..... 6
 - Sir Trust-A-Lot & The Shield of Digital Identity win best Halloween Costume! 6
- About IIW 7
- Thank You to Our Sponsors! 9
- IIWXXXIX Daily Schedule..... 10
- IIW39 Agenda Creation = Schedule & Workshop Sessions..... 12
 - Tuesday October 29, 2024 Day 1 / Sessions 1 - 5..... 12
 - Wednesday October 30, 2024 Day 2 / Sessions 6 - 10..... 14
 - Thursday October 31, 2024 Day 3 / Sessions 11 - 15..... 16
- Notes Day 1 / Tuesday October 29 / Sessions 1 - 5 21
- SESSION #1 21
 - FedID / FIDC 21
 - OAuth 101 - IIW 101 Session 22
 - Agents and the Mee Data Network..... 25
 - Progressive Trust in Issuer Registries with LinkedClaims 26
 - OpenID for Verifiable Presentations Editors’ Draft..... 28
 - Scalable Signing Infrastructure)- 100,000 txns with KERI..... 28
 - A Scarlet AI for Browser UX to show users where slop is / Ross K. Rohit Khare..... 29
 - MOSIP Introduction - Imagining Digital Transformation Through DPI 29
 - Verifiable ID with the State of Utah - Why are we different?..... 30
 - Government Go Fast: An introduction. 30
 - Killer Credential Network Effect: An Introduction to the Global Acceptance Network (GAN) 31
 - FedCM, Digital Credentials, and WebAuthn - future of consumer login..... 34
- SESSION #2 38
 - ISO mdoc 101 38
 - Introduction to OpenID Connect / IIW 101 Session 38
 - Social Media/Web and Identity discussion 42
 - Anonymity vs Privacy 46
 - How to Make \$Money\$ from SSI? 48
 - Privacy and the Mobile Drivers License (MDL)..... 48
 - SD-JWT and SD-JWT VC 101..... 50
 - Sync is not Send 50

VLEI Update - Verifiable Legal Entity Identifier - GLEIF	50
Has our SSI Ecosystem become Morally Bankrupt?.....	51
Digital Fiduciary Initiative	53
The Challenges and ROI of Verifiable Credentials in Enterprise Use Cases	57
SESSION #3	61
SD-JWT VC over proximity/offline	61
IIW 101 Session - Authorization 101 Intro/Tutorial on the AM in IAM.....	63
OCA Schemas.....	63
C2PA vs TOIP TSP - What are they good for anyway?	66
Security Questions - Back from the Dead	66
Decentralized Trust / Trust Registries	67
EIEIO = Embracing Interop in Enterprise Identity Online	70
Crossing the Rubicon: Road to CESR.....	71
Personal AI on Digital Public Infrastructure	73
Universal Basic Bandwidth	74
CBOR DID & VC Controller Documents, Implementing Elision Privacy with Gordian Envelope	75
Migrating from DID:Web to DID:Webs at Switchchord	75
DID Method Squid Games.....	76
SESSION #4	79
Digital Credential Query Language	79
IIW 101 Session - Passkeys 101 AKA FIDO	86
Open Wallet Ask Me Anything	86
Consumer Reports AI Agent - discussion - - - > / Dazza Greenwood, Ben M, Ginny F	87
Come build your project with DIF Labs	87
Regulation Identity & Privacy - Why you need to care!	88
OpenID AuthZEN: the "OIDC" of Authorization	89
Credential Schema Standards: KYC and Proof of Personhood.....	90
SESSION #5	91
KERI Security Duplicity Evident Data Provenance + AI Safety.....	91
IIW 101 Session - Intro to Self Sovereign Identity.....	92
Zero Trust with Zero Data	92
Autonomous Worlds	94
Brainstorm way to link de-identified health data for population health in a privacy-preserving way.....	96
Delegation / Authorization for consumer-driven AI agents/ Standards for Human Agency/ ..	97
Intro to Trust Over IP (ToIP).....	101
Web Authn + EUDI RP Authentication.....	101
Technical introduction to Global Acceptance Network (GAN).....	102
Identity Practitioner Pipeline - a conversation with DIAF, IDPro, OpenID... and you :-) about bringing New People into identity	103
Edge Identifiers, Cliques, and other Opportunities of Multi-Party Computation (MPC) & ZKP	104
Notes Day 2 / Wednesday October 30 / Sessions 6 - 10	105
SESSION #6	105
Germany EUDI Wallet Project update	105
An abstraction for "pluggable" Verifiable Credentials and Zero Knowledge Proof libraries: Now with implementation and test framework!	106
Aviation Security Trust Framework	108

Delegation & Impersonation for AI (and other) agents “on Behalf of” Human Users.... Token Focus	113
State-Endorsed Digital Identity.....	115
HumanOS Stack * How you evolved your Digital Identity	117
Decentralized ID - Selective Disclosures - BLE! WORKS! - eID -Me = A Canadian View	119
Digital ID toolkit: come give us feedback and learn how to play!.....	119
Scope and Role Granularity for Usability	120
SSB Intro to Secure Scuttlebutt (10+ years and more)	123
The First Person Credential.....	123
UR CODES Turn “BEARER” Documents -> Biometric-Bound Documents!	124
OpenID Foundation FAPI 101.....	127
SESSION #7	128
FedID / FIDC	128
The Laws of Externalized Authorization	129
Trust Network Design Session	131
SESSION #8	133
Google’s ZKP for MDOCs.....	133
Wallet and Agent Overview @ OWF.....	133
Dude (Person), Where’s Your DID? (An update on how individual and organizational identity fits into the C2PA ecosystem)	134
“Verifiable AI”: Content credentials, proof of personhood, proof of “approved AI agent” and more.....	135
Personalized AI	136
Device Profile as a VC for Device Recognition	137
Identity Brokers in OAuth	137
Identity and the Social Web	145
Why is the OpenID Foundation hopping right now? An overview of the 14 work groups and community groups on now	147
DWeb Deep Dive and Web 5 / OWN Updates + Wallet	147
Portable Communities	148
Adopting OAuth2.0 for First-Party Applications - Building the Authentication Layer	149
Secure Technology Alliance - Mobile Driver’s License (mDL) Jumpstart	150
How does a person’s agent talk to an RP	152
SESSION #9	153
RP Authentication and Authorization for the EUDIW (European Union Digital Identity Wallet)	153
Interoperable, Private and Feature-rich?! Tru.net The new town center built on JLINC w/Fed DID’s / Simply Sharing Credentials.....	154
BYOC - Bring Your Own Use Cases - Whatever! Real or Imaginary	155
AI - Oh My! Practical 101 on RAG Architectures and what it means for Identity.....	155
Intro to Originator Profile.....	156
Open Source AI	157
Accountable Wallet - A wallet can prove your legitimacy using VC’s ZKP’s	157
The Business of Enterprise Identity.....	158
Personal AI on Digital Public Infrastructure	160
World ID Proof of Human (WorldCoin).....	161
UX For SSI Products	162
Primer on the CEDAR AUTHORIZATION POLICY LANGUAGE - What Why How.....	162
Did:btc1.....	163
OCA Render Method for Verifiable Credentials	163
SESSION #10	164

DCQL Part 2	164
Germany's Digital Identity History	166
How do we get to verifiable credentials in academia and government?	167
Packet Graph.....	169
Better Login for the Fediverse and the Social Web	170
Customer Commons + IEEE P7012 - by which sites and services agree to YOUR terms.....	173
Bridging Trust: DIDs + DNS + X.509	174
Sneaking SSI into the Music Industry - AMA with Switchchord	175
Should the Sustainable + Interoperable Digital Identity/SISI HUB and Open Wallet Foundation/Forum converge efforts?.....	175
Unintended Consequences of Digitizing Personal Data (the impacts of Dobbs)	176
Social Media/Web - Exciting Opportunities for Collaboration in the next 6-12 months.....	177
JSON-LD VC with BBS, OID4VCI, OID4VP, and Pseudonymous DID Key	181
Delegated Authorization with AI	185
Personal knowledge management & tolls for thought: 5C of knowledge management framework (an optimal method to learn metacognition)	187
Key recovery using secret location entropy comparison with seed phrase	187
Notes Day 3 / Thursday October 31 / Sessions 11 - 15.....	189
SESSION #11	189
Revocation/Status mechanisms Comparison	189
KERI as a Service health KERI's KaAs Platform	189
Decentralized reputation and social attestation	190
Expanding ACA-Py support for DID Methods using DIF's DID Registrar Drivers.....	193
DOCUMENTARY Film - the Legacy of the Identity Industry - open idea brainstorm.....	195
Policy As Code - The practical magic of Authorization development.	196
HomeAssistant as an example for Identity.....	200
GOV'T GO FAST Part 2: Challenges + Ways Forward.....	203
SESSION #12	220
RP Auth & EUDIW Part 2	220
The 7 Privacies or How our misconception of Privacy Preserving Tech prevents a full solution. - Ugly Baby Pagent.....	223
A gentle CRDIs into to (the foundation of local-first SW)	223
Data Coops with JLINC.....	224
Exploring Remarkable Regenerative Patterns of IETF: What do its governance practices have to teach us for our ID communities protocol work.	224
Identity in Telecom 101: STIR/SHAKEN, Rich Call Data & Authenticated Communications	225
Self-Describing DID Methods - OR - Decentralizing DID Method Names.....	229
Cloud Wallet Architecture - come discuss	230
How we lose the Attention Wars?.....	230
Election / Voting System Using VCs - Let's Build One!	230
Payments & Identity: Past, Present & their increasingly linked future	230
GOV'T GO FAST Part 2: Challenges + Ways Forward.....	231
SESSION #13	232
Digital Credentials API: Updates & Demos.....	232
KERI Security II - AI Safety Verifiable Agents.....	232
OpenID Federation 2.0.....	233
OAuth Scopes vs Dynamic Authorization - Why can't we just get along??	235
KYC, PASSKEYS & SECURING Customer data with Trinsic.....	236
Personal AI (not personalized AI from giant services).....	236
5 Alternatives to WorldID/Worldcoin.....	237

Auth Z 201 - Current developments & new ideas for policy decent IAM.com	241
Copy Protected credentials in Decentralized Environment using Hardware Security Modules	241
Brainstorming Organizational Identity for Digital ADS Industry.....	242
Discussion started with ad network structure.....	242
Did:btc1 Deep Dive.....	243
Dazzle Update - Getting back personal data, Fediverse, what?.....	244
Session #14	245
OIDC4 VCI Browser API Issuance Profile / OIDC4 VC presentation during issuance	245
Consumer/Service interaction in Travel is a Mesh, not a Supply Chain	246
How do we all run engineering & product teams in ID companies? Swap advice and stories on what works (“do we hate agile”), etc.....	246
The HumanOS Stack - How You Evolved Your Digital Identity	247
Trust Registries 101	250
It’s 2025, how do I set up a Digital Notary? (for a known authority)	254
SESSION #15	255
OID4VC Credential versions (updates) and DQCL Purpose	255
Revocation/Status mechanisms for ZKP.....	255
Trust DID Web (did:tdw) – Status and Demo.....	256
COLAPSE (& ID?) a conversation	257
Social Web _ Indie auth + FedCM PART 2	258
Use Cases & Business Models	258
Looking for the Use Cases for Issuer-Hiding VC	259
Security and Privacy Standards for Biometrics. Trends, challenges and opportunities for digital ID & SSI	260
Breaking free from Issuers. You can be the “Issuer” of your data-path to TRUE SSI. ZKTLS	260
Travel + SSI Mesh Not Supply CHN	261
Credential Schemas for Age Verification and Estimation - Working Session	261
Concept Mapping Techniques.....	262
#IIWRunners Club Run	264
Demo Hour / Wednesday October 30 th	265
Diversity and Inclusion Scholarships	270
Thank You to our Women’s Breakfast Sponsor Curity	271
Event Photos taken by Doc Searls.....	272
Stay Connected with the Community Over Time - Blog Posts from Community Members	274
Upcoming IIW Inspired™ Regionally Focused OpenSpace unConference Events	275
Identity ‘Funnies’ (comic strips) Shared by Alan Carp!	276
Password Magic	276
Phishing Badge.....	276
Hope to See you April 8,9 & 10, 2025 for IIWXL	277

The Book of Proceedings Helps with FOMO

 **James Monaghan** ID+ 🌱 + 🗣️ @james_monaghan · Oct 29 ...
I have considerable FOMO over the amazing conversations that will happen this week at @idworkshop #IIW, but Halloween is sacred in our family, so I'm going to be following along remotely instead! 🍁🎃📱📺



Sir Trust-A-Lot & The Shield of Digital Identity win best Halloween Costume!

 **Yuriy Ackermann** · 2nd + Follow ...
#Passkey #Product #AI #FIDO #Authentication #Securi...
2w · Edited · 🔄

Top halloween costume at #IIW

A collage of three photographs showing a person in a costume. The main photo shows a man in an orange long-sleeved shirt, brown pants, and a black helmet with a white visor. He is holding a large, round, gold-colored shield with a white label that reads "The Shield of Digital Identity". He is standing in a large, well-lit indoor space, likely a conference hall, with other people in the background. Two smaller photos are on the right: the top one shows a close-up of the shield being held, and the bottom one shows the person from behind, wearing a grey backpack.

About IIW

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

It has been one of the most effective venues for promoting and developing Web-site independent identity systems like OpenID, OAuth, and Information Cards. Past IIW events have proven to be an effective tool for building community in the Internet identity space as well as to get actual work accomplished.

The event has a unique format - the agenda is created live each day of the event. This allows for the discussion of key issues, projects and a lot of interactive opportunities with key industry leaders that are in step with this fast-paced arena.

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

The event is now in its 19th year and is Co-produced by Phil Windley, Heidi Nobantu Saul and Kaliya Young. IIWXL (#40) is April 8- 10, 2025.



Next Event is IIWXL #40
April 8, 9, 10, 2025

<https://internetidentityworkshop.com/>



Phil Windley ✓

@windley



We held the 39th edition of Internet Identity Workshop last week. Like always, it was a great week. » Internet Identity Workshop XXXIX Report windley.com/archives/2024/...



Last edited 8:13 AM · Nov 8, 2024 · **132** Views

https://www.windley.com/archives/2024/11/internet_identity_workshop_xxxix_report.shtml



IIW is powered by Open Space Technology and the magic Self Organizing and has been since 2007!

Thank You to Our Sponsors!

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



IIWXXXIX Daily Schedule

IIWXXXIX 3 Day Schedule

TUESDAY, October 29 / Doors Open at 8:00 AM for Registration Barista! - Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme Donuts - Fruit - String Cheese etc.				
Barista! And Continental Breakfast	8:00 - 9:00		Lunch	1:00 - 2:00
Welcome Introduction	9:00 - 10:00		Session 3	2:00 - 3:00
Opening Circle / Agenda Creation	10:00 - 11:00		Session 4	3:00 - 4:00
Session 1	11:00 - 12:00		Session 5	4:00 - 5:00
Session 2	12:00 - 1:00		Closing Circle	5:00 - 5:45
Welcome Reception & Dinner 6:00 Off the Rails Brewery 111 S Murphy Avenue Sunnyvale, CA 94086 (408) 773-9500				

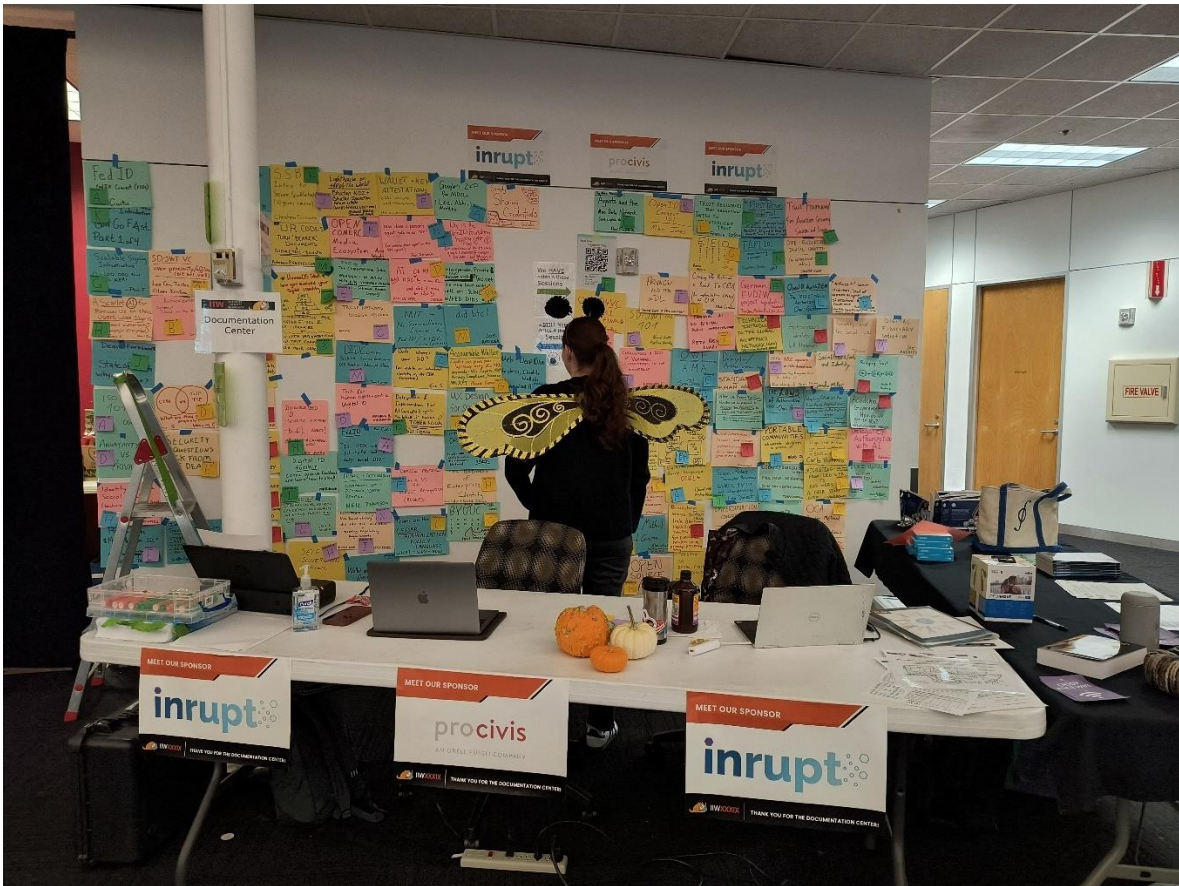
WEDNESDAY, October 30 / Doors Open at 8:00 Barista! - Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme Donuts - Fruit - String Cheese etc.				
IIW Women's Breakfast Roundtable's	7:45 - 9:00		Lunch	12:30 - 1:30
Opening Circle / Agenda Creation (SHARP)	8:45 - 9:30		Speed Demo Hour	1:30 - 2:30
Session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

THURSDAY, October 31 / Doors Open at 8:00
You're invited to Celebrate IIW Halloween "Costume Light"
 Those who are so moved can wear a special dress up item of any kind
 A funny hat, bloomers, clown nose, wig, cape, or something Identity Themed :-)

Barista! - Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme Donuts - Fruit - String Cheese 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	IIWXL APRIL 8 - 10, 2025	

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



IIW39 Agenda Creation = Schedule & Workshop Sessions



176 sessions were called and convened over 3 Days.

We received notes, slide decks, links to presentations and photos of whiteboard work for 135 of these sessions.

Tuesday October 29, 2024 Day 1 / Sessions 1 - 5

Session 1

1A/ Fed ID Connect (FIDC) / Ben Curtis

1B/ IIW 101 Session - Oauth 101 / Aaron Parecki

1C/ The Mee Foundation | Agents and the Mee Data Network (a quick demo) / Paul Trevithick

1D/ NO SESSION

1E/ Help Us Design a Progressive Trust Registry / Jim Goodell, Phil Long, Golda Velez, Dmitri Z

1F/ OpenID4VC 101 We're going FINAL / Kristina Yasuda, Joseph, Torsten Lodderstedt

1G/ Scalable Signing Infrastructure - 100,000 txns with KERI / Phil Feariheller.

1H/ A Scarlet AI for Browser UX to show users where slop is / Ross K. Rohit Khare

1G/ How MOSIP Identity is used by 2+ Billion people inclusively, across 30+ countries / Sasikumar Resham

1I/ Verifiable ID with the State of Utah - Why are we different? / Denise Farnsworth

1J/ GGF: Introduction Govt Go FAST Part 1 of 4? Troy Samuels

1K/ KILLER Credential Network Effect - an introduction to the Global Acceptance Network (GAN) / Drummod Reed, Andre Kudra and more

1L/ NO SESSION

1M/ FEDCOM, Digital Credentials & Webauthn - Future of Social Login / Heather Flanagan.

1N/ NO SESSION

Session 2

- 2A/ ISO mdoc 101 / Oliver and Andrew
- 2B/ IIW 101 Session - Open ID Connect 101 / Mike Jones
- 2C/ Social Media Web and Identity / Brenden Miller & Johannes
- 2D/ Anonymity vs Privacy / Ken Griggs
- 2E/ How to Make \$Money\$ from SSI? / Harrison Tang
- 2F/ Privacy and the mDL / Timothy Ruff & Phil Windley
- 2G/ SD - JWT (vc) 101 / Daniel F and Kristina Yasuda
- 2H/ Sync is not Send / Aaron D Goldman
- 2I/ VLEI Update - Verifiable Legal Entity Identifier - GLEIF / Karla McKenna
- 2J/ NO SESSION
- 2K/ NO SESSION
- 2L/ Has our SSI Ecosystem become Morally Bankrupt? / Christopher Allen
- 2M/ Digital Fiduciary Initiative / Joe Andrieu
- 2N/ Challenges & ROI of Verifiable Credentials in Enterprise / Heather Flanagan.

Session 3

- 3A/ SD-JWT VC over proximity/offline / Lee, Cam, Torsten, John, Oliver, Kristina Yasuda
- 3B/ IIW 101 Session - Authorization 101 Intro/Tutorial on the AM in IAM / Steve Venema
- 3C/ OCA Schemas - If you liked it then you should have put a SAID on it. / Carly Huitema
- 3D/ C2PA vs TOIP TSP - What are they good for anyway? / Wenjing Chu, Eric S
- 3E/ Security Questions - BACK FROM the DEAD / Matt Vogel
- 3F/ Trust Registries Trust Resolution - Intro to Decentralized Trust / Fabrice Rochette
- 3G/ EIEIO = Embracing Interop in Enterprise Identity Online / Aaron Parecki
- 3H/Crossing the Rubicon a Road to CESR (An implementation sketch of CESR) / Charles Lanahan
- 3I/ Personal AI on Digital Public Infrastructure / Resa Rassool - KWAAI
- 3J/ UBB Universal Basic Bandwidth / Christian Tschudin
- 3K/ CBOR DID & VC Controller Documents, Implementing Elision Privacy with Gordian Envelope / Christopher Allen
- 3L/Migrating from DID:WEB to DID:WEBS A case study GLEIF SWITCHBOARD / Cole Davis, Lance Byrd, Jona T
- 3M/ DID Method Squid Game / Alex w/Cheqd, Markus w/Danube Tech, Kim w/DIF
- 3N/ NO SESSION
- 3O/ NO SESSION

Session 4

- 4A/ Digital Credentials Query Language DCQL / David F, Kristina Yasuda
- 4B/ IIW 101 Session - Passkeys 101 AKA FIDO / John Bradley
- 4C/ OWF (Open Wallet Foundation) AMA / Sean Bohan
- 4D/ NO SESSION
- 4E/ NO SESSION
- 4F/ Consumer Reports AI Agent - discussion - - - > / Dazza Greenwood, Ben M, Ginny F
- 4G/ NO SESSION
- 4H/ Come Build Your Identity Project With DIF (Decentralized Identity Foundation) LABS / Ankur Banerjee, Kim HD, Andor
- 4I/ Regulation Identity & Privacy - Why you need to care! / Linda Jeng

4J/ NO SESSION

4K/ NO SESSION

4L/ Open ID AuthZEN - The “OIDC” of Authorization / Omri Gazitt

4M/ Credential Schema Standards: KYC and Proof of Personhood / Otto and Kim w/DIF

4N/ NO SESSION

4O/ NO SESSION

Session 5

5A/ KERI Security Duplicity Evident Data Provenance + AI Safety / Sam Smith

5B/ IIW 101 Session - Intro to Self Sovereign Identity / Limari and Steve

5C/ Zero Trust w/ Zero Data (verifiable creds) / Phil Windley

5D/ Autonomous Worlds / Will Abramson

5C/ Brainstorm way to link de-identified health data for population health in a privacy-preserving way. / Alan Viars

5E/ Delegation / Authorization for consumer-driven AI agents/Dazza G Standards for Human Agency/ Adrian Gropper

5F/ While we Block the Bots, how are we supposed to Allow the Agents to login and “do” stuff with AI / Rohit Khare

5G/ Intro to Trust Over IP (ToIP) / Judith Fleenor

5H/ Web Authn + EUDI RP Authentication / Torsten Lodderstedt

5I/ Technical Introduction to the Global Acceptance Network (Gan) / Drummond Reed, Andor, Dave

5J/ Identity Practitioner Pipeline - a conversation with DIAF, IDPro, OpenID... and you :-) about bringing New People into identity. Heather Flanagan , Erick D. Elizabeth G.

5K/ NO SESSION

5L/ NO SESSION

5M/ Edge Identifiers, Cliques, and other Opportunities of Multi-Party Computation (MPC) & ZKP / Christopher Allen

5N/ NO SESSION

5O/ NO SESSION

Wednesday October 30, 2024 Day 2 / Sessions 6 - 10

Session 6

6A/ German EUDIW Project Updates / Daniel F, Torsten L, Karko, Paul, Kristina

6B/ An Abstraction for “Pluggable” VC’s & ZKP Libraries - Now with implementation and test framework. / Mark Moir Oracle Labs

6C/ Trust Frameworks for Aviation Security / Savita and Lumy

6D/ Delegation & Impersonation for AI (and other) agents “on Behalf of” Human Users.... Token Focus / Paul Figura

6E/ NO SESSION

6F/ State - Endorsed Digital Identity (an alternative to the MDL) / Timothy Ruff

6G/ HumanOS Stack * How you evolved your Digital Identity / Jeff Orgle

6H/ Decentralized ID - Selective Disclosures - BLE! WORKS! - eID -Me = A Canadian View / Steve Borza

6I/ Digital toolkit: come give us feedback and learn how to play! / Marianne Diaz-Hernandez

6J/ Scopes - Roles - Granular Permissions USABILITY and interoperability / Lisa Dusseault

Impersonation Considered Harmful / Rohit Khare

6K/ SSB Intro to Secure Scuttlebutt (10+ years and more) / Christian Tschudin

6L/ The First Person Credential - Solving proff-of-personhood with verifiable credentials and GAN / Drummond Reed, Brad D, Andre Kudra, Dave P, Andor Khare,
6M/ UR CODES Turn “BEARER” Documents -> Biometric-Bound / Andrew Hughes
6N/ FAPT 101 #openbanking #opendata / Nat Sakimura, Daniel, Joseph
6O/ NO SESSION

Session 7

7A/ FedID “If OIDC and Activity Pub had a baby named DID” / Ben Curtis
7B/ The LAWS of Authorization (102) / Omri Gazitt
7C/ Trust Network Design Session / Andor Kesselman
7D/ Tech for human rights-centric Digital ID / Mariana & Marianne Diaz-Hernandez
7E/ INJI => The credentialing Stack. OpenID4 VCI in Action with W3C JSONLD Verifiable Credentials / Sasikumar, Resham Chugani (MOSIP)
7F/ Wallet + Key Attestations EIDAS WIA/WTE / Paul & Christian
7G/ DEMO: BBS Signature on FIDO Authenticator / Ken Watanabe & Shigeo Misuro
7H/ Self Sovereign Hardware / Gave Cohen, Daniel B
7I/ Let’s talk long-term non-repudiating in did:tdw and did:webs - meeting regulatory requirements/ Victor Dods
7J/ Lighthouse on Top of the World: Bhutan NDI + Bhutan Innovation Forum Update / Michael Becker, Drummond Reed
7K/ OPEN Commercial Media Ecosystem / Andy Woodruff
7L/ DISCUSSION - Streamlining vendor efficiency and quality at scale across KYC, KYB / Isha Bhatnagar, Mike Pellin
7M/ DIDComm Quick 101 - Formal Verification - DID Rotation - Advanced Flows / Sam Curren
7N/ Travel and Accessibility - Component of a Personal Data Profile / Neil Thomson
7O/ NO SESSION

Session 8

8A/ Google’s ZKP for MDOCs / Lee, Abhi, Matteo
8B/ Wallet and Agent Overview @ OWF / Mirko
8C/ Dude, where’s your DID? (an update on individual identity in the C2PA ecosystem) / Eric S
8D/ “Verifiable AI”: Content credentials, “proof of approved AI agent”, proof of personhood... and much more / Ankur Banerjee, Kim H-D, Steve McCown, Linda J, Wayne Chang
8E/ Portable AI Personalization - Brainstorm / Jim Goodell + Neil Thomson
8F/ Device Profile as a VC for Device Recognition / Rudra Pandra
8G/ IDENTITY BROKERS in OAuth Facilitator... but at what cost? Do we have better solutions? / Tommaso Innocenti
8H/ Identity on the Social Web (technical /product/UX) / Johannes Ernst
8I/ Why is the OpenID Foundation hopping right now? An overview of the 14 work groups and community groups on now. / Nat Sakimura + Gail Hodges
8J/ DWeb Deep Dive and Web 5 / OWN Updates + Wallet / Daniel B and Liran Cohen
8K/ PORTABLE COMMUNITIES interoperable identifiers in service of / Brad Degraf
8L/ Adopting OAuth2.0 for First-Party Applications - Building the Authentication Layer / Janak Amarasena
8M/ STA mDL Jumpstart RP-Adoption / Carolyn Sorensen + Tony Loprieto
8N/ How does a person’s agent talk to an RP / Paul Trivithick
8O/ NO SESSION

Session 9

9A/ RP Authentication & Authorization (EUDIW) / Torsten Lodderstedt, Giuseppe, Dima
9B/ Interoperable, Private and Feature-rich?! Tru.net The new town center built on JLINC w/Fed DID's / Jim Fournier, Ben Carson, Tonia Abdul & Simply Sharing Credentials / Golda Velez
9C/ BYOC - Bring Your Own Use Cases - Whatever! Real or Imaginary / Seth Kwon
9D/ AI - Oh My! RAG 101 / Alec Oliver
9E/Intro to ORIGINATOR PROFILE / Shigeya Suzuki
9F/ OPEN SOURCE AI / Sam Johnston
9G/ Accountable Wallet - A wallet can prove your legitimacy using VC's ZKP's / Masato Yaman
9H/ The Business of Enterprise Identity / Sam Etter & Rebekah Johnson
9I/ Personal AI on Digital Public Infrastructure / Reza Rassool (KWAAL)
9J/ WorldCoin - How to take orbs and World ID, ID Credentials to Provide a Private SSI for the Internet / Adrean, Tawanda, Ajay Patel
9K/ UX Design for SSI Products / Janet Gonzales
9L/ Primer on the CEDAR AUTHORIZATION POLICY LANGUAGE - What Why How
9M/ Did:btc1 / Joe Andrieu
9N/ OCA Render Method for VC / Patrick St-Louis
9O/ NO SESSION

Session 10

10A/ DCQL Part 2 / Daniel Fett
10B/ Germany's digital Identity History / Mirko Mollik
10C/ Academia Government: How do we get to VC's? Nicole Roy, Giuseppe De Marco, Stefan Listrom
10D/ Packet Graph - Identity and Other Qualities Embedded in Node-and-Edge Graphs. / Joe Rasmussen
10E/ Better Login for the Fediverse and the Social Web / Aaron Parecki
10F/ Customer Commons + IEEE P7012 - by which sites and services agree to YOUR terms / Iain Hendersen + Doc Searles
10G/ Bridging Trust DNS <-> DIDs <-> X509 / Andre Kudra, Markus Sabadello
10H/ Sneaking SSI into the Music Industry - AMA Switchchord / Cole Davis
10I/Should the Sustainable + Interoperable Digital Identity/SISI HUB and Open Wallet Foundation/Forum converge efforts? / Daniel Goldsneider, Gail Hodges, Elizabeth Garber
10J/ Unintended Consequences of Digitizing Personal Data / Karen Studders
10K/ Social Media/web Exciting Opportunities for Collaboration in the next 6 - 12 months! Brendon Miller
10L/ DEMO - JSON-LD BBS VC with OID4VCI & VP and Pseudonymous did:key / Dan Yamamoto
10M/ Delegated Authorization with AI / Adrian Gropper
10N/ Personal knowledge management & tolls for thought: 5C of knowledge management framework (an optimal method to learn metacognition / Michael Becker
10O/ Key recovery using secret location entropy comparison with seed phrase / Matt Vogel

Thursday October 31, 2024 Day 3 / Sessions 11 - 15

Session 11

11A/ Revocation / Status Mechanisms / Paul B + Mirko Mollik
11B/ KERI as a Service health KERI's KaAs Platform / Phil Fearheller
11C/ Towards decentralized reputation + social attestations protocols + draft standards - Envisioning next steps / Brenden Miller
11D/ NO SESSION
11E/ NO SESSION

11F/ EXPANDING ACAPy support for DID methods using DIF's DID Registrar drivers / Ankur Banerjee + Marcus Sabadello
11G/ DOCUMENTARY Film - the Legacy of the Identity Industry - open idea brainstorm / Oliver Mellan
11H/ Policy As Code - The practical magic of Authorization development. / Gert Draper
11I/ NO SESSION
11J/ NO SESSION
11K/ NO SESSION
11L/ What can Digital Identity learn from Home Assistant? / Sam Curren
11M/ GOV'T GO FAST Part 2: Challenges + Ways Forward / Troy Samuels
11N/ NO SESSION
11O/ NO SESSION

Session 12

12A/ RP Auth & EUDIW Part 2 / Torsten Lodderstedt
12B/ The 7 Privacies or How our misconception of Privacy Preserving Tech prevents a full solution. - Ugly Baby Pagent / Sam Smith
12C/ A gentle CRDIs into to (the foundation of local-first SW) / Christian Tschudin
12D/ Data Coops with JLINC / Brad deGraf + Jim Fournier
12E/ NO SESSION
12F/ Exploring Remarkable Regenerative Patterns of IETF: What do its governance practices have to teach us for our ID communities protocol work. Kaliya Young
12G/ Identity in Telecom 101 / Pierce Gorman
12H/ Self - Describing DID Methods OR Decentralizing DID Method Names / Kevin Dean
12I/ Cloud Wallet Architecture - come discuss / Patrick St. Louis
12J/ How we lose the Attention Wars? / Aaron Goldman
12K/ Election / Voting System Using VCs - Let's Build One! / Matt Vogel
12L/ Payments & Identity: Past, Present & their increasingly linked future / Tony Lopreinto
12M/ Gov't Go Fast Part 3: The End Game / Troy Samuels
12N/ NO SESSION
12O/ NO SESSION

Session 13

13A/ Digital Credentials API - updates and demos / Tim Capalli/ Lee Cam / Helen
13B/ KERI Security II - AI Safety Verifiable Agents / Sam Smith
13C/ OPEN ID Federation 2.0 / Dima Postnikov, Alex T
13D/ OAuth Scopes vs Dynamic Authorization - Why can't we just get along?? / Omri Gazitt
13E/ KYC, PASSKEYS & SECURING Customer data with Trinsic / Michael Boyd & Mahesh Balan
13F/ Personal AI - Not personalized AI as a service / Doc Searles
13G/ 5 Alternatives to WorldID/Worldcoin - Come help make the list / tell a better story / Kaliya Young
13H/ Auth Z 201 - Current developments & new ideas for policy decent IAM.com / Rohit Khare
13I/ Copy Protected credentials in Decentralized Environment using Hardware Security Modules / Andre Roder
13J/ NO SESSION
13K/ NO SESSION
13L/ Brainstorming Organizational Identity for Digital ADS Industry / Vinod Panicker - Amazon and Per BJORKE - Google
13M/ Did:btc1 Deep Dive / Will Abramson
13N/ Dazzle Update - Getting back personal data, Fediverse.... What? / Johannes Ernst

Session 14

- 14A/ OIDC4 VCI Browser API Issuance Profile / Joseph, Kristina, Sam & OIDC4 VC presentation during issuance / Sam we need you + Mirko
- 14B/ NO SESSION
- 14C/ Travel + SSI MESH Not Supply CHN / Neil Thomson
- 14D/ NO SESSION
- 14E/ How do we all run engineering & product teams in ID companies? Swap advice and stories on what works (“do we hate agile”) / Ankur Banerje
- 14F/ NO SESSION
- 14G/ HumanOS Stack - How you evolve your digital identity / Jeff O
- 14H/ NO SESSION
- 14I/ Trust Registries 101 / Dmitri Z & VC Longevity & End of Life Planning / Dmitri, James, Alex
- 14J/ NO SESSION
- 14K/ NO SESSION
- 14L/ NO SESSION
- 14M/ It’s 2025, how do I set up a Digital Notary? (for a known authority) / Adrian Gropper
- 14N/ NO SESSION
- 14O/ NO SESSION

Session 15

- 15A/ OID4VC Credential versions (updates) and DQCL Purpose / Oliver and Daniel
- 15B/ Revoke for ZKPs (new proposal) / Christian +Paul
- 15C/ Trusted DID web did:tdw Status and Demo / Stephen Curran + Patrick St. Louis
- 15D/ COLAPSE (& ID?) a conversation / Kaliya Y
- 15E/ Social Web _ Indie auth + FedCM PART 2 / Sam and Aaron & Bring your blog|DNS and leave with an Indie Web Auth and FedCM server
- 15F/ Use Cases & Business Models / Timothy Ruff
- 15G/ Looking for the Use Cases for Issuer-Hiding VC / Shigeo Mizuno & Ken W.
- 15H/ Selective disclosure function for existing certificates using ZKP / Ken N & Security & Privacy standards for Biometrics - Trends Challenges Opportunities / Julian Bringer
- 15I/ Breaking free from Issuers. You can be the “Issuer” of your data-path to TRUE SSI. ZKTLS /Subhash
- 15J/ NO SESSION
- 15K/ NO SESSION
- 15K/ Travel + SSI Mesh Not Supply CHN / Neil Thomson
- 15M/ Credential Schemas for Age Verification and Estimation Working Session ? Otto
- 15N/ Concept Mapping / Andrew Hughes
- 15O/ NO SESSION



Digital Identity Advancement Foundation

710 followers

2w • 🌐



We are at the [Internet Identity Workshop](#) and can't wait to talk to you about creative ways to grow the identity practitioner talent pipeline! Stop by "Room" J Session 5!



You and 28 others

1 repost

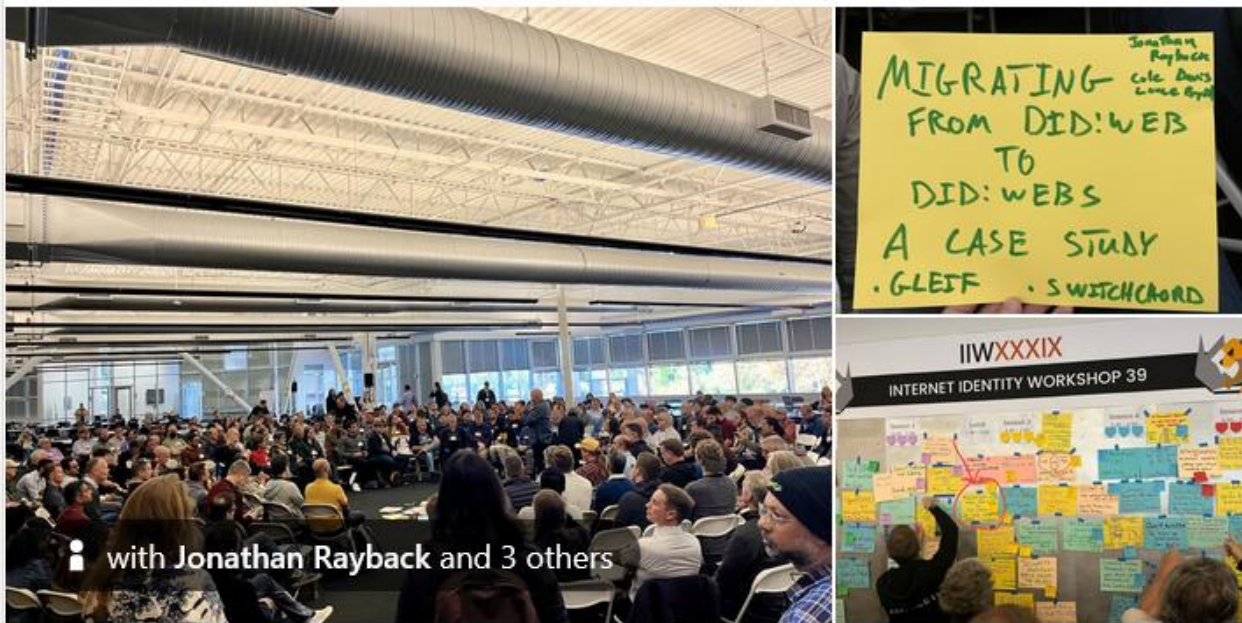




Cole Davis • 2nd
 Musician | Banker | Lawyer | Technologist
[Visit my website](#)
 2w • Edited • 🌐



Opening circle at the [Internet Identity Workshop](#). I've been participating in these virtually or in person for 4 years and today I'm calling my first session! [Global Legal Entity Identifier Foundation \(GLEIF\)](#) and [Switchchord](#) will be unveiling a very cool project we've been working on quietly in the background. For technical readers, we've blended the worlds of KERI key management + ACDCs with W3C DIDs and VCs within the music industry 🧐🎸 This enables secure organizational identity through vLEIs for music publishers and record labels, and bolsters our other identity verification workflows for songwriters and recording artists.



with Jonathan Rayback and 3 others

You and 58 others

3 comments · [2 reposts](#)

Notes Day 1 / Tuesday October 29 / Sessions 1 - 5

SESSION #1

FedID / FIDC

Session Convener: Ben Curtis

Session Notes Taker(s): Jim Fournier

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

<https://fedid.me>

<https://www.jlinc.com>

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

An online representation of you, that you own and control.

FedID is the root technology behind FedID Connect (FIDC), which leverages the portability of OpenID Connect (OIDC) and distribution of ActivityPub to provide usernames and identifiers that individuals own and control, no matter what happens to the site they signed up on.

We took attendees through the creation of a FedID on a mobile device, and its use to login to an existing tool that already supports OIDC, and thus, FIDC.

Available as of the first day of IIW:

- Detailed documentation, DID format, and protocol overview: <https://fedid.me/about>
- Flutter library: <https://fedid.me/libraries/flutter>
- Containerized server infrastructure: <https://fedid.me/server>

We have released the FedID DID server / DID resolver under an MIT + no surveillance licence

OAuth 101 - IIW 101 Session

Session Convener: Aaron Parecki

Session Notes Taker(s): Brandon Mott

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

There are a lot of specs and extensions to OAuth.

The original reason OAuth was created was to stop the Anti-Password pattern.

How do you revoke this app's access to your password?

Do you trust the app to not store your password?

Do you trust the app to access only the things it says it needs.

How do we let apps access data without sharing the password?

Similar to going to the hotel to share your ID card.

Limited access that is timed (expires)

Using a token that represents the identity instead of giving the password.

The consent screen is fundamental to the design.

- The pattern is the third party wants to access your data, do you want to allow it?

Twitter talking to Twitter is first-party access, so there is no trust issue here.

There's no easy way to tell if you're logging into the authorized site.

How do you know the identity when the website is real? Are you using a real Apple login?

Some MFA are better than others.

Some MFA are Phishable.

Google using accounts.google.com enables good MFA - they don't have to use multiple sites

Another reason OAuth is useful to let apps access data.

Like the hotel door. The keycard doesn't care who you are.

OAuth doesn't tell the app who is logged in.

Question: Is there anything that in OAuth that can tell you if you were logged in before?

Correct, Example, if the app is trying to upload a file to Google, it doesn't care who is logged in. It only wants to know if the app can perform the action. There's nothing about the OAuth flow that tells you who is logged in.

Open ID Connect standardized the pattern to tell the application about the user.

Access token - Like a hotel key. The app doesn't care about what's in the token.

ID Token - receipt (statement of what happened). For when your app cares about who they are.

Who is the audience? Who is meant to read the token? The API

Question: So the access token is meant to be tunneled through the App to the and passed to the API? You can think of it like that.

Question: So the app is going to request ID token? The ID token is meant to be read by the App.

Is there a principal to only share the minimal amount of data possible? Yes, we want to use data minimization.

Generally, you should design this to have ???

Question: Is it not a best practice to use token to the associate the subject to a User? Yes, that's how the ID token is used.

There's a difference between pure OAuth and Single Sign On.

Question: Would you then want to use the access token to give permission to use an API? Typically, no. That information is going to live in the application itself.

The website that uses an OAuth service doesn't need to know who you are.

Question: In reality there are going to need an identifier, right? For that ideally you would use Open ID Connect.

There are different ways to obtain access tokens - The OAuth flows

- Authorization code flow is most common.
- Device is useful when there's no browser.
- Client Credentials is server to server.
- Password flow was originally useful for apps to collect passwords when use it to login - but is no longer used.
- Implicit flow has its use case but is not recommended.

The authorization code is a one-timed short lived code to is used to get the access token.

Question: If a third party sends an authorization code to the browser, is there opportunity to steal it? Yes, there's plenty of opportunity to steal the authorization code.

Because of this, we can use PKCE.

As the authorization server,

PKCE creates a link between front and back channel.

Question: No one (user agent) is interacting with the back channel? Correct.

The back channel is from client to server

The front channel is passing data via the browser's address bar.

The front channel is like sending something in the mail. How do you know it's getting delivered.

PKCE basically ensures whoever is using the authorization code is the same thing that requests it.

Question: By the same thing, what do you mean? The same user agent/application (session in the browser).

Question: Is it the app or the OAuth server creates a PKCE? It's the app. It generates a random string.

Question: The nonce in the OAuth Spec is the same as the PKCE? The nonce is different. It's not used in the token request. Instead the OAuth server adds it.

The app knows to check the ID token for the nonce. The app has to check it. The authorization server doesn't know if the attack happened.

Agents and the Mee Data Network

Session Convener: Paul Trevithick

Session Notes Taker(s): Ammar safdari

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

Personal data is the new oil - Mee.foundation “we are a nonprofit with a mission to develop a human centered user experience for the internet”

your data is stored in corporate silos - you don't have access to all of it at one time

Status Quo

- You can't control who has your data or how they'll use it
- Business treat your data as their property
- Data brokers buy and sell your data without your knowledge

We lack autonomy, agency, privacy, and convenience on the internet.

Mee data network (MDN)

A data network of compatible apps sites where the information held by them is controlled by your identity agent

- MDN puts you in control of your personal data wherever it lives
- MDN benefits — convenience of an agent having your information so it can enter for you on all websites, you can actually control your data (delete, access, edit) wherever it lives

itsmee.org — a decentralized identity agent. It is a mediator — it stores no personal data, only metadata. Your data is stored at N provider-hosted MDN nodes

MDN License

Mee authorized apps/sites — MDN license — Mee identity agent

UX

you don't need to login
personalization
brand reputation

Never repeat yourself on the web!

Compliance

guaranteed compliance with privacy regulations

Respects data subject rights

consent management — all data sharing events are logged to support audit

structure of MDN

MDN — manages your personal “self”, connects digital providers to your data

Willow layer — protocols for delegation and data sync

Iroh.computer layer — move the bytes

MDN relays your info through peer to peer protocols from Walmart to UsaToday

Related: Smart Data regulation in Britain / data use and access bill

Progressive Trust in Issuer Registries with LinkedClaims

Session Convener: Jim Goodell

Session Notes Taker(s): Golda Velez, others?

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

Core idea: [Progressive Trust Registry](#)

LinkedClaims: <https://github.com/Cooperation-org/LinkedClaims/blob/main/LinkedClaimsRFC.md>

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

- Progressive Trust using Linked Claims
- How can trust be built over time
- low bar, low friction
- Core idea: an issuer registry that anyone can join, and THEN build trust by adding claims pointing to them

*** A little bit better is better than nothing at all. ****

similar concept - Alex - Tweetdale

going up to a root of trust is broken - openid federation

allow to issue specific credential sets

what if someone got hacked, not go to single source of truth

wanted to add endorsements in trust registries

"I never heard of you but i see you were " - FOAF

what are issuer registries - look up key who it belongs to

traditional - do the kyc and filtering before you get on the registry

progressive - anyone can get on the list - free and meaningless - but can progressively add value

can start in a forum

phil - any given recommendation credential has the ability to have in it can have bona fides inside the credential, evidence can be included

jo speer - if you feel confident in the context - if you choose to accept it
power of the receiver to decide

yoshiro - gaps between trust and verifiability - trust-capable issuer

discoverability - Different types of registry may have different levels of requirements

the lightweight registry can point to the heavyweight one

how do we say what kind of thing it is

LinkedClaims are a decorator pattern across the vocabularies
an issuer registry may specify a vocabulary
and press for common vocabularies

EU - european blockchain .. has defined schemas, with minimum properties for accreditation
accreditations by schema - regulatory pressure ***

OCA schema language - terms in your schema to external concepts
allowing a term to match to multiple concepts - mapping under regulatory regimes

how do we prevent noise - ability to have layers who can choose whether to keep your claim
around or throw it out, whether to share or aggregate it

registries still need some centralized governance to make those decisions of bars and levels

what makes the quality of the trust registry actually usable

we need to be able to do this - what is it used for?

fraud - from academic publishing - prewrite academic paper and sell it - citing -

problem - people will buy into the other sources of trust - it will maybe pollute everything

levels the playing field - more inclusive to be listed on things -

where do you store it? how do you know its not tampered with

Jim: put it on github, each claim has essentially an inbox or reply-to
golda: they are signed blobs, can be hashed, addressed

phil - use case: rank specific departments in crappy institutions

stephen curran: - this is what business registries are!

what about aspect - what is the aspect of your reputation
within this org i know who to ask for

can make claims about dids **or** about claims

comment: this makes it a permissionless marketplace, democratizes trust

Core concept: the claims are just signal, the score or model is a rollup or aggregation that might
have different filters or rules or algorithms to decide how to evaluate them

The analysis, such as "trust scores", should not be baked into the registries or use hard coded
rules but separate external systems and contextualised because all evaluation of trust is valued in
context.

OpenID for Verifiable Presentations Editors' Draft

Session Convener: Kristina Yasuda, Torsten Lodderstedt, Joseph Heenan
Session Notes Taker(s): Nicole Roy, ...

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

[Editors' Draft](#)

[Slides](#)

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

Wallet selector API collab in browsers
ISO mDL stuff

Not going super deep into the protocol today, doing updates since last time

Trying to standardize VC issuance into wallets and VC presentation from wallets. Would like to just have to have one way to do that.

Mobile drivers' license: Developing OpenID4VC high assurance interoperability profile for mdoc is being developed in ISO.

Scalable Signing Infrastructure)- 100,000 txns with KERI

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

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

Type Here

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

NO NOTES SUBMITTED

A Scarlet AI for Browser UX to show users where slop is / Ross K. Rohit Khare

Session Convener: Ross K. and Rohit Khare

Session Notes Taker(s):

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

Good informative session. Deep Learning models integrated with AI will enhance the solution.

MOSIP Introduction - Imagining Digital Transformation Through DPI

Session Convener: Sasikumar Ganesan, Resham Chugani

Session Notes Taker(s): Resham Chugani

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

1. [MOSIP Introduction - Slides](#)
2. [MOSIP Documentation](#)
3. [MOSIP Website](#)
4. [MOSIP Community Forum](#)
5. [MOSIP Sandbox Collab Environment](#) - Try It Out Yourself
6. [MOSIP Collab Setup Guides](#)
7. [MOSIP YouTube](#)
8. [MOSIP Academy](#)
9. [MOSIP LinkedIn](#)

Note: Access to specific documents will be provided on request.

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

Session Description: How MOSIP Identity is used by 2+ billion people inclusively across 30+ countries globally

An introduction and detailed overview of MOSIP (**M**odular **O**pen **S**ource **I**ntity **P**latform) was provided. Questions were duly addressed.

MOSIP Open Source Identity Platform is ready for Integration and collaboration in The W3C ecosystem.

Verifiable ID with the State of Utah - Why are we different?

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

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

This session presented an introduction into how the US State of Utah introducing Verifiable Credentials as a state credential.

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

Presentation slides: <https://www.dropbox.com/scl/fi/qviptsz9zr93ikqglh3tw/FINAL-IIW-Verifiable-Cred-in-Utah-Deck-28-Oct-2024-JJ.pptx?rlkey=35e5hacee8ns93rod4c3hm362&st=wb0vlhdo&dl=0>

Government Go Fast: An introduction.

Session Convener: Tchaikawsky “Troy” Samuels
Session Notes Taker(s): Shannon

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

OpenID, MOSIP, NAPHSIS

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

The objective of this meeting was to get the groups thinking about what it would take to have a cradle to grave system that made getting access to services/credentials seamless. Doing so by limiting the amount of visits and paperwork needed by having a federated system communicate on a common standard to issue access to any service/resource with a single digital wallet.

National Association of Convenience

Don't need to be used outside of gov content (Erik)

-Create standards for vital records (state) NAPHSIS non-profit (connected with KG at ID Connect)

-share of an operational use case (not privacy and policy)

-use of drivers licence is to drive and to limit it to the one attribute instead of use for something else (Joyce)

- is the goal (vision) to create one identity (answer: it's a hub Troy) this biometric is the ideal instead of something else.
- biometrics are a user name not a password (unlock something) if a company collects it they have it as a use case to provide something to log in because they have it. They can provide it the same way to needed. In general, never useful to know who you are talking to...Ryan (live biometric are spoonful. It's okay to public they're not secrets. You are needing PKI, adding a device need to verify with another device.
- 50 million dollars stole with deep fake to steal money from the company
- Scott (a live biometric) HHS
- have a photo id and not be able in other situations (interoperability, standards) the goal is to be interoperable ; the federal, state, and vendor (laws, agendas) get layered on top of it). It doesn't mean its interoperable.
- federal register notice
- awareness of the use of the ID in the bar and was told I wasn't usable (was this in an approved state)?
- will push back to see if what we need in the use of credentials is convenience (ERIK /schun)

This discussion would later lead to another session where the concept of a federated system, Similar to what Open ID and MOSIP has to offer. The discussion notes and data can be found in Session 1&2 on 10/31 in room M.

Killer Credential Network Effect: An Introduction to the Global Acceptance Network (GAN)

Session Convener: Drummond Reed, [Andor Kesselman](#), David Poltorak, Andre Kudra

Session Notes Taker(s): [Ankur Banerjee](#), Darius Dunlap

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

- [Personhood Credentials](#): Academic paper that was referenced
- [Global Acceptance Network \(GAN\) site](#)
- [Personhood: The Killer Credential](#): The blog post that was shown at the beginning of the session.

Technical details will be in Session 5, Room I.

Another session will cover personal credentials

Expect also a session about Bhutan's involvement in GAN.

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

Envisioning ICANN-like governance

- Passports, drivers licenses are trusted because there's governance and multiple issuers involved
- "GAN Common Employee Credential / Badge" is one of the first common credentials, since many people are employed
 - Dynamic access rights based on which companies are associated or vendors
- "GAN Customer" since almost everybody is a customer of something, proof that you were a customer of something
 - What if verifiers try overusing it? Customers might have 100s of these GAN customer credentials. Verifiers could go asking "show me X more credentials" so that they know more info about the customer or whom to collude with.
 - Can be controlled with governance
- Proof of address / Verifiable Address, Verified phone number
- Goal of GAN is not to create new standards or tech, focus on the business and governance questions
- Who are the [GAN members](#)?
- Does it cost money to join? Yes, but there are non-paying members for non-profits as well
- Analogy to Visa/MasterCard/DNS was made: will GAN have graceful degradation so that everything doesn't stop working like when Visa/DNS goes down?
 - Yes, these are the technical considerations driving lots of choices

Organizational Members

Platinum Members

accenture

FRAGOMEN

Gen

Gold Members

NTT Digital

P Pearson

Credivera

Silver Members



Ecosystem Members



Nonprofit Members



Additional notes: <https://ericscouten.dev/2024/iw39/#session-11-personhood-the-killer-credential-killer-credential-network-effects>

FedCM, Digital Credentials, and WebAuthn - future of consumer login

Session Convener: Heather Flanagan, Tim Cappalli, Sam Goto

Session Notes Taker(s): Heather Flanagan

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

FedCM: <https://www.w3.org/TR/fedcm-1/>

WebAuthn: <https://www.w3.org/TR/webauthn-3/>

Digital Credentials: <https://wicg.github.io/digital-credentials/>

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

For digital credentials, these are fairly new. Passkeys have been available for a bit longer. There are common patterns between them. The DCs and passkeys do one thing really well: that the user has hold of a key. Federated flows (e.g., OIDC) can add more detail than that, but it looks similar. The privacy properties, however, are very different.

In most deployments, OIDC is not as privacy-preserving because you're telling the IdP every time you're going to a site.

If you're using the same VC every time, it also allows interesting tracking mechanisms. You can handle this by batch issuance. There also Zero Knowledge Proofs as an option (eventually).

All three APIs are developed in the W3C, almost entirely with the same people. Why are we doing all three?

What do we actually want **consumer** login to look like?

- Two distinct ceremonies that we need to train people are actually different. Logging into their gym with their mDL is technically possible but not socially good. We should have reauthentication based on a pseudonymous credential with no attributes. Would like to restrict the use of VC expressing attributes to use cases where it's actually required (account creation, gov't use cases). Authentication or re-authentication should be a separate ceremony.

Should we create a passkey for every account creation? Some people say yes.

Do we want the gym to create a passkey, or do we want them to issue a membership card? There is attraction for issuing a branded passkey/a VC for themselves. There are UX reasons some RPs will gravitate to branded passkeys. But in the VC space, we may want to carve out room for self-issued credentials, maybe the UX will be different than what's issued by the RP.

It would be useful to have a bunch of buckets that say "these kinds of sites are in this category, others in that category." Do I want to have a 1:1 relationship with sites I log in to, or do I want to

have a social relationship with the sites I log into? There's no one answer to this. These aren't mutually exclusive.

Does there have to be only one answer re: the consumer use case? For the gym use case, you can give them a dongle they tap each time with no personal info, or you could give them something else. There are different trade-offs, for accomplishing different things. The ecosystem should not force one choice because the gym may have different goals.

- this would be an acceptable outcome, that these things should coexist with an addressable market for each API

What principles/intuition would websites use to choose whether to use a passkey or issue a VC?

One thing that's new: we're exploring physical to digital connection in ways we didn't have before.

In terms of buckets, some success in using the terms "closed loop" (self-issued statement for yourself, used for one organization) and "open loop" (issued and presented for everyone else).

- Finding terms that mean the same thing in the different worlds would also be super helpful. Open loop vs closed loop might also be referred to as first party and third party.

Zooming back out to think about the two different things, presenting a credential vs using a passkey. Membership cards might be red-herring; they aren't necessarily an authentication method. We don't need to use VCs for authentication; passkeys are fine for that. What identity credentials are good for is that during account creation, when I need to prove aspects about me, yes. But for authentication, it should be an anonymous credential that I can choose what entity I want to manage the credential for me (e.g., a password manager). The identification piece will be separate.

There is a grey area in between. People like VISA want to issue payment credentials that are only good at merchants that can do transaction authorization. So there may be a community where it's a student card that can only be presented for certain student things (library, dining hall). You'll limit the scope of identity transactions to the specific community. We don't really understand those use cases yet. But since we're focused on consumers right now.

If we are not careful, we're going to try and create a super credential to solve all use cases. (Bad Idea) We will need multiple APIs; we need to be careful they don't fill each other's ultimate purpose.

- being able to do a federated activity does offer a unique value; stuff that other mechanisms don't use

One of the challenges with this conversation is that you ask for all the information up front, even if you don't need it immediately. Explicitly separating it out is a better idea.

Separation between identification and authentication; verified autocomplete and hydration; are the words account creation and account recovery and login - do they all mean the same things? Is identification the same as account creation?

- largely the same thing, but account creation doesn't always require identification

- Social logins are largely self-asserted, even when the account creation requires verification of email and/or phone number. But this is still different than requiring a real-world identity credential. It's a difference between validating a verifier, not verifying an identity. It's pre-validation.
- Validation that a user can re-access an account

Chrome talks about root identities; they see these as always recoverable. But that's not always true. Example: Telco's may change your phone number.

Identifier is the best artifact of being. Data attributes, however, aren't generally owned by the individual. The being and data need to be separate. VC is a data model about the data. Identity verification is a process. Authentication is part of it. They need to be kept separate.

Another perspective, in eIDAS there are discussions about pseudonyms that can exist between login and account creation. The more privacy preserving approach is pseudonymity so that it can be tracked if absolutely necessary (via court).

One useful thing we're hearing: people from different industries have unique perspectives and different terms. Useful to get those out there. Commonalities between patterns and essential elements are really good to capture – and the edge cases that don't fit the pattern.

FedCM is more a medium to present different ways like OIDC and DC. Digital Credentials are useful during onboarding. OIDC doesn't offer a good way to onboard. Maybe users can plugin their digital credentials to FedCM. If the account creator needs that data, they can trust it from FedCM. Indication of LOA (level of assurance) is useful. Digital credentials are not that useful during authentication.

- There are use cases, esp. when finance/money is involved, where KYC is important as they collect info about users that informs what that user will be allowed to do with money.
- what about explicit ceremonies as separate from KYC processes? Digital credentials are verified; they are easier to use. Is the digital credential data something that would autofill, or would it be an explicit ceremony? Right now, autofill (but it could be separated).

We might not be using the term "pseudonyms" the same way. In some cases, it's something a person chooses. In other cases, it's something chosen for them that could be verified. Pairwise is another term; a verifier you don't control that's only viewable by the other party.

- European regulation vs what we mean in webauthn is different. WebAuthn is non-correlatable, non-recoverable thing created by the verifier. In the EU, it's a pairwise identifier created by the PID issuer that could be recovered and traced back to a unique identity. (But eIDAS interpretation is varied.)

Sites will use WebAuthn in different ways, in some cases for more detail (like a pre-populated CIAM system), in other cases it will be less. Part of FedCM looks similar to passkeys; relying on an upstream social network with similar policies will be helpful to them and solve some of their infrastructure needs. Other orgs will start there and shift to something more specialized to them.

From the POV from the SP, using federated identity will provide a lot of info to the platform you're building, esp. if your platform requires payments. You need a way to contact the user and that's not something that WebAuthn would offer by default. From the user perspective, I would prefer more privacy. What service the platform offers and whether that platform should provide info on that at the beginning is a question.

Talking about identification vs authentication, if I go to a website to buy liquor, I just want to know if of age. Maybe we call that identification?

In the PayPal case, you're trying to transfer money, and that's not identification or authentication.

Everyone here is trying to do different things and seeing this through different lenses; there are several different decisions you have to make about risk, context, the controls available, the relationships, and the purpose. It's not going to be an apples-to-apples conversation until we can compare those five dimensions.

Another use case: these use cases could apply to the fediverse. Finding your social website, trying to "like" it, it's the only thing I'd want to do there. Now I have to take my identifier and enter it into your website in order to do only that thing.

- FedCM is the only API we're talking about that can help with the discovery problem. Passkeys and VCs don't help in that context.
- "Liking" wouldn't be allowed by WebAuthn or passkeys.

Original use case of OIDC, Google and Apple helped for how to share things like use calendars to third-party sites, allowing the user to authenticate and choose what info to share. But now we have different tools and privacy requirements. VCs can't provision OAuth token for that kind of API sharing.

It would be nice to establish a better ceremony for the fediverse use case (see the Identity in the Social Web sessions coming next).

Regarding discovery, Digital Credentials need significant scoping in order to find the correct credential. FedCM allows a much broader capability for finding the identity provider. These capabilities may be able to be merged at some point, though for right now, FedCM does allow for solving a much bigger problem space. FedCM doesn't expect the information of what credentials are available to be stored locally.

SESSION #2

ISO mdoc 101

Session Convener: Oliver Terbu & Andrew Hughes

Session Notes Taker(s): See the slides

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

Gave an introduction to ISO 18013-5, ISO 18013-7 standards & fielded questions.

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

Slides for the session are here:

<https://www.slideshare.net/slideshow/iso-mdoc-101-session-presented-to-internet-identity-workshop-iiw-iiwxxxix/272919383>

Introduction to OpenID Connect / IIW 101 Session

Session Convener: Mike Jones

Session Notes Taker(s): Nicole Roy

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

Presentation posted at <https://self-issued.info/?p=2584>

OpenID Connect page <https://openid.net/connect>

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

- Intros from the group
- Result of the collab of a whole lot of people and organizations
- Identity layer on top of OAuth 2.0
- Enables RPs to verify identity of end-user, obtain basic profile info about you

Built using REST/JSON

Described at <https://openid.net/connect>

Almost certainly using it every day

OIDC is infrastructure, not a brand

Spans use cases/scenarios: internet, enterprise, mobile, cloud, federated, user-centric

Span security and privacy requirements from non-sensitive to highly secure

Spans sophistication of claims usage

Tries to maximize simplicity of implementation

Won lots of awards along the way

“Keep simple things simple”

- UserInfo endpoint for simple claims about user
- Designed to work well on mobile phones

“Make complex things possible”

How we made it simple

- Built on OAuth 2.0
- Uses JSON
- Lets you build only the pieces that you need

Goal: Easy implementation of all modern development platforms

Explicit decision: Do not do any canonicalization

Make complex things possible

- Encrypted claims
- Aggregated claims
- Distributed claims

Key diffs from OpenID 2.0

- Support for native client apps
- Identifiers using e-mail address format
- UserInfo endpoint for simple claims about user
- Designed to work well on phones
- Uses JSON, not XML
- Support for encryption and LoAs

“Artifact Binding” WG formed in March 2010. Closed many design issues at IIW in May 2011.

Branded “OpenID Connect”

Five rounds of interop testing (super critical to success) between 2011 and 2013

Final specs approved February 2014

Bunch of additional/related work since then

OpenID Connect specs published as ISO PAS specs, October 2024. (publicly-available specifications)

ID Token is the most foundational data structure in OIDC

- JSON Web Token (JWT) - signed claims representing logged-in session
 - Issuer
 - Subject
 - Audience
 - Issued at
 - Expires
 - Nonce

RPs can request claims using OAuth scopes:

- openid
- profile
- email
- address
- phone
- offline_access (requests refresh token issuance)

Requests for individual claims can be made using JSON “claims” request parameter

List of the userinfo claims goes here (lots of ‘em)

Examples of authorization request and response

Example of UserInfo request example

RP-initiated logout spec finalized as of September 2022

What does “logout” mean? The answer is: “It depends...”

OP-initiated logout:

- Session management
- Front-channel logout
- Back-channel logout

Finalized specs September 2022

Session management and front-channel logout are affected by recent browser privacy changes

Definition of “unmet_authentication_requirements” error code where the RP can cause an error to happen if the user’s login method does not meet RP’s requirements.

prompt=create spec allows account creation if an account doesn’t already exist

Tenth anniversary of OIDC this year

Lessons learned:

- Keep simple things simple
- Repeated interop testing and incorporating resulting feedback from developers
- Certification enables an ecosystem of interoperable implementations

More happening now than at any time since the original specs were created

Examples:

- OpenID Federation
- OpenID Federation Wallet Architectures
- OpenID for Verifiable Credential Issuance and Presentation (these are credential format agnostic)

Self-Issued OpenID Provider v2.0 "SIOP" - extends to use DIDs as subjects

Native SSO for mobile apps spec (became I-D in December 2022)

Second errata set published December 2023 - lots of these came out of the work to publish as ISO standards

Related working groups:

- MODRNA
- FAPI
- eKYC-IDA (final in October, 2024)
- DCP
- CIBA Core (final in September, 2021)

Certification program

3,753 certifications to date

Automated interop testing

Social Media/Web and Identity discussion

Session Convener: Brendan Miller and Alberto Leon, Applied Social Media Lab, Harvard University

Session Notes Taker(s): Brendan Miller, Darius Dunlap

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

Some framing questions:

- What humans are responsible for what content? How can we mitigate harms?
 - Manipulating public opinion using AI bots and paid influence campaigns
 - Harassment, bullying and and threats
- How can we protect appropriate levels of privacy in private, semi-private and pseudonymous environments?
 - Managing the “intimacy gradient”
- Can portable identity and data enable users to break out of existing “walled gardens” and empower them with new choices that better meet their needs?
- Is there value in separating the identity services from the content services?
 - Can this better align incentives and prevent abuses?

Other possible topics for discussion:

- Portable identity and data
- Levels of assurance vs privacy
- Data/content provenance
- Platform <-> User vs User <-> user verifications?
- Interoperability, open protocols and federation/decentralization
- Usable, forgiving identity (e.g. backup/restore)
- Reputation and person to person, relational credentials, social attestations
- Developing clarity on requirements: User segments, user stories

—

Reza: KwaaiNet kwaai.ai - Personal AI agent

Running at the edge

Joe Rasmussen: Wikipedia as a social media site. Complete openness and transparency, but allowing anonymous edits also. Like identity approach from our villages in the past. A reputation pool.

Denise Duncan: Project Liberty - Decentralised Social Networking Protocol (DSNP) backed by Frequency blockchain - portable identity to break out of walled gardens. Partner with MeWe. Creating an incentive program to make the move?

Dmitry Z: Co chair of W3C Social Web community group. Working on specs for better identity can enable portable data.

DIDs in social media? Bluesky is using DIDs

Draft specifications in Fediverse as well

Johannes: Many projects running in this space. Recommends introducing active projects

Ben: Creator of FedID (fedid.me) - OIDC integration with ActivityPub
Separating identity services from content services is an important challenge
Provenance of data

Lisa G____: multiple proposals for fediverse portability
identity is separate from data portability

Paul: Mee Foundation
Identity agent to manage information about you separate from content providers

Johannes: Collaborating with Kaliya on Fediform, Next one in March, online.
Also interested in interop, creator of a test suite, Feditest (<https://feditest.org/>)
ActivityPub vs Bluesky vs DSNP vs ??
How will they connect and interop?
ActivityPub was created exactly for that purpose
Cost of entry is high: how can it be reduced?

Jim Fenton: Digital editing guidelines
Pessimistic about separating identity providers from content providers. "All liability and no revenue?" What is a business model that does not require violating privacy.

Jeff: "When something very private goes very public" - Burning Man going online during the pandemic. Worked pretty well. Emulated a real world experience online.
Examples of identity vs content services in the real world?

Kaliya: Is the frame wrong? Do we need tools for humans to engage and work with real world communities online?
Next generation of social tools as next level of public infrastructure for neighbourhoods and communities?

Joseph: Coming out of web ashes: e-community. More natural based things. Organic communities where we can engage and coordinate.
Sick and tired of building identity systems: it is dumb. Need ability to have a global protocol for identity and don't have to build them anymore.
KERI fan: <https://keri.one/>

Tanya: TRUE- working on this exactly. Places to help people organize, make it easy.
Protect privacy while maintaining data provenance. Different needs are contextual.

Question: What can this convening/community do to contribute to social media/web?

Johannes: Many places for collaboration already exist
Do not build something new when it is not needed

Add more oomph to existing efforts

Kwaai - Doc is the Chief Intention Officer. His vision is what they are trying to build.

AI at edge, peer to peer, a new infrastructure

Practical issues are being solved through that challenge. Distributed AI. Petals, Hivemind, etc.

Solving problem of my data is private to me, keep it local, but don't have enough compute resources. Outsource compute over private data.

TrueInternet Inc: Hub networking structure built for orgs, small businesses. Start small then become interoperable.

Ben: What is the industry looking for? They want easy, not expensive.

Make it easy and beneficial for orgs with a lot of money can get behind

Reza - Sees it differently: Start with the problems of individuals instead. Trickle up.

Tania: Look beyond the capitalist model. Strength in numbers, generativity, communities.

D: Internet was not always based on gigantic silos. Does not have to be.

His Mom and him engage on history and would love to have some space to do it that's better than a stupid Facebook group. Empower individuals and groups.

Joseph: Protocols being us together. Not more silos.

Kaliya: Protocols for developing protocols - she has been studying this

Johannes: what problems can be solved? User personas in social networking. Lots of use cases how people use social media.

To connect, to organize. To be entertained, etc. To self promote.

Get clear about different personas and their needs.

A guideline how to use different social media, so don't have to use Twitter. Content branding guidelines share with the public.

Brandon: How the internet became popular. Top down constraints and bottom up emergence. Public, private, civil society collab and constraints.

Reza: Heavy on identity here. Sharing knowledge. Instead of centralized silos. Need a distributed architecture. Public and private knowledge. Different groups of collective knowledge. Worth exploring those structures?

Look at enable technologies that enable richer forms of sharing.

Joseph: Nostr protocol also

Johannes: Who uses what social media here

- Established platforms? Most people

- Less than 2 years ago: A bunch
- ActivityPub: a bunch
- Bluesky: a couple
- DSNP: few
- Nostr: none
- Signal groups
- Matrix: a few
- IndieWeb: a few
- Farcaster: none

?: Cozy web (e.g. chat threads) vs dark forest web

Gradients of intimacy

Not either or. Contextual.

Data sovereignty, holonic.

Something higher

Next steps:

- **Host a “part 2” session tomorrow**
- **Johannes will be hosting a more tech focused session tomorrow**
- **True Internet will be hosting a session on Thursday**

—

Referenced:

Personhood Credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online

<https://arxiv.org/html/2408.07892v1>

<https://arxiv.org/pdf/2408.07892>

Anonymity vs Privacy

Session Convener: Ken Griggs

Session Notes Taker(s): Ken Giggs

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

One time credentials

Domain proofs

Pseudonymous identifiers

C2PA

Concordium

Verifiable encryption

Trust Spanning Protocol

Transparency Log

Corroboration Security

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

I started the session as a discussion about the distinctions between anonymity and privacy, with the intent to discuss what those meant and how they were valued across a range of participants:

(Issuer -> Subject -> Holder -> Verifier -> Relying Party) + Governance

Where subject and holder are often the same entity, and verifier and relying party are often the same entity. Over the course of the discussion, Governance was added.

As a starting point, I offered a “vocabulary” we could use to begin to discuss anonymity and privacy:

- Recognizability (can a verifier / RP recognize a returning subject / holder?)
- Selective Disclosure (can a presentation contain less than all of the claims in a credential?)
- Trackability (often also called linkability, can the interactions between a subject and one relying party be correlated with interactions between the same subject and another relying party?)
- Zero knowledge proofs (can I prove that I have a credential without sharing it at all?)

On the topic of anonymity, respondents offered that we can define anonymity as the case where a RP “can’t tell the difference” between one subject and another, and that anonymity offers the ability to “be unknown”.

On the topic of privacy, another respondent noted that privacy exists on a spectrum from pseudonymity to full identity. Another noted that privacy is context dependent.

There was a lot of discussion on the various ways to protect privacy and/or anonymity:

- The principle of Data Minimization: RPs should only ask for the information they need. It was noted that RPs often ask for more information than they strictly need, and there is little incentive for most RPs to follow data minimization.
 - it was additionally noted that we should minimise data capture across all parties.
- There should be some permission required to ask for a credential. Unclear how this would be implemented.
- There should be accountability for data gathering, but unclear what form that would take, or what degree of accountability was appropriate. Also there is a need to balance accountability with privacy.
 - This is the topic on which the issue of identity ecosystem governance was raised. We did not attempt to delve into governance.

Aside from credentials, also related is the issue of data provenance / origination. How might we ensure privacy while also enabling verifiable data authenticity attribution? Same for ownership and the right to use data?

One issue raised that is often an issue for maintaining privacy is the revocation process. It was noted that revocation should be non-traceable.

Two tools offered for maintaining privacy that I have not looked into yet are a “transparency log” and the notion of “corroboration security”. Another is “domain proofs”.

Some other tools of which I am more familiar that were raised in the session were:

- one time credentials
- pseudonymous identifiers

Two more specific tools mentioned were:

- C2PA - the Coalition for Content Provenance and Authenticity, which I believe to be led by Adobe.
- Concordium - a blockchain based identity solution that is focused on privacy
- The Trust Spanning Protocol, which had multiple sessions at this IIW of its own

I had come to the session expecting that zero knowledge proofs would unambiguously enable anonymity and therefore inhibit accountability for users presenting with ZKPs. In this session, I learned about Verifiable Encryption, whereby a presentation using a ZKP can actually be pierced to reveal the presenting holder with participation from the issuer. TIL!

Also highlighted was the Warren / Brandeis treatise from 1890 on the “Right to Privacy” as important reading material in the space.

Several attacks on privacy and anonymity that were identified include:

- Collusion among parties
- Key sharing (there was some debate on whether this is really an issue)
- Visibility to outsiders (eg. observers of a public blockchain)
- Key management issues (users are exceptionally bad at this)
- Censorship
- Social Engineering (noted to be the most prevalent type of attack today, and not directly addressed by anything we do in the identity space)

How to Make \$Money\$ from SSI?

Session Convener: Harrison Tang
Session Notes Taker(s):

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

Monetization with SSI credentials is to be authenticated Via Spokeo and Verified ,for best results.

Privacy and the Mobile Drivers License (MDL)

Session Convener: Timothy Ruff, Wayne Cheng
Session Notes Taker(s): [Ankur Banerjee](#)

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

- [Identity Crisis: What Digital Driver’s Licenses Could Mean for Privacy, Equity, and Freedom](#) from ACLU
- [Digital ID State Legislative Recommendations](#) from ACLU

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

- Device engagement: NFC / QR code
 - SSID
 - Public Key
- Transmission
 - Bluetooth Low Energy (BLE)
 - Server Retrieval
- On Apple Wallet, you can only do NFC device engagement
 - It’s pretty locked down, so 3rd party wallets
- Standards in US have user showing QR code rather than scanning a QR code, because the police objected that a user holding up a phone could look like them holding up a gun

Summary of recommendations

Our 12 specific recommendations are listed below, followed by proposed legislative language for each item, preceded by an explanation of each item and its importance.

1. No police officer access to phones
 2. No Issuer ability to track via “phone home” mechanism
 3. Granular control over data released (selective disclosure)
 4. Unlinkability by verifiers (no digital ID as a ‘super cookie’)
 5. An open ecosystem
 - a. Open wallets
 - b. Private wallets
 - c. Transparent source code
 - d. A standardized provisioning process
 6. Verifier accountability
 7. A reporting requirement
 8. No remote government “kill switch” to disable people’s IDs
 9. A “right to paper”
 10. Restrictions on ID demands
 11. Restrictions on data use
 12. Enforcement through a private right of action
- Verifiable Credentials issued or endorsed by the government has greater weight
 - Our digital identity is given out by private companies
 - Not happy with EU identity model with trusted parties/trusted 3rd parties
 - ISO-18013 specification for MDL
 - “Server retrieval” is the “phone home” mode
 - Biggest implementer of MDL is AMVA, in server retrieval mode there’s no way to prevent that phone home

SD-JWT and SD-JWT VC 101

Session Convener: Daniel Fett
Session Notes Taker(s):

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

<https://danielfett.de/talks/2024-10-29-sd-jwt-101-iiw/>

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

No written notes submitted

Sync is not Send

Session Convener: Aaron D Goldman
Session Notes Taker(s):

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

<https://arxiv.org/abs/2212.13567> Range-Based Set Reconciliation [Alioscha Meyer](#)

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

We need a sync protocol for completeness and a gratuitous push protocol for new data.

VLEI Update - Verifiable Legal Entity Identifier - GLEIF

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

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

<https://www.gleif.org/en/vlei/introducing-the-verifiable-lei-vlei>

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

https://drive.google.com/file/d/1WOKb9eflLtjelljgT5kWY5AaqoFDmx_/view?usp=sharing

Has our SSI Ecosystem become Morally Bankrupt?

Session Convener: Christopher Allen

Session Notes Taker(s): Kim Duffy

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

The following posts were referenced in the discussion:

- Musings of a Trust Architect: Has our SSI Ecosystem Become Morally Bankrupt?
<https://www.lifewithalacrity.com/article/ssi-bankruptcy/>
- The Path to Self-Sovereign Identity: <https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/>
- Why Verifiable Credentials Aren't Widely Adopted & Why Trinsic Pivoted:
<https://rileyparkerhughes.medium.com/why-verifiable-credentials-arent-widely-adopted-why-trinsic-pivoted-aee946379e3b>
- The Greatly Exaggerated Demise of SSI: A Rebuttal to Premature Eulogies :
<https://decentralgabe.xyz/the-greatly-exaggerated-demise-of-ssi-a-rebuttal-to-premature-eulogies/>

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

Quote of the day: "There was no demand for liquid hand soap"

Christopher Allen, author of 10 Principles of SSI, challenges the SSI community to reflect on this question: "Have we strayed from founding principles?" This is in response to several factors:

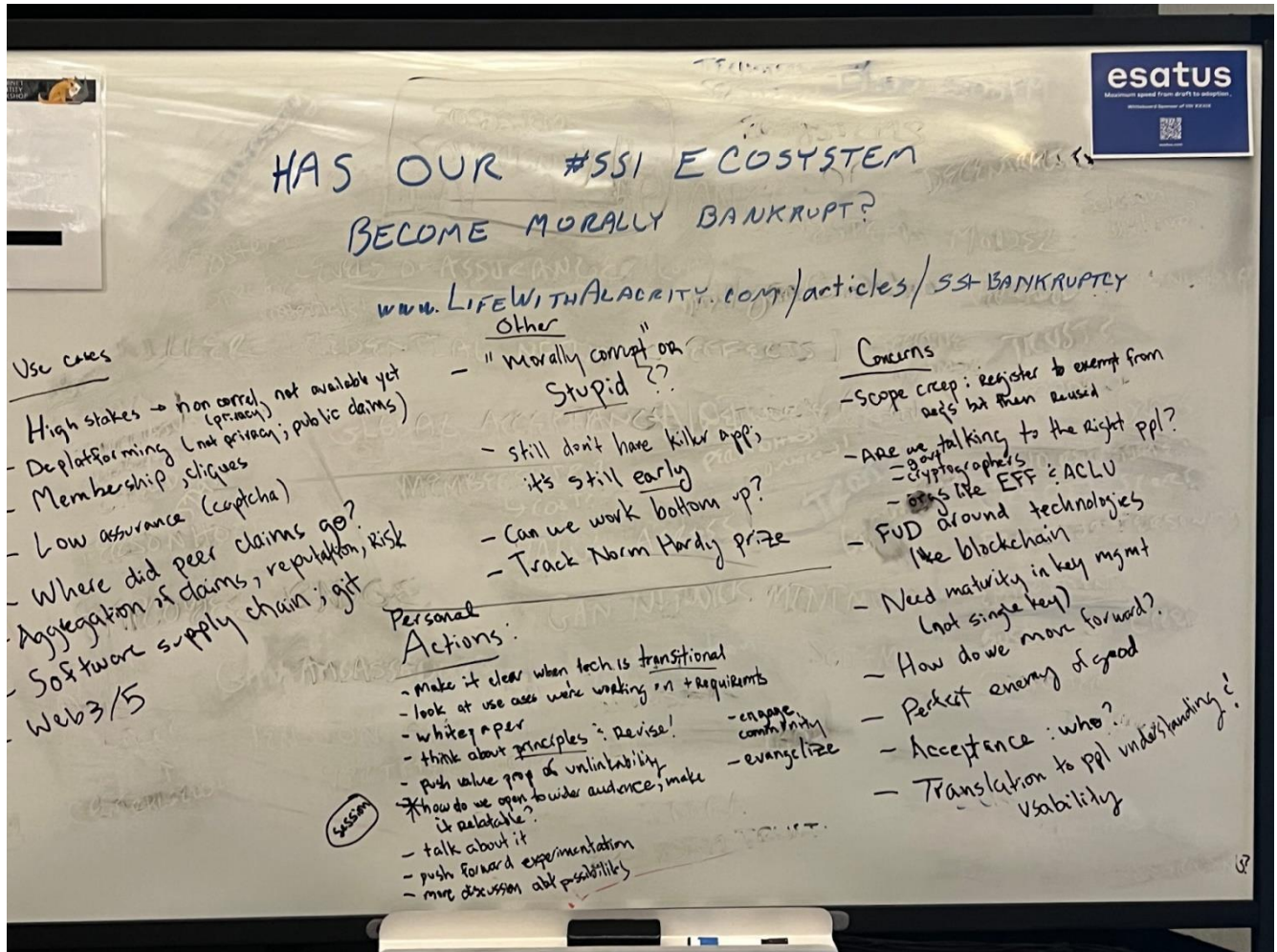
- Riley Hughes' talk and post (see link above)
- In pursuit of adoption, we've neglected principles
- Authoritarian encroachment, e.g., Texas atty general and name change requirements; discrimination
- Risk of pervasive surveillance and control

SSI was intended as a defence against encroachment, without fear of manipulation and incursion. A design goal is avoiding coercion. Have we compromised by accepting watered down specifications? GDPR should apply to gov and businesses. Risk of tyranny is a real threat.

Our compromises have left us vulnerable as a community. We're losing to watered down specifications like mdl and mdoc, and also losing to federated approaches that give lip service to SSI.

Christopher hypothesizes that such compromises – not market reasons – are the real reason SSI hasn't had traction. We have not committed unequivocally to uphold the values of SSI.

The group discussion was captured on the whiteboard:



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:

Putting Humanity Back
In Identity
We are creating a new professional class, the Digital Fiduciary.

Fiduciaries

Fiduciaries address situations where a principal necessarily depends on the loyal engagement of agents. Doctors, lawyers, and accountants are fiduciaries, each in their own specialty. Doctors help people manage complex health issues, beyond the expertise of the typical citizen. Lawyers help people and businesses deal with legal matters beyond most people's understanding including civil, criminal, procedural, and regulatory issues. Accountants help people and businesses document, understand, and apply financial tools in both personal and business contexts. Digital fiduciaries help individuals and organizations manage identity.

Digital Fiduciaries

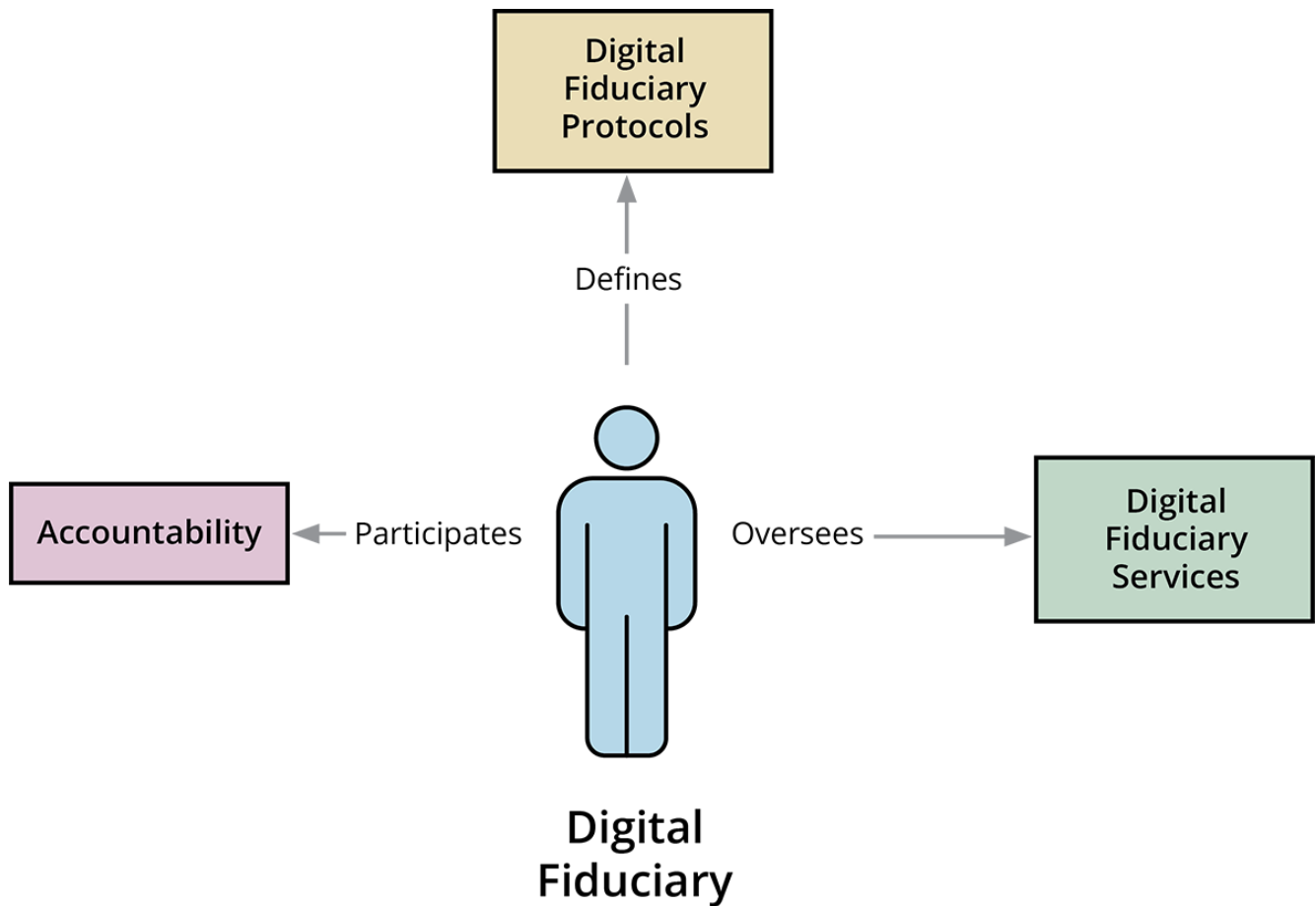
Digital Fiduciaries are oath-bound professionals with the moral, ethical, and legal commitment to place the interests of identity subjects above their own. They help us manage how society recognizes, remembers, and responds to specific people and things. They advise individuals and organizations about how best to manage identity, both their own and others, and are entrusted to deal with personal information in a privacy-respecting, yet verifiable manner.

Digital Fiduciary Association

The DFI will create the Digital Fiduciary Association (DFA) as the Self-Regulating Organization (SRO) for Digital Fiduciaries to establish best practices and ethical rules for its members. Through the DFA, Digital Fiduciaries collaborate to define Digital Fiduciary Protocols, which rigorously describe how to provide Digital Fiduciary Services, in which the identity interests of users are addressed in a fair and equitable manner. Providers of Digital Fiduciary Services legally sign the protocol's operating agreement, appoint a Digital Fiduciary to oversee the service, and accept the Digital Fiduciary Association's dispute resolution process as the first venue for resolving concerns. These Digital Fiduciary Signatories have a legally enforceable commitment to delivering the service as defined.

The Virtuous Triangle

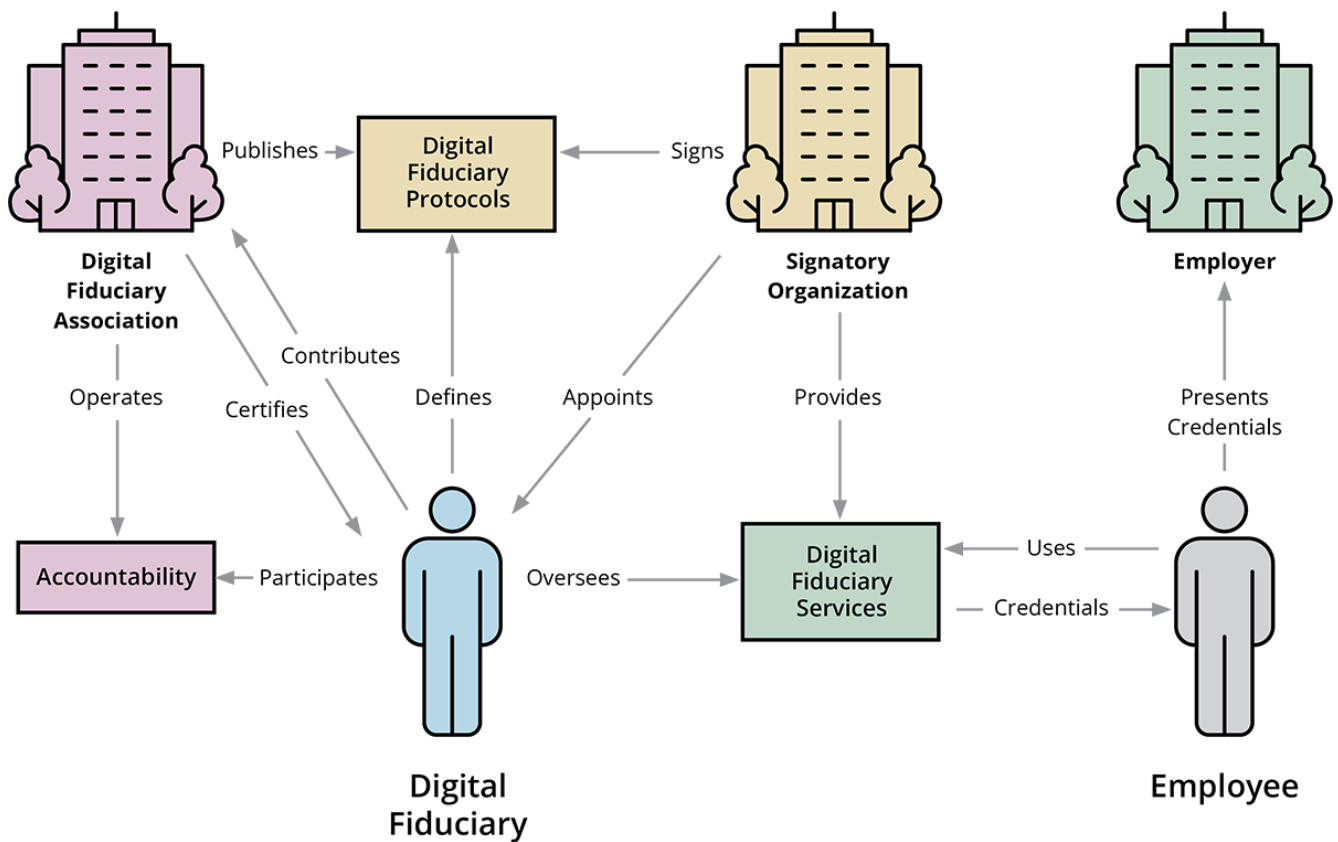
The Digital Fiduciary Association enables a powerful virtuous circle of protocols, services, and accountability that literally places a human being at the center of how we ensure auditable identity assurance in any domain.



- 1) Protocols defined by Fiduciaries
- 2) Services offered by Signatories and managed by Digital Fiduciaries, and
- 3) Accountability enforced by Digital Fiduciaries through the DFA

Together, these create a self-sustaining, generative architecture for advancing the state of the art in privacy-respecting identity, enabled by Digital Fiduciaries.

Our first protocol: a Digital USCIS I-9
 USCIS I-9 Proof of Eligibility to Work is the most broadly used identity verification protocol in America. Every legal employee and every legal employer performs this verification. We digitize it through the Digital Fiduciary, enabling anyone in America to prove their employment eligibility without revealing national origin or immigration status.



Our first protocol: a Digital USCIS I-9

The Digital USCIS I-9 service is provided by a Signatory who has legally agreed to the protocol’s operating agreement and appointed Digital Fiduciaries to manage and perform it. Prospective employees (at any employer) can use ANY Digital USCIS I-9 service provider to get a Digital USCIS I-9 Verifiable Credential, which they can present to any employer to prove eligibility requirements for working in the United States, all using open technology compatible with emerging global standards from the World Wide Web Consortium.

Fair Witness Credentials

The Digital USCIS I-9 credential is the first Fair Witness Credential, issued as a result of Fair Witness Ceremony, where identity claims are physically verified in person and evidence is digitally archived and stored offline to enable post-facto verification of the initial evaluation to any level of precision supported by the protocol. The resulting Fair Witness Credentials are usable by the data subject at any relying party that accepts that protocol. In case of anomalies, Signatories can challenge any particular Fair Witness credential (according to the rules of the protocol) and have any Digital Fiduciary re-evaluate the archived details. Fair Witness credentials ensure that oath-bound Digital Fiduciaries can verify the accuracy of claims without revealing the claims to the public or competitors.

Other protocols

For novel situations, where no existing protocols satisfy jurisdictional or business requirements, new protocols can be defined, fully leveraging the ethical framework that makes Digital Fiduciaries trustable. Email and web hosting. AML and KYC. Key escrow and data backup. These are all potential

areas for protocol development. The DFA creates a meta trust framework for identity related protocols appropriate for any jurisdiction and level of confidence.

The Oath

All Digital Fiduciaries must take an oath to put the interest of identity subjects above their own. This oath binds the individual fiduciaries to the legal, moral, and ethical obligations that make them trustworthy.

I, _____, do solemnly swear to faithfully execute the responsibilities of a Digital Fiduciary, protect the interests of identity subjects, and advance best practices in how to recognize, remember, and respond to specific people and things.

- I shall place the interests of identity subjects above my own, in any and all actions taken regarding information about, or related to, those subjects,
- I shall ensure the fair and appropriate use of subject information by services placed under my care,
- I shall treat all information received in the course of acting as a Digital Fiduciary with the utmost duty of care to ensure its security and confidentiality,
- I shall cooperate with all appropriate audits made by oath-bound Digital Fiduciaries, retrieving and providing onsite access to archived evidence according to rules established by the Digital Fiduciary Association (DFA),
- I shall cooperate with, and defer to, the DFA's dispute resolution processes for any and all Digital Fiduciary activity,
- I shall engage with fellow Digital Fiduciaries, the public, and private stakeholders to advance the best practices of Digital Fiduciaries and Digital Fiduciary Services,
- I shall make Fair Witness credentials based solely on those facts which I have physically observed, verified, and documented, according to the practices recognized by the DFA,
- I shall document, retain, and register all necessary evidence for the independent audit of all Fair Witness credentials made by me, and act as an ambassador to advance the profession of Digital Fiduciary.

By this act, I proclaim myself a Digital Fiduciary and join the community of Digital Fiduciaries.

Join

If you are ready to help create this new social institution, take the oath and join the movement.

The Challenges and ROI of Verifiable Credentials in Enterprise Use Cases

Session Convener: Heather Flanagan

Session Notes Taker(s): Heather Flanagan

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

Two things to consider: if there is an ROI, there is an initial investment. What is the cost of adopting VCs. The other side is what we're getting out of it. The initial cost is actually very very small, at least from a development perspective. Once people have credentials, the problem is more "what can they do with them?" Right now, there aren't enough verifiers to make it viable, so it doesn't matter that the investment is small.

With any network you're building, whether it's centralized or not, you have to start with the one piece people actually need. Nice to have, or "save a little money" is a tough sell. The efficiencies need to be shown on both sides. It's similar to a company saying "we're going green." They get some PR value, but they only get serious cost savings if it's done right.

If you just take identity proofing, not enough orgs are doing it. It's not just the verifier side. A company could be both a receiver and an issuer. Microsoft would be great to issue VCs to say how compliant a device is.

One thought, in the healthcare space, having insurance cards as VCs would be hugely helpful and we shouldn't give up too soon about it. It's a matter of ecosystem building and getting competitors to agree to something.

Large enterprise need to identity cross-boundary user journeys.

Supply chain management is another use case. Lots of use cases are kicking off. If an employee is issued a VC including qualifications and certifications, that credential is shared between different aspects of the supply chain (e.g., employee is certified to handle dangerous goods; they share that VC with the driver such that they can accept the material). Credavera (a Microsoft Partner) is an example of how this is being done.

- supply chain still has a bit of trouble with mapping to the real world, but there are so many efficiencies to be gained.

In the supply chain, they've been using similar documents for hundreds of years; it's ripe for moving to this model. Making the document actually digital will be transformative. It's not just digital, its cryptographically verifiable in specific contexts that allows an enterprise to reduce the complexity of docs and doc sharing, but also increase the assurance level of that document claim. Any implementation that requires that is fairly low hanging fruit.

One of the things with VCs is that you have to look at the full lifecycle of their documentation. It starts with a birth certificate, and you need that for the next credential (e.g., a passport or drivers

license). If you're able to mess with the initial credential, then you can get in and create a false digital identity that you can use for the rest of your life.

With ecosystem building, the tech foundation is fast, but the ecosystem needs help. In the energy industry, you need to share info about assets or usage data, and there's some interest in the industry but they first ask "where are the verifiers?" Not everyone is the same place. Maybe part of the investment piece is the ecosystem building. Do we need time to set up the relationships and then we can bootstrap the technology.

- how did this happen in the supply chain? Organically? No, there's already an established system for the supply chain. what was layered on was the benefit to layer on VC to replace digital documentation with cryptographically verifiable information that could follow the driver or the goods throughout it's existence. What was missing was the complexity of how to set up and use VC in a simple way. That's why they partnered with Microsoft.

In New Zealand, it's more a top-down approach. There are requirements to use VCs.

For the supply chain use case, is it a cascading VC where each step adds more info?

Don't confuse access tokens with verifiable credentials. Though a VC could be an access token (though that makes the federation people twitch.)

Are there qualities that an ecosystem possesses that would make it more amenable to disruption to use VCs?

- information already passing between parties
- endpoints that have authority about how information will be delivered
- a regulatory component

Enterprises have done B2B credentials for years. You have to push through not just that it's a more elegant, more secure solution, it needs to be a bigger improvement.

But this is bigger than B2B because peer-to-peer is too limited a use cases. In those cases, a VC doesn't help enough. If every Business in the world had VCs implemented, they could talk about API implementations and endpoints signature, all that would go away. "If you talk VC, it's already solved."

Looking at government issued credentials (birth certificates, SSNs etc). Most people don't care. The ecosystems do exist, but people don't see the value proposition. In a disaster scenario, it's more obvious what the value proposition will be. More likely they'll have their phone. It speeds up processing and you can have more trust because it's built in a digital environment. It's not just data, it's data that's been attested by a relevant third party. We have to build on the messy world that is here, not what we wish it would be.

There is still a digital divide that exists. Example: someone who isn't familiar with technology may receive lots of DocuSign documents, but the only verification is that they received the email. As technology practitioners, we recognize we need to ask questions, but other people won't.

There needs to be a trust model, too. Maybe the Global Acceptance Network could help solve for this?

We have to start from where we are today. There can be no adoption unless the problem is clearly framed and understood, and how it can be solved. We also have to know who we want to have adopt this and their own technical debt, product life cycles, their ability to handle new processes. We have to recognize there is a ramp from where we are today, the perfect use case, the perfect problem framed, there is a timing for adoption that must be considered.

There are different layers, business to employee, business to business, business to consumer. These are all different stories.

For the actual ROI on the supply chain example, was it lower the cost of the trust train process, or was it making trust possible? Both. Delivery of good was faster, lower cost, and verifiable. Sometimes the government increases the cost of not doing it (e.g., see forced labor supply chain laws). Orgs can't afford to have teams sort through all the documents required for all the components in their import. Also, in pharma, you have to be able to identify every component before you can invoice and get paid. Proof of provenance before payment is made is (again) becoming a thing.

The more global we become and the more parties are involved, the more necessary this becomes to scale and increase trust. But also, if there are 100 parties that would benefit, it's still a hard sell to try and coordinate 100 parties to all migrate. So far, the people who tried to solve this on a global scale tried to do this too early (e.g. Sovrin network, no one used it).

There is a ton of value in the flexibility of the system, but the requirements of online access made things hard to sell. It's hard to sell the "insurance" of how good it could be. People need to see a current, tactical need. Need to show the tactical problems that will be solved plus the strategic scenarios that could be coming.

What about outside supply chain? Age verification is a common use case. Licensed professionals (e.g., lawyers, electricians, forestry) may be gaining traction (e.g., go to a home and be able to show you are a licensed electrician). Travel may be seeing investment. Trade trusts in Singapore is another. Singpass has a lot of B2C value. First responder is another solid use case (see First Modern Digital Badge; discussion at the recent W3C).

GS1 are the barcode people - every bar code issued rolls back authorization up to GS1. With VCs, GS1 global issues a credential, GS1 chain that credential to what they issue to companies. The companies attaches product key credentials (bar code). The final VC will show the whole chain of credentials. (This is in prototype right now.) A lot of these problems that would have been better with a decentralized method have been solved with federated systems today. Unraveling that is hard; the economic model is slightly different. The economics are that there is only one party you can charge. The verifiers are subsidizing the issuers. It's an inversion of traditional relationships.

Are there standards for chaining VCs? No. There are ways people do it, but it almost feels too simple to standardize. But probably work to do here. It could be done in different ways, either by

chaining or with a trust infrastructure that represents different entities. That could also open up different ways to monetize this. The difficulty in directly monetizing aspects of the the VCs drive more conversations to efficiencies because directly monetizing VCs is hard. There are lots of patents around how to make a verifier pay an issuer for the verification.

The provenance of a VC is directly correlated with who is issuing it.

Another consideration: we need to recognize that there is the whole management of the credential life cycle, all the unhappy path, revocation, etc, all those things have to mature before broader scale adoption. WE're in a transition stage where parties are known to each other, trust is established, so it's logical to add this in.

SESSION #3

SD-JWT VC over proximity/offline

Session Convener: Lee, Cam, Torsten, John, Oliver, Kristina Yasuda

Session Notes Taker(s): Dima Postnikov

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

Problem statement

	Offline (wallet)	Over the internet
mdoc	18013-5	OID4VP (incl. Browser API)
SD-JWT VC	What do we do here?	OID4VP (incl. Browser API)

Options analysis:

	Extend ISO 18013-5 deviceRequest	Extend ISO 18013-5 OID4VP request	OID4VP over BLE	OID4VP with CTAP
Standard body	ISO?	ISO?	OpenID?	FIDO
Device engagement / Channel establishment	QR or NFC		BLE?	QR or NFC
Changes required	Extend deviceRequest / Response	Add OID4VP request / response	None?	NFC needs to be added (Happening anyway for cross device flows)
Deployment considerations	Aligned with 18013-5 existing deployments Not aligned with OID4VP online presentation	Aligned with 18013-5 existing deployments Not aligned with OID4VP online presentation		Aligned with OID4VP online presentation and existing CTAP deployments. Not aligned with 18013-5 existing deployments

Feature parity between online and offline	N		N	Y
Live implementations	Y Y	Y Y?	Y(?)	Y growing VERY fast
Format	CBOR	JSON	JSON	JSON
Built at	App level	App level	App level	OS or app level
Migration	Not required	?	Required	Required
Reliability	Y	Y	N	Y
	Standard extension in can be done in ISO or outside of ISO	Standard extension in can be done in ISO or outside of ISO	Couldn't use ISO	<ul style="list-style-type: none"> • Secure tunnel between 2 devices • Can send arbitrary • Invocation: • QR code goes through the cloud; • NFC is possible but was taken out • QR code + BLE? • Future UWB is possible • CTAP is available on almost all Android devices

Considerations:

- Bluetooth has security and reliability issues
- Any IPR issues on extending ISO protocols

IIW 101 Session - Authorization 101 Intro/Tutorial on the AM in IAM

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

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

Type Here

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

NO NOTES SUBMITTED

OCA Schemas

Session Convener: Carly Huitema
Session Notes Taker(s): Carly Huitema

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

<https://www.semanticengine.org/> - An implemented OCA schema generator with tools

<https://agrifooddatacanada.ca/> - The host organization of the Semantic Engine

<https://oca.colossi.network/> - The OCA specification

<https://kentbull.com/2024/09/22/keri-series-understanding-self-addressing-identifiers-said/> - A description of how SAID values are calculated in the CESR specification

<https://datascience.codata.org/articles/1729/files/66b5e0fc6116c.pdf> - A publication describing OCA


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

Overlays Capture Architecture (OCA) is a schema standard authored by the Human Colossus Foundation and implemented at Agri-food Data Canada (ADC). ADC is using OCA to help make research data more FAIR (Findable, Accessible, Interoperable and Reusable). OCA lets anyone document their tabular (and nested tabular) data with a data schema providing context for data and helping data users understand the data.

OCA has two unique features for a schema standard: OCA embeds digests into the schema architecture and OCA is organized by features which has implications in schema governance and data interoperability.

Digests used in OCA are Self-Addressing Identifiers (SAIDs) from the CESR specification. Digests are calculated using hashing algorithms from the contents of the OCA schema and then embedded into the schema itself. Digests enable benefits such as reproducibility - if you find the resource and calculate the digest (hash) you can verify that you are using the original resource when it is referenced by its digest.

Digests have costs, to verify a digest you need to ensure that you can canonicalize (order) the schema, serialize (write out) the schema, and calculate the digest the same way as when it was originally calculated.



Schema contents

- Schemas document attributes described by features

Attributes
Features

Attribute	Type	Sensitive	Label (en)	Information (en)	Units	Unit mapping (UCUM)	Format	Character encoding
animal_id	Numeric	Y	Animal ID	Farm-level unique animal ID			^[1-9]\d*\$	UTF-8
duration	<u>DateTime</u>		Duration	Milking event Duration in minutes	min	min	^(12 0?[1-9] 1[0-2]):[0-5]:[0-9](AM PM am pm)\$	UTF-8
session_n	Numeric		Session Number	Unique count of the milking event per cow, per day, per milking system. Resets at midnight.			^[1-9]\d*\$	UTF-8
total_yield	Numeric		Total Yield	Yield of milking event in <u>litres</u>	L	l	^\d*\.?\d+\$	UTF-8
milking_location	Text		Milking Location	Location of where the specific milking event took place			^\.(0,250)\$	UTF-8


10 | OCA schemas


Figure 1: Data schemas can be understood in a tabular format, where attributes of a dataset are described in a schema with a variety of features.

Schemas document the attributes of a dataset and describe them by features. Schemas will take the information documented in Figure 1 (attributes and features), and serialize it either row-by-row or column-by-column. Most schema languages such as JSON schema or XML schema will write out a schema attribute-by-attribute (row-by-row in Figure 1). In contrast, OCA describes schemas feature-by-feature (column-by-column) and this has implications in governance and interoperability.

Being organized feature-by-feature means that the OCA schema is optimized for feature management. A feature will be some kind of related task, e.g. a feature would be the Japanese translation of the schema labels, or the units used such as metric or imperial, or entry codes such

as a list of regions. The schema 'capture base' (the base listing of attributes) can be kept constant while features are swapped leaving the base data structure the same.

Each feature in an OCA schema is a separate object in JSON which has a calculated digest (aka fingerprint). Thus, adding additional features to an OCA schema will not disrupt the calculated digests for all the other features because additional features are not interwoven into the existing data structures but rather appended to the end (Figure 2). This is in contrast to feature addition in attribute-by-attribute architected schemas.

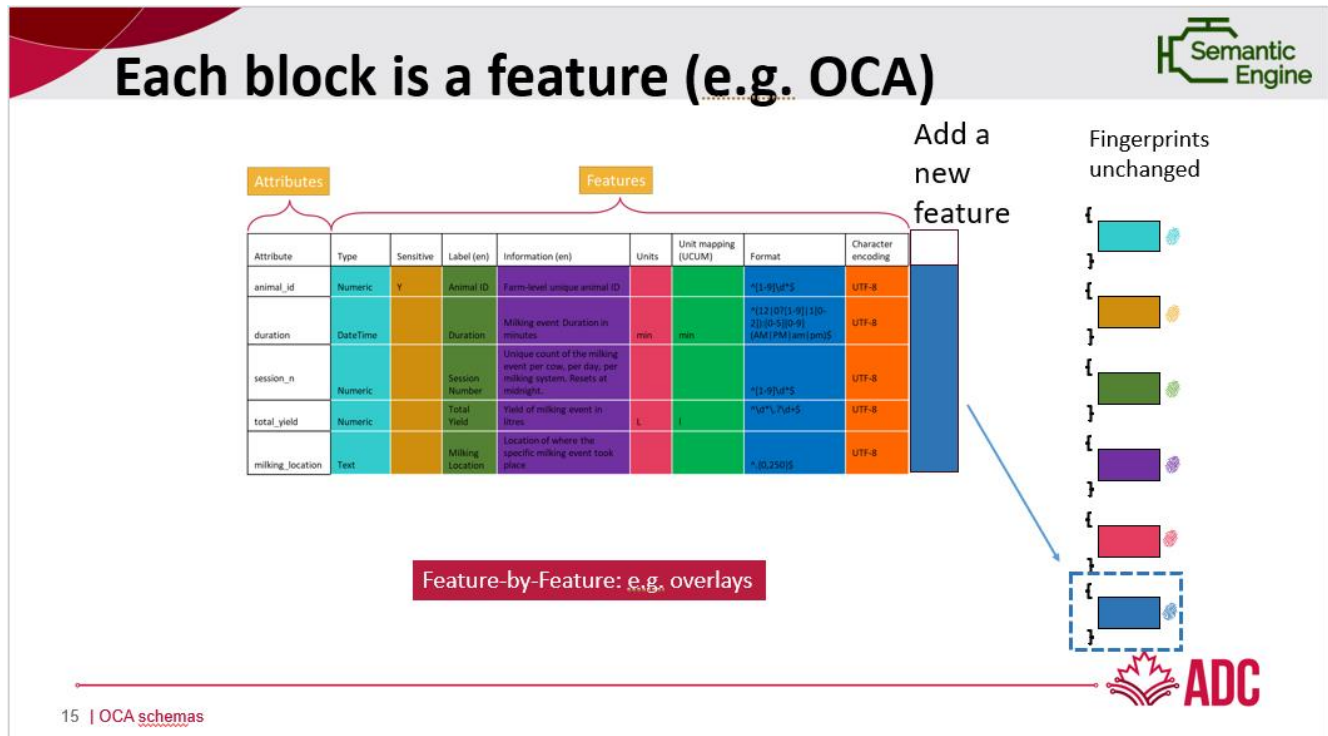


Figure 2: An OCA schema is organized feature-by-feature which OCA refers to as overlays. Each feature calculated has a digest (the fingerprint in the figure). Adding a feature does not disrupt the digests of all the other features in a schema.

A demonstration of writing and using an OCA schema is available at <https://www.semanticengine.org>, which is being used by researchers to document their data, verify their data and generate preformatted Excel sheets for data entry. These all support the FAIRness of research data and they can be implemented in a bottom-up approach.

Discussion in the seminar preceded with implementers of OCA from BC Gov and Swiss ID discussing the data structure, the addition of overlays that are outside of the specification and how to handle nested schemas and nested data structures.

C2PA vs TOIP TSP - What are they good for anyway?

Session Convener: Wenjing Chu, Eric S
Session Notes Taker(s):

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

Type Here

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

NO NOTES SUBMITTED

Security Questions - Back from the Dead

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

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

Notes from Matt MacAdam (not the official note-taker):

Matt Vogel proposes a new mechanism for key recovery/secret questions that uses geographic locations chosen from a map instead of personal data questions (e.g. “what was your first car?”).

Decent amount of skepticism from the audience around spearfishing and limited or popular locations. Matt V noted that certain locations can’t be chosen (e.g. major landmarks like the empire state building), as well as the ocean or open desert. One attendee pointed out that in rural areas what looks like an empty area in the middle of nowhere might be a popular recreational spot.

It was noted this is a potentially good mechanism since humans are pretty good at geographic navigation (see also: “memory palace”). One interesting proposal from the audience was also using interactive maps from game environments (“find on the map your favorite camping spot from Call of Duty 3”).

Decentralized Trust / Trust Registries

Session Convener: Fabrice Rochette

Session Notes Taker(s): Nicole Roy / Ariel Gentile

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

<https://github.com/verana-labs/decentralized-trust-spec>

<https://github.com/verana-labs/decentralized-trust-spec/blob/main/docs/iiv39/CM-EE-202410271834A%20Introduction%20to%20the%20Decentralized%20Trust.pdf>

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

Would like to build a model where both user and services are trusted

Concept: “Decentralized Trust Service” or “DT-S”

Decentralized Trust - Service

A DT-S is a service that:

- is able to identify itself with **Verifiable Credential(s)** **before** connecting to it;
- Is capable of resolving trust of peers that connect to it (**DT-S** and/or **DT-UA**) and drop untrustable connections.

Modern Bank - Identity Verification
KYC Service of Modern Bank SA

didwebauth-bank.demos.2060.io is a trusted service

Service provider:
Modern Bank SA
NIT: 17361841878

Terms and conditions
Privacy policy
Age restrictions: 18+

Proof of trust

Root of Trust
Mobile Business Intelligence S.R.L.
NIT: 30408029
Modern Bank SA
NIT: 17361841878
Modern Bank - Identity Verification

Confidential Information - ©2060 OU - IIVXXXIX Fall 2024

Concept: “Decentralized Trust User Agent” or “DT-UA”



Concept: “Decentralized Trust Trustable Communication Channel” or “DT-TCC”

A persistent communication channel where all participants are DT-S and/or DT-UA.

Concept: “Decentralized Trust Essential Credential” or “DT-ECS”

The basic credential schemas used to build this trust resolution: Service, Organization, Person, UserAgent

Question: communication from UserAgent to UserAgent? No answer yet. Spec is open!

Concept: “Decentralized Trust Registry” or “DT-R”

Identified by a resolvable DID whose DID Document references its credential schemas.

Credential schemas have their own Credential Schema Permission tree. Permissions are rules determining how the schema may be used (e.g. issuing, verifying, adding issuers, verifiers, etc.)

Question: why do we need DIDs for this? They are necessary mainly because they are described by a Document where we can find key material and services where their trust registry and essential schemas are referenced.

Each Essential Credential Schema is a LinkedVerifiablePresentation service conforming to Linked VP (<https://identity.foundation/linked-vp>).

Trust Resolution: DT-UAs and DT-S Query the DT-R to verify authorizations: for credential issuance and verifiable presentation

Question: What is decentralized about it? Everybody can create their own Trust Registry. But that does not mean that everybody will trust it.

Question: Relationship with GAN (Global Acceptance Network)? At some point it would be nice to make them work together.

Info and contributions/discussions welcome at <https://github.com/verana-labs/decentralized-trust-spec>

Slides for this session available at <https://github.com/verana-labs/decentralized-trust-spec/blob/main/docs/iw39/CM-EE-202410271834A%20Introduction%20to%20the%20Decentralized%20Trust.pdf>

EIEIO = Embracing Interop in Enterprise Identity Online

Session Convener: Aaron Parecki

Session Notes Taker(s): Michael Krotscheck

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

All in markdown

```
# EIEIO

Gathering use cases for federal IDP's.

- SSO
  - OIDC / SAML
- SCIM
- Entitlements
- Shared Signals (SSF)

Collections of use cases. What is your ideal world?

### Use Case 1: SSO

One part of the organization is Entra, another is AzureAD, integration for each different IdP is a lot of work. Also, verify that the authentication from the upstream comes back with MFA.
- An existing session may already have verified via MFA, we don't want to double-verify?
- How can we enforce cross-border policy restrictions?
- The origin of the authentication request must originate in a specific country, in a specific corporate network.
- Should some of these restrictions be applied at a lower network level?
- Schema negotiation?
- Schema Claim Registry?
- JIT Provisioning vs SCIM push provisioning?
  - SCIM Create / Update / Entitlements / Delete
  - OIDC
  - SSF
- Token BCP's for things like token explosion?
- There's no schema for entitlements

### Use case: More than one IdP

- Resource pools do not overlap.
- Account recovery
- Scoped Delegation

### What about shared signals?

- Synchronizing session events across different IdP's.
- A logout event with session TTL's that mismatch between the RP, IdP, etc.
```

```
- Mobile application session management
- Voluntary logout of one session, vs. invalidation of all sessions.
- User expectations around logout.
- What are the promises and obligations from the upstream IdP? Is there some way to broadcast that?
- The entire point of these systems is that they're disconnected and independent and everyone can do their own stuff, but that's also means that each organization can choose to prioritize.
- SCIM requests are not opinionated enough, or are too opinionated but fragmented.
- The SCIM schema isn't really specific enough, and there's too much customization in the attributes.

# Start with SAML Assertions, then move to OIDC
```

Crossing the Rubicon: Road to CESR

Session Convener: Charles Lanahan

Session Notes Taker(s): Kent Bull

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

Why implement CESR?

- to learn

CESR at high level

- want to be able to operate in the text and binary domain
- TLV scheme (Type, Length, Value) encoding
 - includes annotations (text domain)
- Primitives
 - cryptographic
 - data
- Field maps -> JSON, CBOR, MGPK
- Count Codes (for grouping)
- Op Codes (TBD)

Should be able to make CESR field map primitives.

Domains

- Runtime (raw) representation in your host programming language.

- Binary - wire protocol
- Text - URL Safe B64 mapped data. Codes encoded to b64

CESR versions

- There are two versions, 1.0 and 2.0. Only 2.0 is in the spec.
- Primitives are the same in both the versions, yet the count codes are different.
 - CESR v2 count codes count all TLV lengths in their various domains
 - CESR v1 count codes, some count TLV lengths, others count Elements

Field Maps

- JSON, CBOR, MGPK, CESR field maps
- For field maps two things are required
 - insertion ordering
 - serialization must support reading and writing from a stream in insertion order
- You can't put just any JSON or CBOR value, you have to use field maps.

Version String

Primitives

- These are elements in the CESR encoded protocol
- there are fixed length and variable length primitives

Gotchas

- For annotated CESR it relies on universal newlines so you must split on `\n`, `\n\r`, and `\r`, not just on spaces or general whitespace.

Personal AI on Digital Public Infrastructure

Session Convener: Reza Rassool

Session Notes Taker(s): Darius Dunlap

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

Kwaai - <https://www.kwaai.ai/>

Reza had slides that should be included here, with his permission. (Looks like the same presentation deck he showed at VRM Day)

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

Use a small language model for its linguistic comprehension capability only, run locally, against the local data (RAG or Graph-RAG)

pAIOS - the RAG platform for bringing in the source data into the Vector DB, and handling tenancy and other aspects.

How does it scale?

- Query time is linear with the size of the knowledge base
- Fast up to 10GB (but personal data may be a Terabyte or more)
- Sharding is one approach: P2P Distributed RAG

But privacy is an issue, so came up with Confidential Distributed RAG

- Homomorphic scrambler secures each remote shard
 - not fully homomorphic, but homomorphic for vector search

QUESTIONS:

No burden of retraining. The SLM is used only for its linguistic capability, not for its general knowledge. And it's not "retrained" on your personal data.

Adrian: Privacy implications? Under what licence do we have to the produced results?

[Sorry, lost track of the questions - D.]

Universal Basic Bandwidth

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

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

- a. From the Secure Scuttlebutt (SSB) value system: we have to **disintermediate communications** as much as possible, intermediaries will always try to come after you. That's why SSB shows how to run social media without servers.
- b. **Directories** are intermediaries with inherent centralization tendencies, self-reinforcing: Many people end up with Facebook because that's where they find their peers.
- c. We are in need of a vendor-neutral **notification channel**, for talking about much more than, but including IDs and social media handlers:
"From now on you can find me on Mastodon"
"my private key for my identity public key was compromised, stop using that ID"
"I'm offline for a month, contact my daughter in case of an emergency"
"there was an earthquake but we are doing fine"
- d. Narrow-band is fine for these singular but vital messages: let's guesstimate it as **300 bytes per month per earth citizen**, or a total of 2TB per month, globally. This number is chosen to be acceptable as a human right even for oppressive governments (you can't orchestrate a revolution with 300BpMpC).
- e. This looks like a central, global broadcast channel, correct, but the implementation can be fully distributed/parallel/decentralised and even must be so for redundancy reasons.
- f. **Airwaves are a commons** - as citizens we need to get our fair share, but valuable spectrum is auctioned to intermediaries, leaving nothing to us. One should therefore mandate carriers, global service providers, satellite networks to implement collection and dissemination of the 300BpMpC, and change the law that gives permission to citizens to create their own store-and-forward networks (even radio amateurs are not allowed to do so, today).
- g. **Bottomline:** Universal Basic Bandwidth is a necessary fallback from intermediaries - although being very narrowband, it enables bootstrapping into a diverse identity directory ecosystem.

CBOR DID & VC Controller Documents, Implementing Elision Privacy with Gordian Envelope

Session Convener: Christopher Allen ChristopherA@LifeWithAlacrity.com

Session Notes Taker(s):

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

<https://youtu.be/k1iIO-bfVhM?si=ElXwyLyLhDqBm5mw>

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

DID / VC Controller Documents: Discussed through the lens of Gordian Envelope, emphasizing the flexibility of elision and encryption for data minimization, vital in privacy-preserving identity verification.

Migrating from DID:Web to DID:Webs at Switchchord

Session Convener: Jonathan Rayback, Lance Byrd, Cole Davis

Session Notes Taker(s): Jonathan Rayback

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

[Slides here.](#)

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

See slides.

Cole Davis discussed Switchchord's use case in the music industry and why did:webs can help Switchchord with certain identity verification workflows plus bridge the KERI and W3C ecosystems. Lance Byrd gave an overview of the did:webs standard and why it improves did:web. Jonathan Rayback discussed his experience migrating to the did:webs codebase with various KERI repositories and KERI agents.

DID Method Squid Games

Session Convener: [Markus Sabadello](#), Alex Tweeddale, [Kim Hamilton Duffy](#)
Session Notes Taker(s): Kaliya Young, [Ankur Banerjee](#)

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

- [The Rubric Podcast](#): “A friendly conversation about DIDs and DID methods”

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

DIF

ToIP

W3C CCG or DID WG

IOTA

all have signed agreements for folks to participate together.

Sign Feedback Agreement.

Code of Conduct

New work Item at DIF

DID Traits <https://identity.foundation/did-traits/?ref=blog.identity.foundation>

A whole list of

Friendly Squid Games

We have been open to accepting a lot of random DID methods

We think it has done a lot of Harms.

They see the big long list of DID methods so they don't take the standard seriously.

There is a lot of vaporware on the list.

We are going to start seeing implementation.

DIDs have fallen out of favor with

CEN is starting to look at DIDs.

Need to look at it through a lens of maturity.

We need to start eliminating DID methods and being more cut throat.

It is no longer 200 DID methods.

Fed Work.

Flag for ones that are no longer actively maintained and don't have a working driver.

We should start to show what methods cover each different DID Trait.

Implementers can see DIDs that best fit their use-case.

Look at how few DID methods actually work
Registrar and resolver project.

Only 11 DID methods are supported in Universal registrar.

Missing feedback channel from people who are trying to use DIDs and have better communication.
Suggestions?

One of Manu's presentations has information on adoption.
DID "Placeholder" that Bluesky has - a lot of traction

Focus where we can engage with community adoption.

The three workstreams are.

The broad effort DIF effort.
Working with the proper SDO.
Nascent effort GitHub Repo - keep everyone posted.

Working Group is very open broadly to participation.

Another part is the core set of traits.

Using Traits and weigh in on opinions.
How to pair with someone doing external reporting.
Liminal, Gartner, Legendary Requirements.

Understanding what ones are still in development and are being maintained.
Oh on one is maintaining this.

DID Web - evaluator (took a couple months)
Looked at all the layers.
DNS - IANA

Is it decentralised if it runs on a company blockchain

DID Rubric - has all

DID Trait - functionality
Rubric is now Decentralised, Secure, Privacy Preserving.

Selected use-case first.
Rubric is an evaluation of a method in the context of a use-case.

To Autos point - this is where an auditor or 3rd party come in.

Auditor could come in.

It would be helpful to stratify - pair-wise, Blockchain ones.

There are so many different ways of doing it.

Keeping track of install bases.

DID WEb

DID Key

DID DHT

DID TDW

There is only a few supported in credential issuance.

If there is no software to work with the DID then it just works in a vacuum.

[DID Directory](#)

If you are single group bringing all these different DID Methods

Good vs Better

Is an opinion.

SDOs can't actually have opinions.

Conformant vs nonConformat

Updated Not Updated.

Reach out to the authors

To show why do I still care about this.

I think there has been a lot of - people don't want to establish another list.

People don't want that.

Personal Details vs entity names.

A good way to look if it is personal vs. organisational.

SESSION #4

Digital Credential Query Language

Session Convener: Daniel Fett, Kristina Yasuda

Session Notes Taker(s):

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

DCQL - Digital Credentials Query Language
[' dak]

The new query language in OpenID4VP

DCQL

- Part of OpenID4VP's soon-to-be-released Implementers Draft
- May or may not replace Presentation Exchange in OpenID4VP
- JSON-based syntax for requesting credential presentations
- *Mostly* credential format agnostic

Not invented here?

Why develop a new query language?

- Introduced mainly due to concerns about the complexity of PE
- More manageable for the browser API

--

Implementation Complexity of PE

PE provides a lot of flexibility at the price of introducing dependencies and implementation complexity, e.g.:

- Requires JSONPath (both Wallet & Verifier)
 - Complex syntax requires string parsing
 - Various functions and predicates
 - Regular Expressions
- Requires JSON Schema filters
 - Regular Expressions

Both JSON Schema & JSONPath bring security challenges.

--

Usage Complexity

PE is feature-rich, but not all of those features are needed for OpenID4VP, e.g.

- Presentation submission data structure
- Optionality in various places

--

PE allows for variation

- How is a claim requested?
- How is a path formed?
- How is a claim's value checked (pattern vs. const vs. enum)?

--

PE is not a perfect match

- Lacks some features, e.g. matching a vct value and subvalues

How does DCQL work?

--

Authorization Request

```
``http
GET /authorize
  ?response_type=vp_token
  &client_id=https%3A%2F%2Fclient.example.org%2Fcb
  &redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb
  &nonce=n-0S6_WzA2Mj
  &dcql_query={...} HTTP/1.1
````
```

Request parameter `dcql\_query` contains JSON-encoded query.

--

### ## Simple example

```

```json
{
  "credentials": [
    {
      "id": "my_credential",
      "format": "vc+sd-jwt",
      "meta": {
        "vct_values": [ "https://credentials.example.com/identity_credential" ]
      },
      "claims": [
        {"path": ["last_name"]},
        {"path": ["first_name"]},
        {"path": ["address", "street_address"]}
      ]
    }
  ]
}
```

```

Request `last\_name`, `first\_name`, `address.street\_address` from an SD-JWT VC credential with the specified `vct` value (or extending it). Return as `my\_credential`.

--

## Now with mdoc

```

```json
{
  "credentials": [
    {
      "id": "my_credential",
      "format": "mso_mdoc",
      "meta": {
        "doctype_value": "org.iso.7367.1.mVRC"
      },
      "claims": [
        {
          "namespace": "org.iso.7367.1",
          "claim_name": "vehicle_holder"
        },
        {
          "namespace": "org.iso.18013.5.1",
          "claim_name": "first_name"
        }
      ]
    }
  ]
}
```

```

```
 }
]
}
...
```

--

### ## More than one credential

```
```json  
{  
  "credentials": [  
    {  
      "id": "pid",  
      "format": "vc+sd-jwt",  
      "meta": { "vct_values": ["https://credentials.example.com/identity_credential"] },  
      "claims": [ ... ]  
    },  
    {  
      "id": "mdl",  
      "format": "mso_mdoc",  
      "meta": { "doctype_value": "org.iso.7367.1.mVRC" },  
      "claims": [ ... ]  
    }  
  ]  
}  
...
```

--

"A or B" claim matching

```
```json  
{
 "credentials": [
 {
 "id": "pid",
 "format": "vc+sd-jwt",
 "claims": [
 {"id": "x", "path": ["last_name"]},
 {"id": "A1", "path": ["postal_code"]},
 {"id": "A2", "path": ["locality"]},
 {"id": "B", "path": ["region"]},
 {"id": "y", "path": ["date_of_birth"]}
],
 }
]
}
```

```

 "claim_sets": [
 ["x", "A1", "A2", "y"], // Option 1
 ["x", "B", "y"] // Option 2
]
 }
]
}
...

```

Important: Not user choice — Wallet MUST select first available option.

--

## "A or B" credential matching

```

```json
{
  "credentials": [
    {
      "id": "pid",
      "format": "vc+sd-jwt",
      ...
    },
    {
      "id": "other_pid_part_1",
      "format": "vc+sd-jwt",
      ...
    },
    {
      "id": "other_pid_part_2",
      "format": "vc+sd-jwt",
      ...
    },
    {
      "id": "nice_to_have",
      "format": "vc+sd-jwt",
      ...
    }
  ],
  "credential_sets": [
    {
      "purpose": "Identification",
      "options": [
        [ "pid" ],

```

```

    [ "other_pid_part_1", "other_pid_part_2" ]
  ],
  {
    "purpose": "Show your rewards card",
    "required": false,
    "options": [
      [ "nice_to_have" ]
    ]
  }
]
}
...

```

How to respond to the "Identification" query and whether to send the rewards card is up to the user.

--

Simple value matching

```

```json
{
 "credentials": [
 {
 "id": "my_credential",
 "format": "vc+sd-jwt",
 "meta": {
 "vct_values": ["https://credentials.example.com/identity_credential"]
 },
 "claims": [
 {
 "path": ["last_name"],
 "values": ["Doe"]
 },
 {
 "path": ["postal_code"],
 "values": ["90210", "90211"]
 }
]
 }
]
}
...

```



## ***IIW 101 Session - Passkeys 101 AKA FIDO***

**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

## ***Open Wallet Ask Me Anything***

**Session Convener:** Sean

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

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

Lots of projects

Majority of project around Decentralised Identity

Open Wallet Forum at ITU

Neither do standards - bring folks to the table to work things out.

Wallet interop - formerly the Aries working group.

Sean Bohan is the "marketing department" of the OWF

OWF Labs github is separate.

Growth phase - move over.

Questions about OWF

Lots of projects doing their own thing.

How do you decide?

Its all up to the groups

Different projects used to

GAC

To advise and inform.

One of the benefits.

Once a project is in Labs

what factors are taken into consideration for growth.

## ***Consumer Reports AI Agent - discussion - - - - > / Dazza Greenwood, Ben M, Ginny F***

**Session Convener:** Dazza Greenwood, Ben M, Ginny F

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

## ***Come build your project with DIF Labs***

**Session Convener:** Andor Kesselman, [Ankur Banerjee](#), [Kim Hamilton Duffy](#)

**Session Notes Taker(s):** [Ankur Banerjee](#)

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

[DIF Labs IIW](#)

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

- Problem: Lots of people don't want to build standards but do want to collaborate with other individuals on real projects.
- Gap in the market between Standards Development Organizations and Incubators
- What is DIF Labs: How can builders in Decentralized Identity applications be guided to successfully navigate the space while balancing a multitude of factors, including market dynamics, legal considerations, and technical complexities? There is no great "safe space" for this use case today.
- Why DIF Labs? DIF is uniquely positioned within the ecosystem to deliver value in decentralized identity/tech.
  - Expertise / central role in the decentralized identity ecosystem. DIF was instrumental in building momentum for DI in the early days; many of the world's leading experts are active participants
  - Developer focus. DIF has always been developer focused. Other SDOs are not well positioned to do this
  - NOT focused exclusively on DIF Specs
- Why now?



- Tech maturity: The specifications have matured, many have moved out of DIF to SDOs
- Market need: The focus is shifting from standards development to implementation
- Safe space: Need for a neutral space to accelerate ecosystem collaboration, with WG best practices, access to technical expertise (provided by DIF member orgs) & IPR protection
- Co-chairs
  - Andor Kesselman
  - [Ankur Banerjee](#)
  - [Daniel Thompson-Yvetot](#)
- Timelines
  - First “beta” cohort starts in November 2024
  - Some projects to be selected from DIF Hackathon (finishing next week!)
  - Fine-tuning process for early 2025 push
- One of the first beta cohort projects: [LinkedTrust](#)

## ***Regulation Identity & Privacy - Why you need to care!***

**Session Convener:** Linda Jeng  
**Session Notes Taker(s):**

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

Decentralized identity, verifiable credentials, ZKP

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

We discussed how laws and regulations are important factors to consider when designing identity products. We discussed the legal history of the Bank Secrecy Act and how that has led to a surveillance regime and lack of privacy. We discussed how we can leverage decentralized identity tech to meet regulatory requirements while protecting our privacy. We discussed KYC, liability, due diligence, policy, and legal concerns. As well as the recent data hack of Change Healthcare that has leaked data of over one hundred million Americans.

## *OpenID AuthZEN: the “OIDC” of Authorization*

**Session Convener:** Omri Gazitt

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

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

- [Presentation](#)
- OpenID AuthZEN WG [page](#)
- Interop [website](#)
- [Todo app](#)
- Interop [architecture](#)

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

We covered the differences between traditional and modern authorization.

We introduced the principles of modern authorization - fine-grained, policy-based, real-time.

We reviewed the goals of the AuthZEN effort, the progress over the past year, and future directions. We also demoed the initial interop use-case.

Links to the materials above.

Cedar expressed interest in joining the AuthZEN effort.

## ***Credential Schema Standards: KYC and Proof of Personhood***

**Session Convener:** Otto Mora and Kim Hamilton Duffy  
**Session Notes Taker(s):**

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

[2024-10 Credential Schemas IIW](#)

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

Discussed the credential schemas work item in the Decentralised Identity Foundation (DIF), as well as the usage of abstract data models for interoperability across credential formats. Presented the “Basic Person” schema which is a schema to be used for KYC purposes in the Financial services industry and similar. The audience provided feedback on the schema.

On Proof of Personhood: Kim discussed an [associated white paper "Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online"](#) which she contributed to. The paper discussed the importance of anonymity and how bad actors leveraging artificial intelligence could make the internet unusable. Proof of personhood has therefore become very relevant and this

We discussed the joint effort between the Ethereum Foundation for a Proof of Personhood the effort will be done both in terms of a credential schema standard, as well as defining a spec for how to wrap a government issued id (such as a passport, aadhar document, or drivers licence) with a zero knowledge proof derived from it. This would constitute a self attested proof of personhood. The working group is being defined and the effort will commence in early 2025.

## SESSION #5

### *KERI Security Duplicity Evident Data Provenance + AI Safety*

Session Convener: Sam Smith

Session Notes Taker(s):

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



Lance Byrd • 2nd

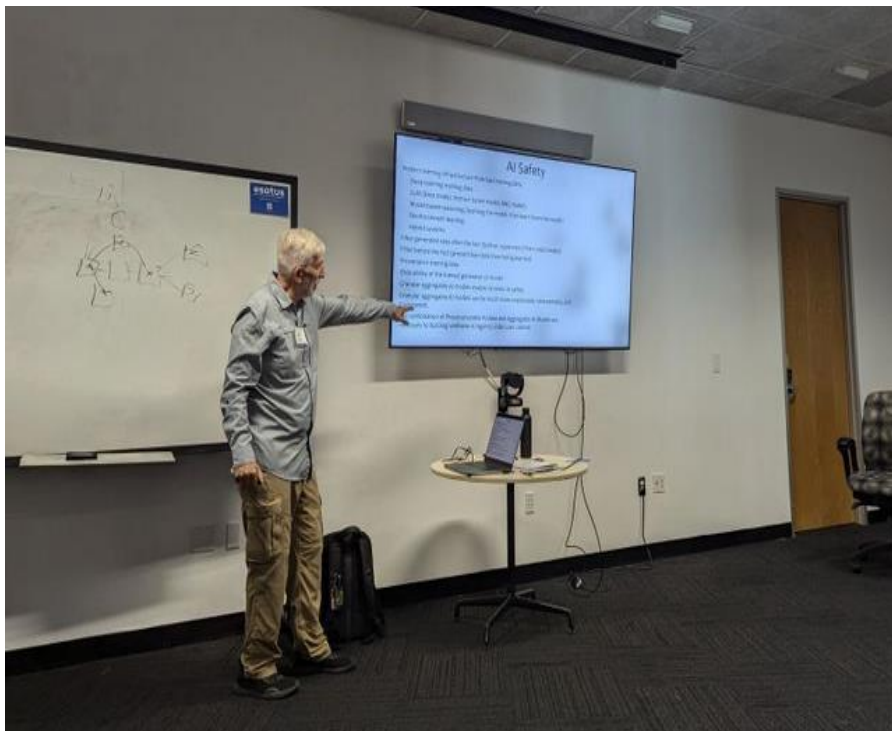
Identity Developer and Co-Founder - Secure Organizational Ide...

2w • 🌐

+ Follow ...

**Samuel M Smith PhD** at **Internet Identity Workshop** returned to his original field of AI. He covered different types of AI properties; Transparency, Interpretability, Explainability.

Using KERI we can track the provenance of training data in order to correct data over time. And build auditable AI agents that can be decentralized and optimized for your own use case.



## ***IIW 101 Session - Intro to Self Sovereign Identity***

**Session Convener:** Limari N and Steve V  
**Session Notes Taker(s):**

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

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

NO NOTES SUBMITTED

## ***Zero Trust with Zero Data***

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

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

Presenting your ID to buy beer is used so often as an example of how verifiable credentials work that it's cliché. Cliché or not, there's another aspect of using an ID to buy beer that I want to focus on: it's an excellent example of [zero trust](#)

*Zero Trust operates on a simple, yet powerful principle: "assume breach." In a world where network boundaries are increasingly porous and cyber threats are more evasive than ever, the Zero Trust model centers around the notion that no one, whether internal or external, should be inherently trusted. This approach mandates continuous verification, strict access controls, and micro-segmentation, ensuring that every user and device proves their legitimacy before gaining access to sensitive resources. If we assume breach, then the only strategy that can protect the corporate network, infrastructure, applications, and people is to authorize every access.*

**From [Zero Trust](#)      Referenced 2024-02-09T08:25:55-0500**

The real world is full of zero trust examples. When we're controlling access to something in the physical world—beer, a movie, a boarding gate, points in a loyalty program, prescription drugs, and so on—we almost invariably use a zero trust model. We authorize every access. This isn't surprising, the physical world is remarkably decentralized and there aren't many natural boundaries to exploit and artificial boundaries are expensive and inconvenient.

The other thing that's interesting about zero trust in the physical world is that authorization is also usually done using [Zero Data](#). Zero data is a name [StJohn Deakin gave](#) to the concept of using data gathered just in time to make authorization and other decisions rather than relying on great stores

of data. There are obvious security benefits from storing less data, but zero data also offers significantly greater convenience for people and organizations alike. To top all that off, it can save money by reducing the number of partner integrations (i.e., far fewer federations) and enable applications that have far greater scale.

Let's examine these benefits in the scenario I opened with. Imagine that instead of using a credential (e.g., driver's license) to prove your age when buying beer, we ran convenience stores like a web app. Before you could shop, you'd have to register an account. And if you wanted to buy beer, the company would have to [proof the identity of the person](#) to ensure they're over 21. Now when you buy beer at the store, you'd log in so the system could use your stored attributes to ensure you were allowed to buy beer.

This scenario is still zero trust, but not zero data. And it's ludicrous to imagine anyone would put up with it, but we do it everyday online. I don't know about you, but I'm comforted to know that every convenience store I visit doesn't have a store of all kinds of information about me in an account somewhere. Zero data stores less data that can be exploited by hackers (or the [companies we trust with it](#)).

The benefit of scale is obvious as well. In a zero data, zero trust scenario we don't have to have long-term transactional relationships with every store, movie, restaurant, and barber shop we visit. They don't have to maintain federation relationships with numerous identity providers. There are places where the ability to scale zero trust really matters. For example, it's impossible for every hospital to have a relationship with every other hospital for purposes of [authorizing access for medical personnel who move or need temporary access](#). Similarly, airline personal move between numerous airports and need access to various facilities at airports.

Finally, the integration burden with zero trust with zero data is much lower. The convenience store selling beer doesn't have to have an integration with any other system to check your ID. The attributes are self-contained in a tamper-evident package with built-in biometric authentication. Even more important, no legal agreement or prior coordination is needed. Lower integration burden reduces the prerequisites for implementing zero trust.

How do we build zero data, zero trust systems? By using [verifiable credentials](#) to transfer attributes about their subject in a way that is decentralized and yet trustworthy. Zero data aligns our online existence more closely with our real-world interactions, fostering new methods of communication while decreasing the challenges and risks associated with amassing, storing, and utilising vast amounts of data.

Just-in-time, zero data, attribute transfer can make many zero trust scenarios more realizable because it's more flexible. Zero trust with zero data, facilitated by verifiable credentials, represents a pivotal transition in how digital identity is used in authorization decisions. By minimizing centralized data storage and emphasizing cryptographic verifiability, this approach aims to address the prevalent challenges in data management, security, and user trust. By allowing online interactions to more faithfully follow established patterns of transferring trust from the physical world, zero trust with zero data promotes better security with increased convenience and lower cost. What's not to like?

## Autonomous Worlds

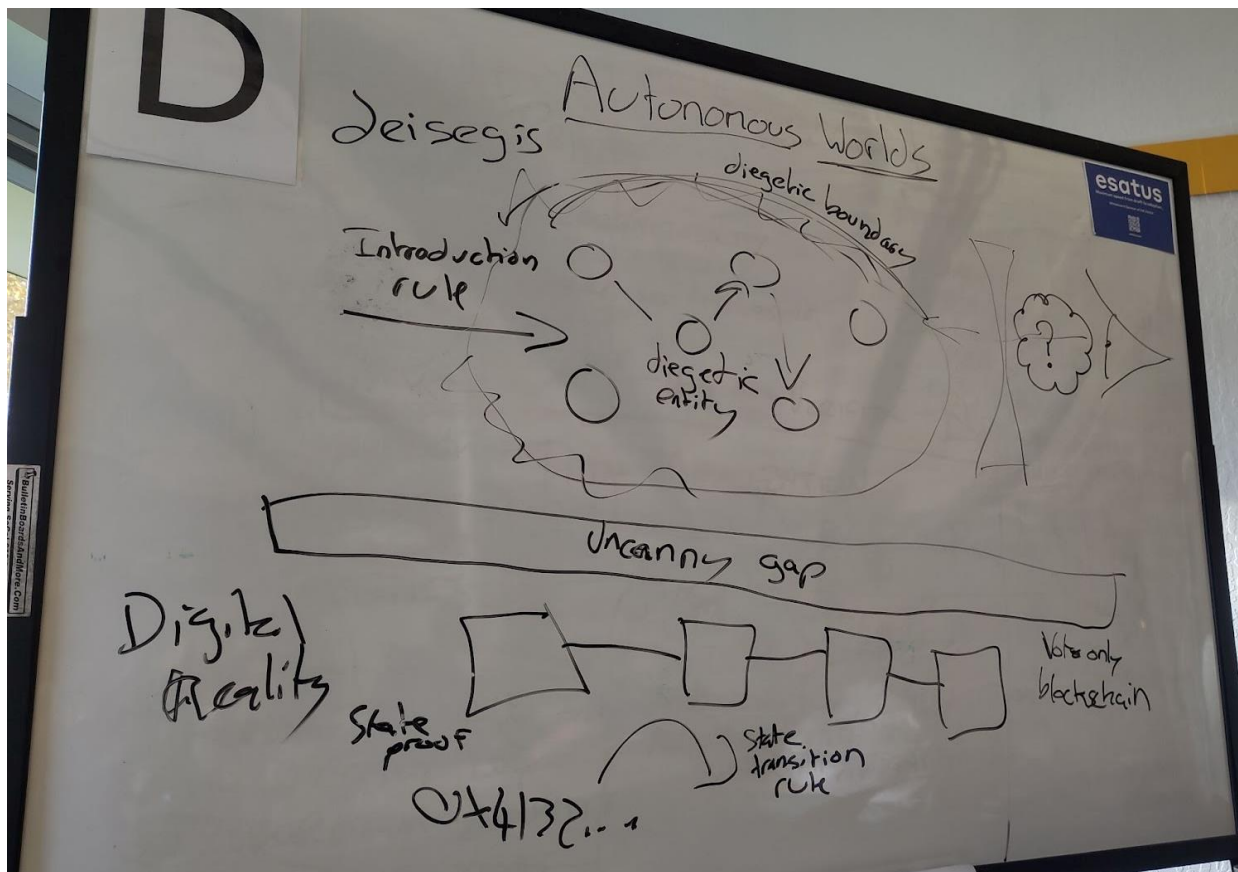
Session Convener: Will Abramson  
Session Notes Taker(s):

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

<https://0xparc.org/blog/autonomous-worlds>

<https://autonomousworlds.metalabel.com/aw01>

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



### World

A container of entities and the rules under which entities interact. We breathe life into these these containers through stories which layer meanings and positive, life sustaining interactions between entities within the world.

Worlds are perceived by minds and persisted within a substrate.

Memory, words, song, writing and now blockchain are all substrates for Worlds.

Examples: Fiction, the US dollar.

A dynamic system of entities interacting according to some rules contained within a diegetic boundary across which new entities and rules can be introduced according to an introduction rule.

### **Diegesis**

The process by which entities and interaction rules are introduced into a world following an introduction rule. An entity within a world is called diegetic.

### **Introduction Rule**

The mechanism defining how new entities can be introduced into a world.

### **Diegetic Boundary**

The boundary determining which entities are diegetic within a world. The gravity or force that shapes how minds subjectively perceive entities as diegetic.

We spend lots of resources enforcing the hardness of diegetic boundaries. E.g Law, Policing, Military all attempt to enforce the diegetic boundaries ensuring that diegetic entities are entities introduced according to an introduction rule. A hard diegetic boundary ensures that only entities introduced across the diegetic boundary can be seen as diegetic.

### **Diegetic Lens**

The lens that minds perceive diegetic entities through. How we evaluate an entity in diegetic.

### **Coherence / Canonical**

Individuals can come to consensus, share a communal sense, of which entities are diegetic to a world. Intersubjectivity.

### **Autonomous World**

A world where anyone can introduce new entities as diegetic following the introduction rules. And anyone can independently distinguish diegetic entities without relying on authorities.

Hard diegetic boundary leads to unambiguous definition of world.

### **Inter-Objectivity == Autonomous Worlds**

**Autonomous worlds give us a way to construct a shared inter-objective digital reality. We can have confidence that entities are diegetic and that others will also view them in this manner without depending on any authority.**

Still a limit to the facts of an autonomous world running on a blockchain substrate. Must cross the uncanny gap as we attempt to graft autonomous worlds onto our physical reality.



***Brainstorm way to link de-identified health data for population health in a privacy-preserving way.***

**Session Convener:** Alan Viars

**Session Notes Taker(s):** Jim Goodell jim at INFERable.app

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

Privacy, health data, data enclave, ZKP, SNOMED-CT, FIRE, xAPI, Confidential Computing,

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

PPRL – Privacy-preserving record linkage

CDC wants anonymized data that linked persons longitudinally but does not identify them

Zero Knowledge Proofs can support unlinkability

Most privacy-preserving way to to verifiable presentation is to ask a question that can be proved with VCs but not reveal them (but that requires data in personal wallets)

Distributed queries ( federated queries)

Statistics Canada does (special rooms that profs can enter queries and then a ‘librarian’ checks the query before letting the prof see the result)

It’s possible to analyse a query to see if it can allow identification and if cell size suppression is handled

Rice university data enclave

Distributed data can be by jurisdiction

Confidential computing - India is using this method

Term mapping: Simple Standard for Sharing Ontological Mappings (SSSOM)

## ***Delegation / Authorization for consumer-driven AI agents/ Standards for Human Agency/***

**Session Convener:** Dazza Greenwood, Rohit, Adrian Gropper

**Session Notes Taker(s):**

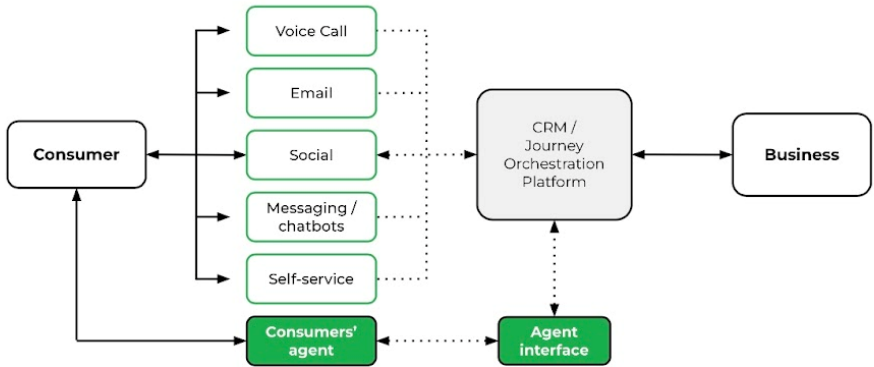
**Tags / links to resources / technology discussed, related to this session:**

[IETF GNAP RFC 9635](#)

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

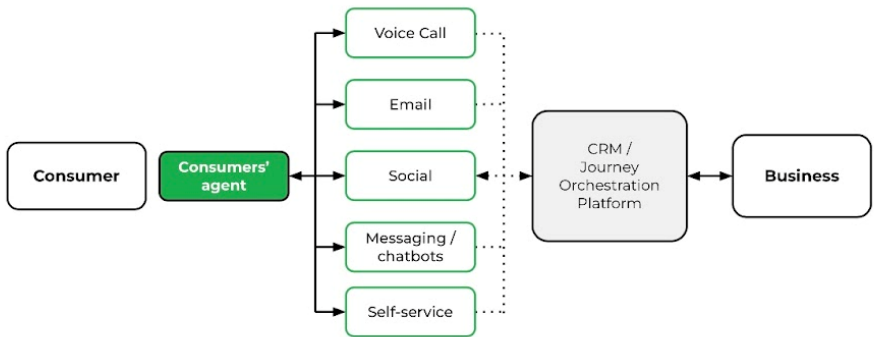
- In the future, consumers will have access to many kinds of “agentic AI” services that are designed to transact on their behalf.
- There are many unknowns about how this will play out, but is potentially an opportunity to re-wire how consumers and businesses transact, in a more consumer-driven way.
- Consumer Reports showed a “proto-agent”, called Permission Slip, that’s designed to help consumers exercise their data privacy rights. It’s based on the “authorized agent” provisions of CCPA and they developed a Data Rights Protocol to enable “agent-to-agent” transactions (e.g., a consumers’ agent delivers the request to a business’ agent)
- CR sees an opportunity to extend this pattern to many “customer service” or “customer experience” (CX) transactions. There’s a window of opportunity because AI is driving a lot of investment / rethinking around CX processes inside enterprises.
- CR’s hypothesis is around convening providers of enterprise SaaS for CX (Genesys, Nice, Salesforce, Zendesk, etc) and hammering out protocols for agent-to-agent communication.
- This should be in brands’ interest because, they’re going to be dealing a high volume of agents, across support channels, anyway – and they may as well figure out protocols to enable secure transaction, ensure manageable transaction volume, improve efficiency, productivity, and customer satisfaction.
- CR is proposing to lead an effort here, comprised of both consumer-driven tools and services, as well as enabling protocols. Success = exemplar services in the market and catalyzing an ecosystem

**For C-suite, accommodating agents as an “additional interface” in omnichannel is a good mental model**



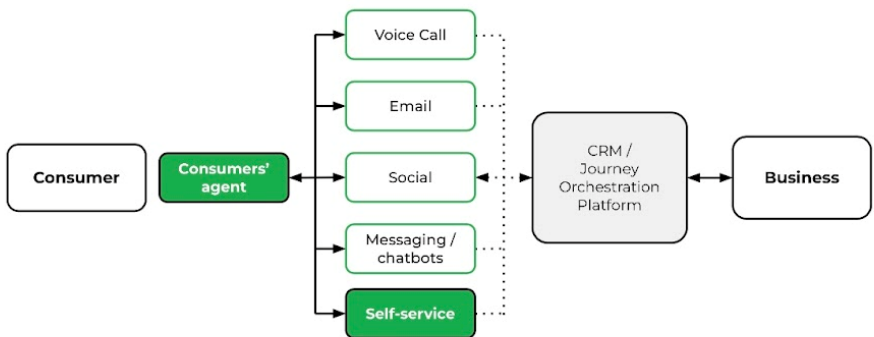
55

**We are already seeing proofs-of-concept for AI agents that leverage existing support channels — but it’s sketchy**



56

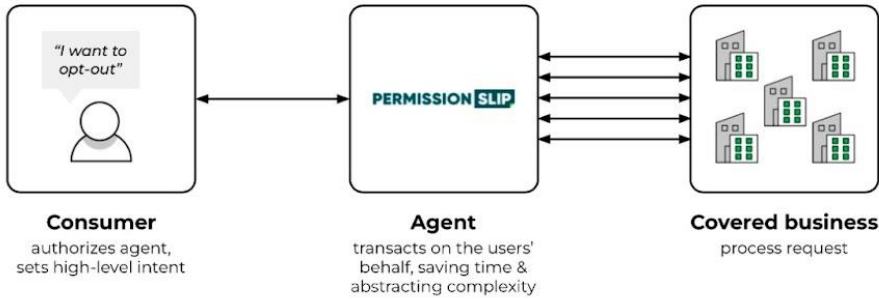
**AI agents authenticated (e.g., through oAuth?) may unlock a lot of immediate value through self-service portals**



57

Case study

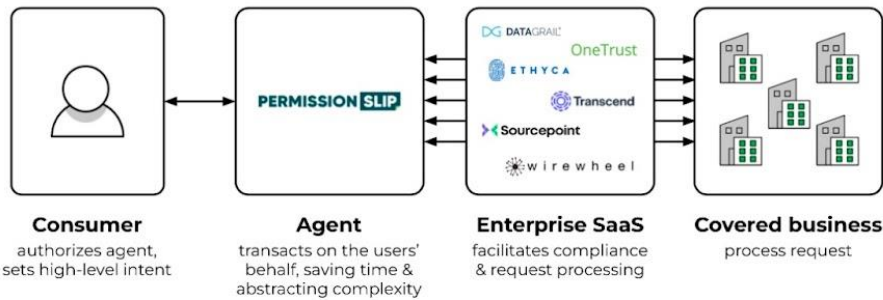
## Agents can help the consumer manage relationships & reduce overheads



43

Case study

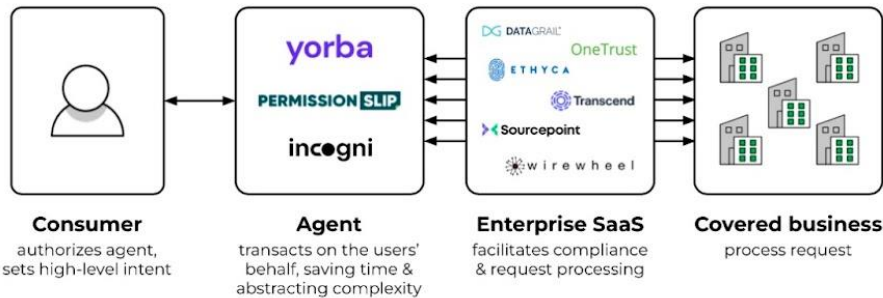
## Enterprise software enables and provides the "interface" to process transactions



44

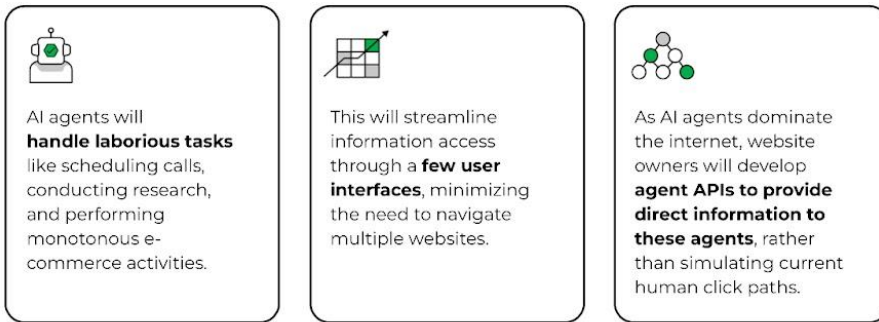
Case study

## We realized that agents should interoperate in a common way



45

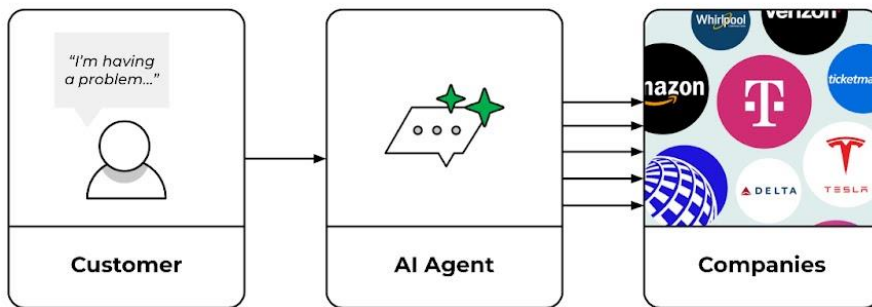
## Agentic AI is going to **change the internet** (and the marketplace...)



by Jeremiah Ouyang

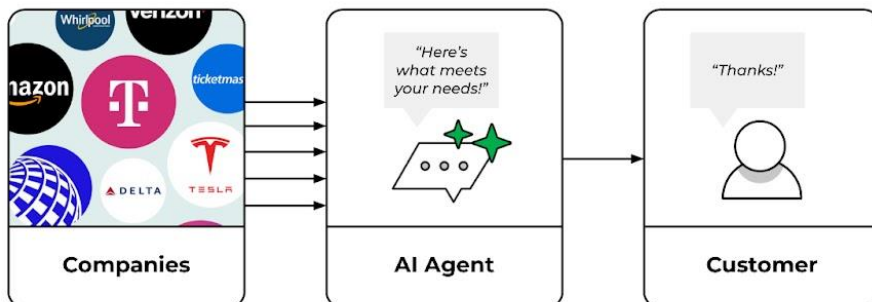
9

## At CR, we're excited by the potential of **agentic AI** to help consumers research, buy, and troubleshoot



10

## Agentic AI could help us **make better choices** and transact more freely



11

Issues:

- What can we code next week?
- The human's agent goes rogue
- agent (software) VS. Agent (fiduciary) The Agent has an accountable human
- Business / Legal / Technical (BLT) criteria across parties with JLINC
- DIDcom can put APIs on your mobile
- What's better than impersonation?

### ***Intro to Trust Over IP (ToIP)***

**Session Convener:** Judith Fleenor

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

### ***Web Authn + EUDI RP Authentication***

**Session Convener:** Torsten Lodderstedt

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

## ***Technical introduction to Global Acceptance Network (GAN)***

**Session Convener:** [Drummond Reed](#), David Poltorak, [Andor Kesselman](#)

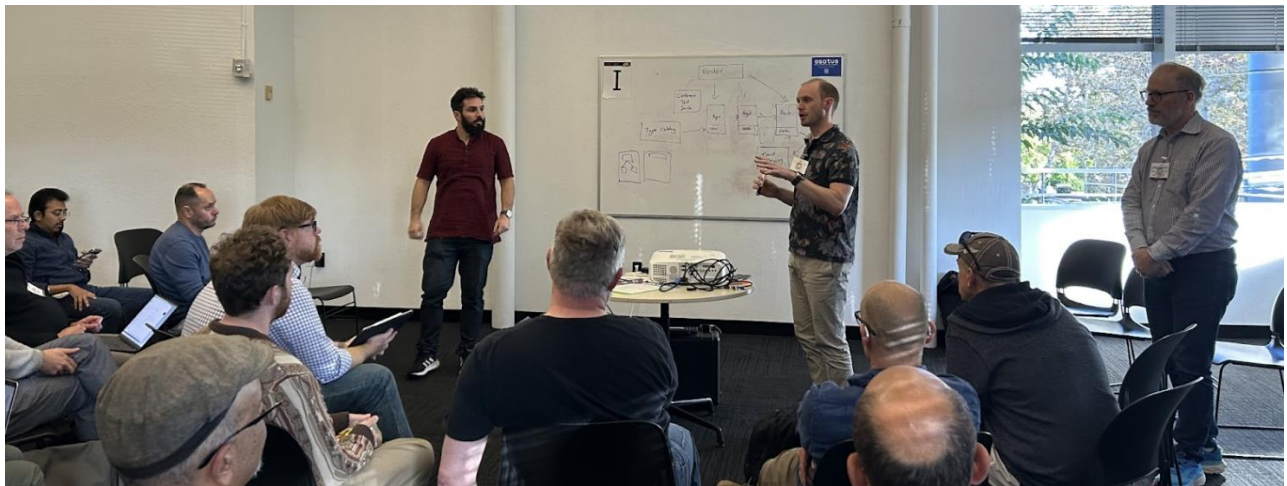
**Session Notes Taker(s):** [Ankur Banerjee](#)

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

- [Global Acceptance Network \(GAN\) website](#)

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

- Be as thin of a technology layer as possible
- Create a registry of registries for ecosystems of ecosystems



## *Identity Practitioner Pipeline - a conversation with DIAF, IDPro, OpenID... and you :-)* about bringing New People into identity

**Session Convener:** Elizabeth Garber, Heather Flanagan , Erick Domingues  
**Session Notes Taker(s):**

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

### Key Insights

1. We need to develop reproducible learning pathways
2. We need to create formalized mentorship opportunities
3. We standards bodies could create formal ways to develop

### Empowering Students

The Office of Biometrics and Identity Management is putting out a Biometrics Bulletin as part of their CITER program

- They do outreach to universities and encourage academics/students to submit whitepapers to get grant funding
- The hope is that this will lead to flourishing startup ecosystem in biometrics
- All government agencies with an interest in biometrics are engaged

Broader notes on appealing to younger audiences, esp students:

- More use of audio-visual tools like YouTube, Notebook LM, Podcasts
  - One participant engaged a lot in philosophy-of-identity podcasts as they were onboarding as an IAM practitioner

### Internal Moves

- How do you get people to move into IAM internally – or to get them to realize that they already ARE identity practitioners (maybe with expertise in one ‘realm’ of identity)
  - Identity curious? Solve a problem - encourage people to take on a challenge that maybe relates to their field but exposes them to another aspect of identity. Get excited about this broader field
- How do you grow within identity
  - The group started talking about viral TikTok videos at this point... it was more about getting excited about the industry and learning in interesting ways.
- Hiring for transferable skills

### Getting Into Standards

Standards has a PR problem: it’s a mystery - even internally

- Treaty-based standards are especially hard to break into
- Open standards are not hard to break into, theoretically, but hard to onboard



With a lot of people aging out and the learning curve getting steeper and steeper everyday, more needs to be done to bring new voices into this world:

- Need to find contributors who are motivated to teach and train
- It doesn't always *feel* inclusive as you are learning and trying to catch up (learn all the RFCs / stds you need to know to catch up with the WG you're interested in.... with every new standard that list gets longer!)
- How do you make a WG meeting easy to join?
  - Intern/volunteer/apprentice opportunities? Paid or unpaid?
  - Campus placements
  - Student trainees

### ***Edge Identifiers, Cliques, and other Opportunities of Multi-Party Computation (MPC) & ZKP***

**Session Convener:** Christopher Allen [ChristopherA@LifeWithAlacrity.com](mailto:ChristopherA@LifeWithAlacrity.com)  
**Session Notes Taker(s):**

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

<https://www.blockchaincommons.com/musings/musings-cliques-1/>

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

We now stand at another crossroads in digital identity. The current paradigm, where an individual's private key is the cornerstone of their identity, has served us well but it also has significant limitations—especially as we move toward a more interconnected, collaborative digital world. Fortunately, advances in cryptography allow us to rethink single-key self-sovereign identity systems, suggesting the possibility for new options such as edge identifiers and cryptographic cliques.

## Notes Day 2 / Wednesday October 30 / Sessions 6 - 10

### SESSION #6

#### *Germany EUDI Wallet Project update*

**Session Convener:** Paul Bastian, Torsten Lodderstedt, Kristina Yasuda, Mirko Mollik  
**Session Notes Taker(s):** [Ankur Banerjee](#)

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

- [SPRIN-D website](#)

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

- Wallet and server-side code will be released as open source
- One wallet from German government, others from 3rd party providers
  - German government funded 6 (smaller) companies
  - 5 non-funded (larger) teams
- 3 teams no longer progressing after jury selection. Lessons learnt will be published later
- All source code will be published for funded track. For the teams that didn't progress from funded track, this has already been published at <https://gitlab.opencode.de/funke>. When the competition ends, all the funded ones will publish their code.
  - The non-funded ones don't *have* to publish their code, but many are choosing to.
- EU ARF sets mDoc and SD-JWT, but does not make any choices on wallet architecture
- A lot of effort went into making sure that Germany didn't end up with something Germany-specific
- Trust anchoring/binding
  - eID: Physical card with a high LOA chip, but then would require every time to tap/read from the card to prove physical suggestion
  - TEE, Strongbox, Secure Enclave:
  - Cloud HSM: Prove some type of 2FA/MFA



## ***An abstraction for "pluggable" Verifiable Credentials and Zero Knowledge Proof libraries: Now with implementation and test framework!***

**Session Convener:** Mark Moir

**Session Notes Taker(s):** Harold Carr

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

Verifiable Credentials, Zero Knowledge Proofs, Abstraction

[Presentation slides](#)

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

### **SUMMARY OF WORK / PRESENTATION**

We're designing an experimental abstraction to enable mixing and matching Verifiable Credential formats and Zero Knowledge Proof libraries, so that different credential formats can take advantage of different (including not-yet-existing) underlying ZKP libraries that provide various features enabling privacy with accountability.

The presentation explains some of the benefits of such an abstraction, and presents an example use case illustrating use of privacy-preserving features including Selective Disclosure, Range Proofs, Membership (important for privacy-preserving revocation), Equality Proofs (e.g., two credentials contain the same Social Security Number), and Verifiable Encryption. The latter involves the Prover providing an \*encrypted\* value of a credential claim (e.g., Social Security Number), the Verifier confirming that it's correctly encrypted for some Authority (e.g., Police), enabling decryption by the Authority, and proof to a Governance Body (e.g. Court), that the decrypted value is the correct value signed in the original credential.

The talk presents an overview of the abstraction we have implemented so far and explains some of the design choices. We've now implemented the abstraction over two different cryptography libraries (DockNetwork crypto and the cryptography support for AnonCreds v2) in our internal Haskell prototype, as well as a test framework and a test suite that can be extended simply by adding a JSON file representing the desired "test steps" and expected outcome.

We have also translated our abstraction and test framework to Rust, implemented the abstraction over the AnonCreds v2 cryptography library, and made this public in a fork of the AnonCreds v2 GitHub repository, to enable receiving feedback and engaging externally towards a contribution to AnonCreds v2 repo.

### **SESSION SUMMARY**

The session was attended by around 20 people, and generated some stimulating questions and discussion. Here is a quick summary of some of them.

One attendee mentioned that modular identity systems have been done before and asked what's new in our work. We mentioned that, straightforward composition of multiple privacy-preserving Zero Knowledge Proofs into a single one does not preserve privacy because it exposes data used to connect the ZKPs, which leaks correlatable information, which is addressed by relatively recent "commit and prove" techniques. Nonetheless we acknowledged that of course abstraction and composition itself has been done before, and will no doubt be done again, because it is a powerful way to reduce complexity and increase flexibility.

Stephen Curran (lead of the AnonCreds v2 project) asked a couple of questions around whether/how the small set of "Claim Types" (a combination of data type and purpose that determines how claim data is treated) can be extended. In some cases, this is not necessary because it is "above" our abstraction. For example, a field representing a birthdate about which predicates such as "more than 18 years ago" will be proven is represented simply as an integer that can be subject to range proofs. How the integer value representing a date is determined is a policy decision to be made and agreed by users of the credential, and the abstraction does not need to treat it differently than any other integer.

Stephen also asked whether our techniques could be applied to SD-JWT. This is a great question -- after we clarify what it is: are we talking about the credential *format* or the underlying cryptography used? These should be clearly and cleanly separated, for example via our abstraction. With that clarification out of the way, the answer is "yes". Without changing the credential format at all, we can target it to our abstraction, and then enable additional privacy preserving features (range proofs, privacy preserving revocation, accountability via verifiable encryption, etc.) by using any cryptography library that implements our abstraction. Furthermore, we can improve the privacy properties of SD-JWTs by enabling selective disclosure without exposing correlatable hashes of non-disclosed attributes. Subsequent discussions during the day, particularly with Stephen Curran, pointed to this approach as being an excellent way to begin to bring value from our work to AnonCreds v1 credential format.

Finally, we got a question about whether performance is sufficient to, for example, enable client-side proof production on mobile devices. We have not yet done detailed performance measurement, and have not done any experimentation with mobile devices. However, we discussed how some features are quite slow in our tests so far, and that we are aware of potential optimisations, such as re-randomising verifiable encryption proofs, essentially enabling reusing previously constructed proofs, without enabling correlation by reusing exactly the same proof.

Intervention of Abstract models via Oracle Labs will enhance privacy preserving features and verifiable encryption. Transparency of performance will further be measured by audible in mobile devices.

## Aviation Security Trust Framework

Session Convener: Lucy Yang, Savita Farooqui

Session Notes Taker(s): Nicole Roy

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

Scenario: Airlines, nation-states, airports, contractors, etc... multiple security requirements at play, differ across all airports, “so much stuff going on, we’re helping them try to figure out where to start”

Understanding the business processes

Challenge is to not try to change everything, but what is most important to do?

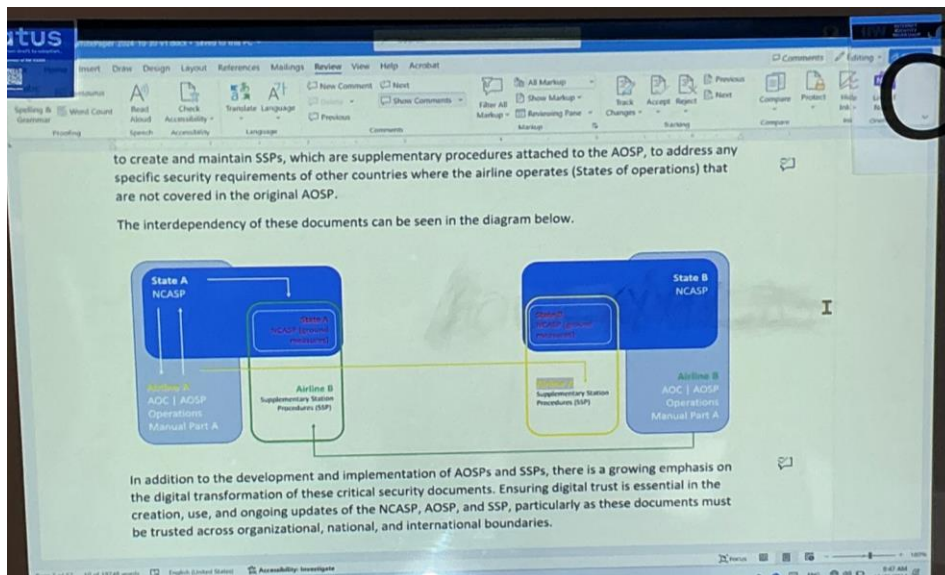
For aircraft to operate in a particular country, they have to work with local / national civil aviation authorities. Example for the US, American Airlines must create an AOSP (Aircraft Operator Security Program), and the TSA must review it and if approved, issue a certificate to the airline. Civil authorities like the FAA must conform to ICAO requirements.

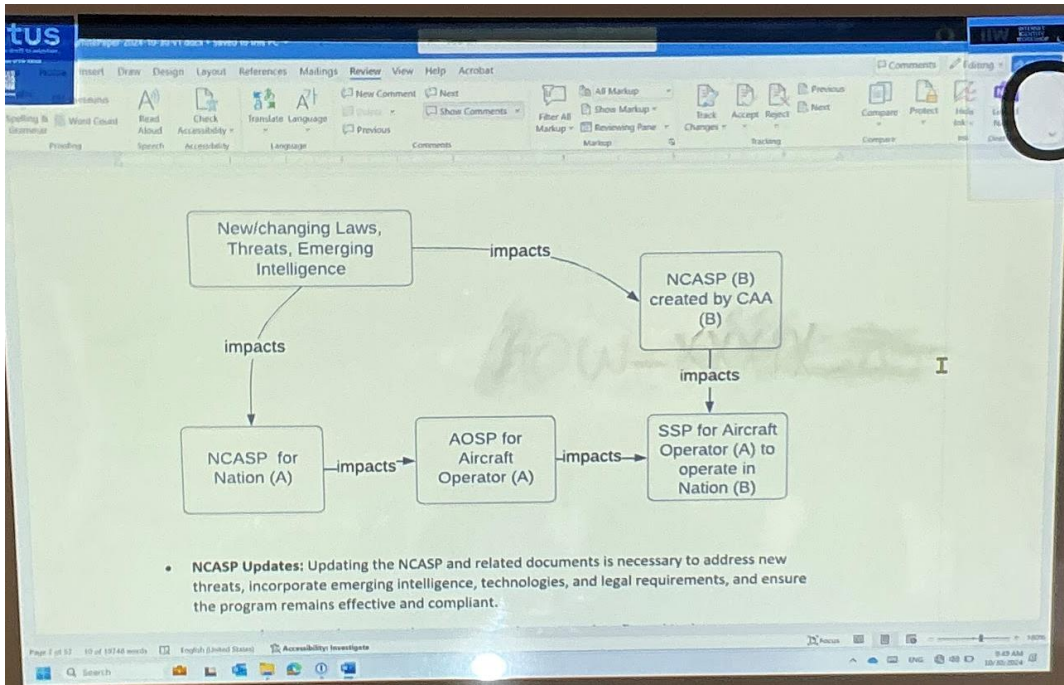
Then there are local guidelines, for example in Boston - municipal airport authorities, etc.

The way these documents are exchanged are really old-school, emailing PDFs around. Then the airlines have their own systems where they input the regulations and manage them. Lots of duplicative work, etc.

Want to make it so the documents can be digital, machine-readable, interchangeable, and use verifiable credential technology for exchange, verification, trust, etc.

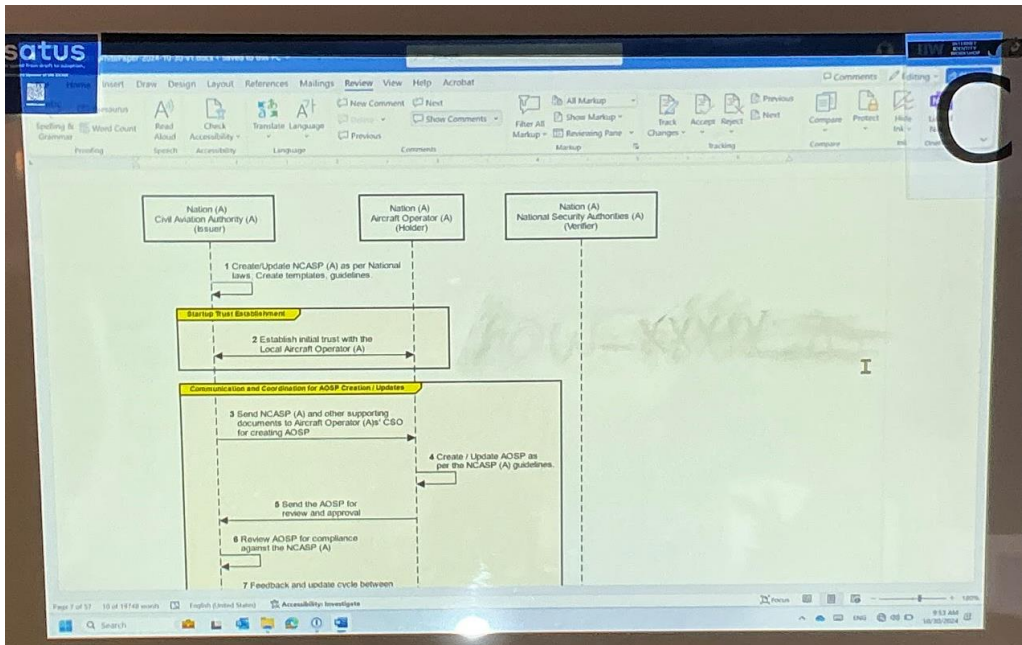
It’s not just the documents, it’s the authorization component of the people involved, managing the policies, documents, signing authorities, etc.



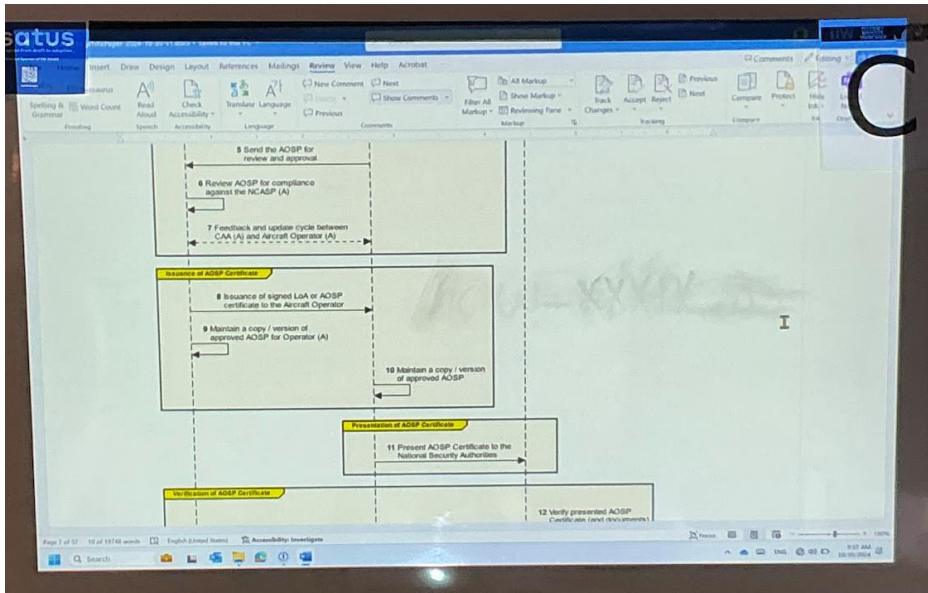


Part of the concern is that mistakes can be made, for example, when regulations change, a document may not get updated on time. Being able to track/audit/alert/etc. Deal with emerging threats in a timely manner and in accordance with evolving regulations.

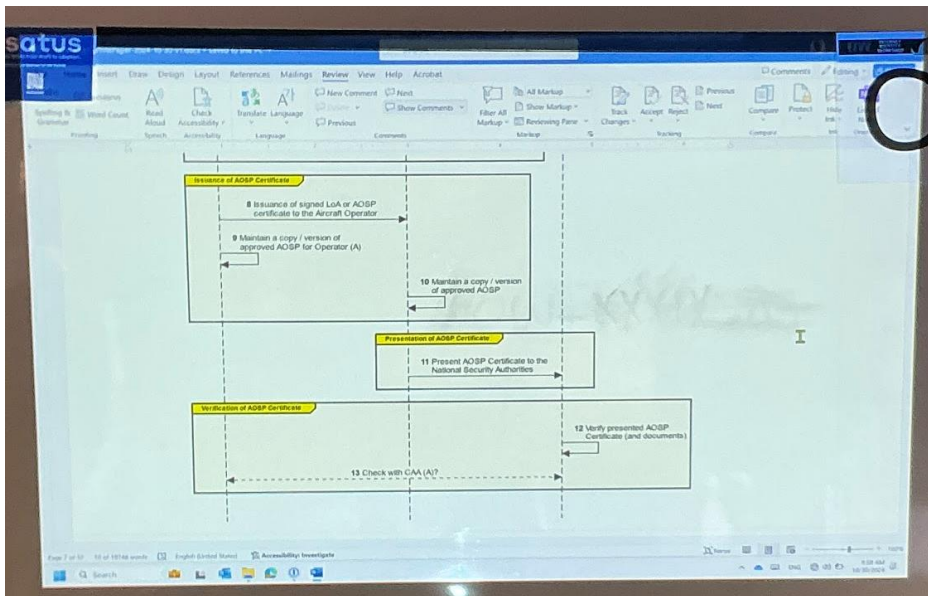
Verification scale is huge. Contractors, for example, the airport food vendors, need to do this, too.



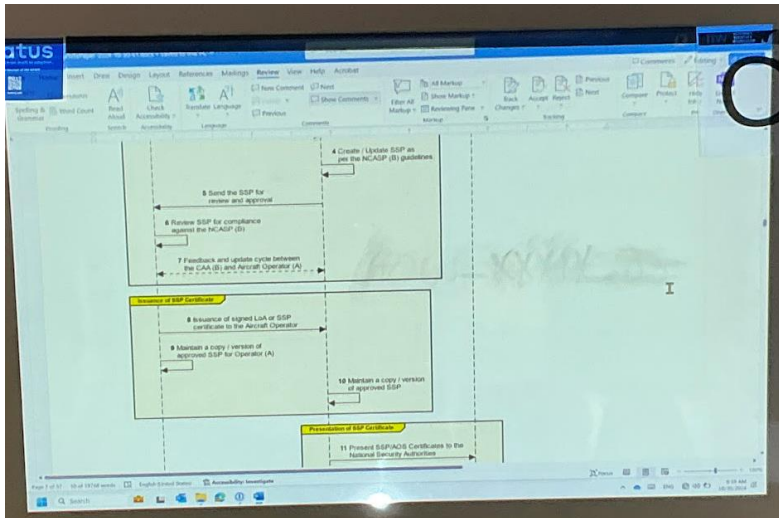
Right now, this ^^^^^ is all happening via emails



Document is huge, like 300-500 pages long, so cannot include the doc in VC directly, but put a hash of the document in the VC.



Similarly, "Station Supplementary Procedures" must be completed (SPs).

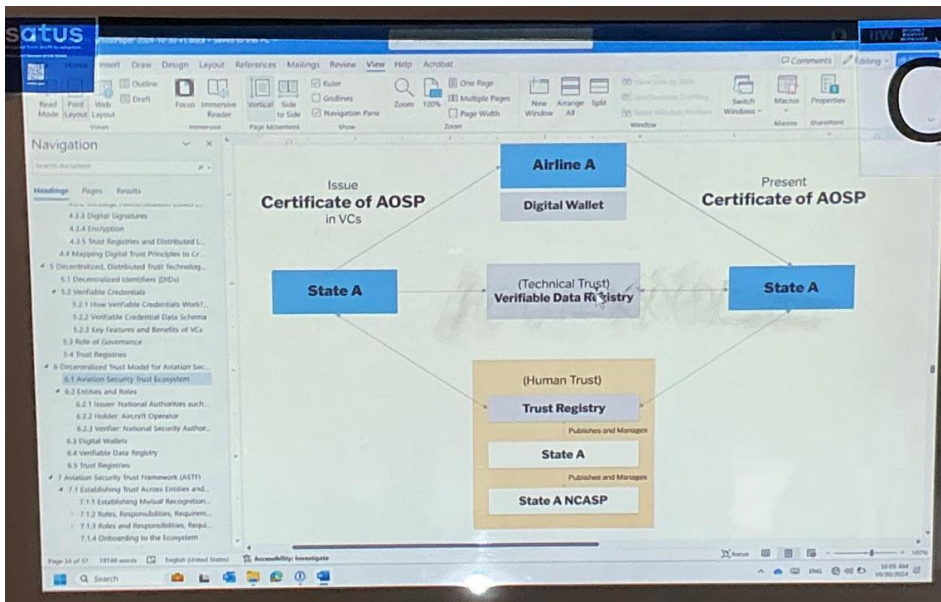


Want to create a trust framework which improves upon existing processes.  
 Hierarchical trust registry, IATA at the top, nation-states, then localities.

Airports must have a chief security officer assigned to create this type of document. How do you verify that the CSO has the credentials they need to be able to sign these documents? They need VCs for those credentials, too.

Also there is an “NCASP” document.

IATA has been doing a lot of standards development for airlines, but they are not a technology provider. Trying to figure out if IATA can do the technology side for the trust framework.



What kind of tooling needs to be deployed?

Countries are all at different stages of development/deployment of digital technologies.

Human trust ≈ Governance

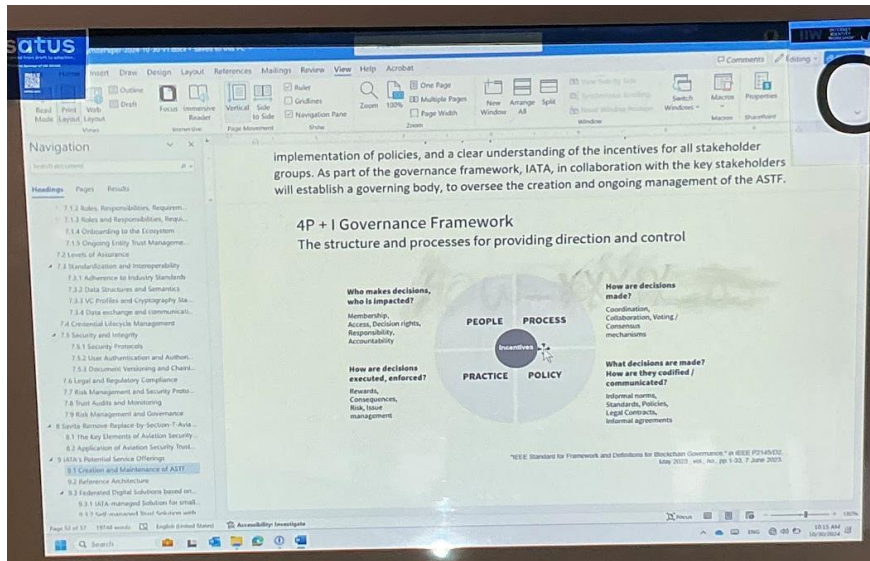
Human trust - Level of assurance



Nicole recommended they take a look at <https://refeds.org> to see how academia is doing this (assurance standards, governance, etc.) <https://refeds.org/specifications>

Risk management - Trust audits and monitoring

This is high-level guidance, IATA will have to take this and do something more detailed with it, starting with the template provided by this work.

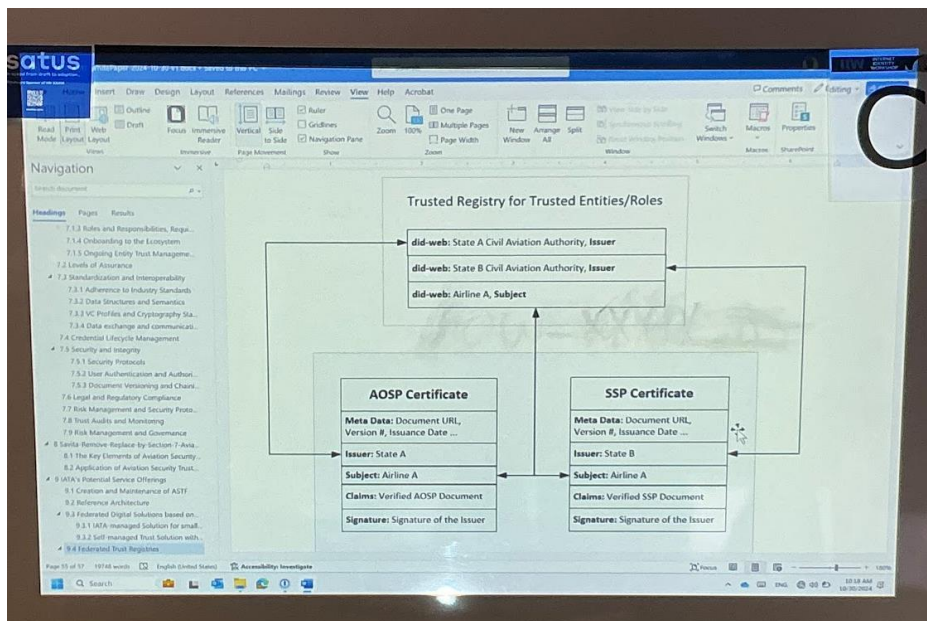


“4 P’s”: People, Process, Policy and Provenance

Could also supply a reference architecture

Create federated digital solutions based on the reference architecture for smaller countries to use

Manage the federated trust / trust registry across the nation-states



Need to figure out if wallets and verifiers need to be in this, too, not just the issuers... (same thing happening in academia/research)

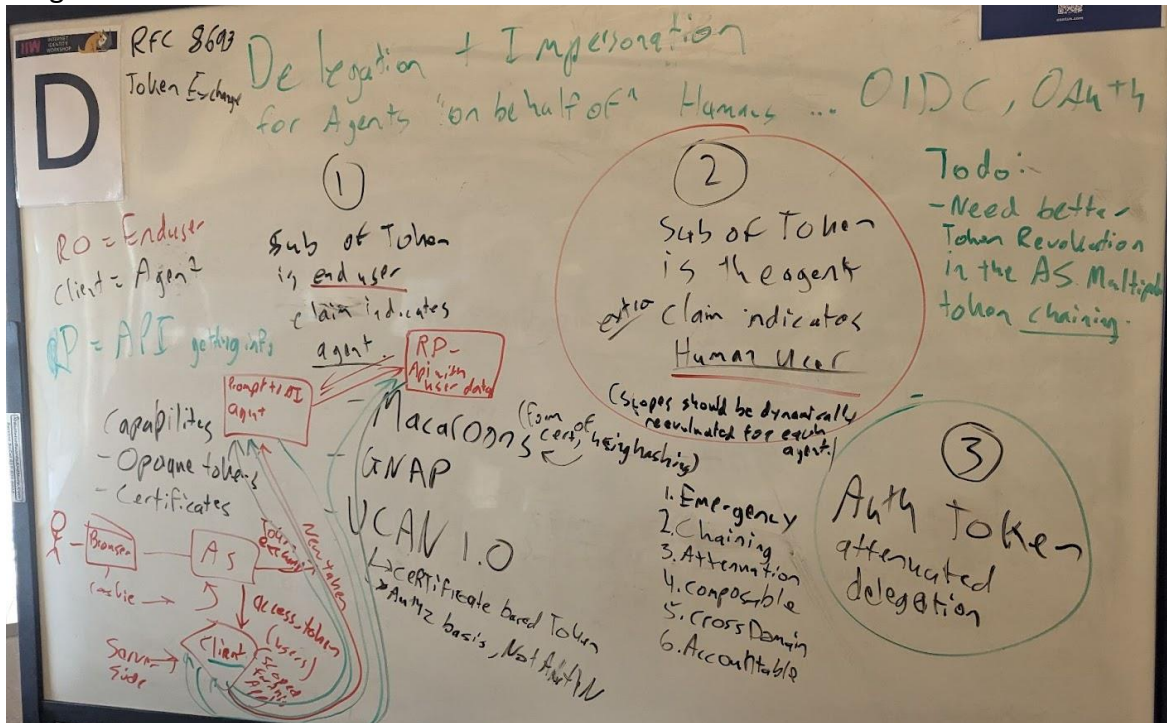
## Delegation & Impersonation for AI (and other) agents "on Behalf of" Human Users.... Token Focus

Session Convener: Paul Figura

Session Notes Taker(s): Paul Figura

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

- RFC 8693 OAuth 2.0 Token Exchange (DRAFT): <https://datatracker.ietf.org/doc/html/rfc8693>
- Diagram of discussion whiteboard:



- GNAP: <https://datatracker.ietf.org/doc/rfc9635/>
- UCAN 1.0: <https://github.com/ucan-wg/spec>
- Macarons: <https://research.google/pubs/macarons-cookies-with-contextual-caveats-for-decentralized-authorization-in-the-cloud/>

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

The main goal of this session to to invoke a discussion between the participants to understand the limitations of AI token impersonation/delegation using *current* OIDC infrastructure and API endpoints.

We specifically steered away from future solutions (such as GNAP and UCAN), since they are not currently implemented in any commercial Authorization Servers.

Additionally, while RFC 8693 was brought up as an example, this draft has not been ratified, and has not been updated since 2020, so it should be taken with caution.

- 2 main approaches to token impersonation
  - 1. Token contains the **sub** of the actual end-user, there is an additional claim in the token to indicate what the machine/agent account is.
    - This approach is simpler to apply for adoption's sake. Most RPs/RSs (APIs) will only care about the sub, which matches an actual user, and will return results to the agent with minimal changes.
    - However, this approach is more dangerous, as existing APIs that were not designed with impersonation in mind can just accept these tokens.
  - 2. Token contains the **sub** of the machine/user account. Additional claim “on behalf of” added to indicate who the end user should be.
    - This approach requires API endpoints to make minor changes to look into the new “on behalf of” claim to identify who the actual enduser being impersonated is
    - This is generally more safe, as these tokens will not really work (or have an impersonation effect on API endpoints that did not adopt this strategy.
    - This is also the same approach that is described in RFC 8693 in a token exchange scenario.
  - 3. *Third approach, attenuated delegation, is really just the same as option 2, with a caveat of only selected scopes get transferred to the impersonated token. Since we can do that in option 2 anyways, we decided this is not really an option.*
- Moving along, Using option 2 as the desired approach to evaluate, we were able to come up with a situation where:
  - a token is generated for the user after authentication to an standard server based application
  - This user invokes some logic in the server based application that would trigger an API call to an API Agent.
  - The server application makes an API call with the user token (actual token, no impersonation) to the the AI Agent.
  - The AI agent exchanges that token for an “impersonated token” with the enduser identity in the “on behalf of” claim.
    - Note: It’s also possible that the server based application can get the new token and send it directly to the AI Agent.
  - The AI agent then makes a call to an API, in the context of the impersonated user, and gets the data as that user. It forwards the data to the server based application, and is displayed to the user.
- There are some limitations to this approach, even if it works
  - There are no current functionalities in the current version of OIDC to mangle token session chaining further than the Refresh token/access token binding. Because of this, invalidating a token on the end user, doesn’t automatically invalidate the token being used by the AI agent,
    - Workaround: the server side application needs to manage extra complexity of session management, and keep all tokens in an internal table/graph and invalidate then in the correct hierarchy,

## State-Endorsed Digital Identity

Session Convener: Timothy Ruff (timothy@digitaltrust.vc)

Session Notes Taker(s): Jim Goodell (jim at INFERable.app)

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

Endorse, State, privacy-respecting,

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

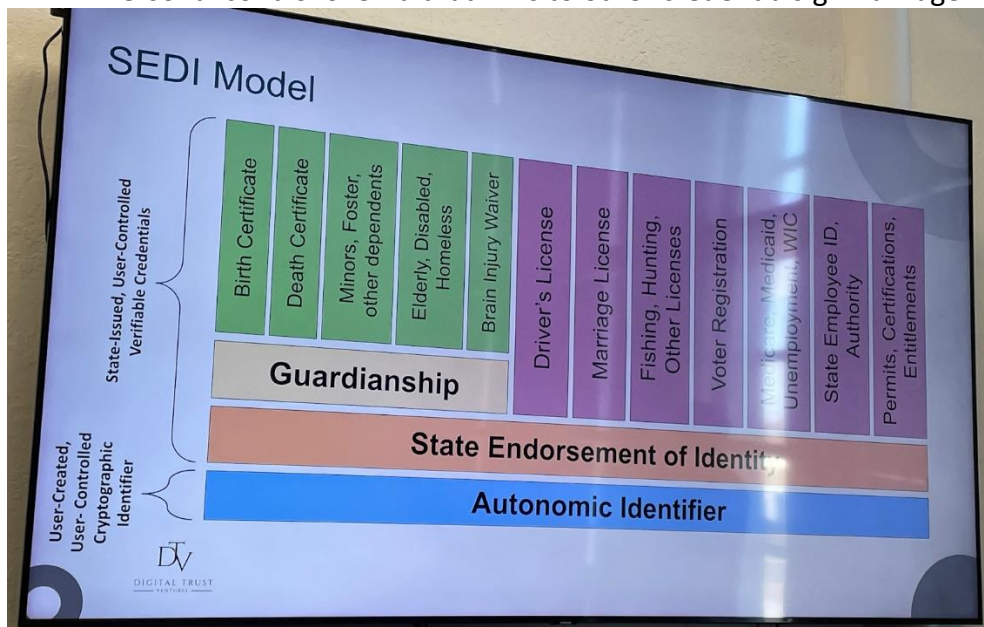
Link to slides: [State-Endorsed Digital Identity.pptx](#)

Model now possible with KERI technology. Key Event Receipt Infrastructure (KERI) protocol

- Most successful models in the digital realm mimic the physical world.
  - When a baby is born, the parents choose the identifier (the name) and the state endorses it with a birth certificate.
  - A model where the state issues the identity means the state controls that identity.
1. Autonomic Identifier generated by a person/entity (universally unique with cryptographic properties) (KERI Model)
  2. State endorsement
  3. Guardianship - KERI allows for multiple signers and power of attorney (over some VC, e.g. Birth & Death certificates)

Comments:


- This could be a problem not just for dependents but also for anyone that doesn't live in the identity space.
- Key concept (value prop from KERI) is portability of identity.
- Personal control over id that links to other credentials.g. Marriage License



Organisation:

## Principles & Goals of SEDI

Utility	Security	Autonomy
Usefulness & Flexibility	Verifiability (Zero Trust)	Privacy
Guardianship & Inclusivity	Mutual Authentication	No Surveillance
Comprehensiveness	Fraud Prevention	Consent & Control
Portability / Vendor Lock-in	Data & Systems Protection	Confidentiality
Paper & Offline	Recoverability	Least Disclosure
Adoptable & Easy to Use	Auditability	Transparency
		Recourse



- Governments want ALL of 1st 2 columns (on switch)
- Last column is cultural and (analog dial)

Questions/comments:

- Q: WHY would the government endorse a new identity when they have the mDL
- A: Can't do some of the utility features (e.g. Guardianship)

## What is SEDI?

SEDI enables residents to securely obtain, present and prove—under their discretion and direct control or that of legal guardians—any entitlements or responsibilities they may have, to anyone anywhere, without disclosing more than necessary and without enabling surveillance by government or any other disclosee, intermediary, or third parties.

Timothy Ruff opinion: mDL & ISO 18013 is surveillance. It has ability to turn on surveillance.  
*The ISO/IEC 18013-5 standard defines principles for the security and privacy of data used in Mobile Driver's Licenses (mDLs).*

## ***HumanOS Stack \* How you evolved your Digital Identity***

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

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

This session presented a thought model which intended to share and build language that could identify the various stages of relationship between human and connected information technology (IT) systems. It also looked to identify the different phases and details likely related to the different phases.

Visually this model is a pyramid type stack with five (5) levels. From the bottom up they are named @0, @1, @2, @3, @4. Each level represents a stage of the relationship. How you navigate, and the decisions you make in that journey, will form the digital DNA-building blocks of your digital identity. This will also impact on your ability to move through this landscape more in charge of, than owned by, the forces in this digital realm. In Real World (RW) we might ask;

“Who’s wearing the leash and who’s wearing the collar?” Are you taking tech out for a walk where you want to go or is IT taking you for a walk where IT wants to go?!

Over-simplified these stages would be roughly described as;

**@0: Before** - human experience with no exposure to connected systems. Examples may be newborn, deeply isolated cultures and all of us pre-1990’s. People who remember saying or hearing someone say, “Have you ever tried the web?” or “Have you been online yet?” would be what is known as a “digital immigrant”, per Marc Prensky. Those who’ve never heard such a thing said are likely “digital natives”, again per Prensky. They were born in a world where that relationship and entanglement has been a matter of fact mostly since birth. They were born into the stage of @1.

**Between @0 and @1** - is the Boundary Line of Awareness and/or Access. After this boundary is crossed in either or both senses, pure @0 is difficult to return to if not impossible.

**@1: Procreative Stage** - awareness of the digital landscape begins for many as a strong attraction which animates the idea of using connected systems. A key value of this stage may be that it delivers awareness that something new – a relationship entanglement – is in the room with you.

**@2: Developmental** – here the inevitable relationship with active systems forms. The Give & Take relationship surfaces rules, strengths and weaknesses present themselves.

Here the Real-IT<sup>®</sup> and the HumanOS<sup>™</sup> bloom more or less so based on numerous idiosyncrasies. Real-IT is the relationship we choose to have, or not to have, with information technologies and connected systems. *Your Real-IT relationship choices will reflect into your Reality.* The Key value here is understanding the synergy between the @0 world designed by

nature for people, and the forces impacting and influencing in your life @1. The HumanOS is reviewed in the next stage @3.

**@3: Maturation** – the refinement of the relationship begins. Crafting of your digital You begins to manifest driven by better understanding of the Real-IT<sup>®</sup> relationship and the HumanOS<sup>™</sup> perspective. Whether your digital twin will be more in your control - or more of a system's marionette - will reflect what does or doesn't happen at this level. Actionable sensibility is key here. Additionally, this level stays in touch and responds to the Give & Take relationship occurring @2. This is because systems are often changing and how we choose to respond affects choices we may make. At this level a person is ideally able to put their relationship choices, referred to as one's Real-IT<sup>®</sup>, into a proportion and balance that will allow for comfort and control and reflect comfortably into their Reality. The balance and degree of comfort achieved is related to the HumanOS's<sup>™</sup> alignment with the individual's wants and needs and how those intentions deliver positive outcomes to one's life.

**@4: Outcome** – How is Your Real-IT<sup>®</sup> reflecting Into Your Reality? How is your You-X\*<sup>™</sup>! The You as a Human having an eXperience related to technologies touching your day, and night - here and there...more or less... Key elements are;

**Control** – owning communication and command of the space

**Safety** – sense of Privacy, Security and respectfulness of those technologies

**Comfort** – how is the pace of the relationship considering all your feeds and accounts, etc.

How does the load feel? *Are you feeling accomplishment of your intentions without dodging or being impacted by hazard, loss or harm?*

Expanded Language Definitions:

\* **Real-IT<sup>®</sup>** – the relationship we choose to have, or not to have, with information technologies (connected systems) *Your Real-IT relationship choices will reflect into your Reality.*

\*\* **HumanOS<sup>™</sup>** – represents *the idea of an emulator mode in the sense that people try to align real world experience/wisdom with their Sense of Self (SoS) on the other side of the glass, @1.*

\*\*\* **You-X<sup>™</sup>** – The You eXperience (You-X) How you are doing having a leg on both sides of two different worlds. One world appears as wind, light, earth and gravity and another world on the other side of glass, which appears as a device screen. One side is a world that is built for us by nature, and one world is built for us by us and only accessible via crossing glass. The UX (User eXperience), a common phrase in software design, is regarding studying how people feel using IT systems. The You-X focuses on the experience of being a human with a foot in two different realms – the realm of natural world and a realm of human built system forces - on the other side of glass.

***Decentralized ID - Selective Disclosures - BLE! WORKS! - eID -Me = A Canadian View***

**Session Convener:** Steve Borza

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

***Digital ID toolkit: come give us feedback and learn how to play!***

**Session Convener:** Marianne Díaz Hernández

**Session Notes Taker(s):**

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

The Digital ID Toolkit <https://www.accessnow.org/whyid>

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



## *Scope and Role Granularity for Usability*

**Session Convener:**

**Session Notes Taker(s):** Michael Krotscheck

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

OIDC, OAuth2, AuthZen, FGA

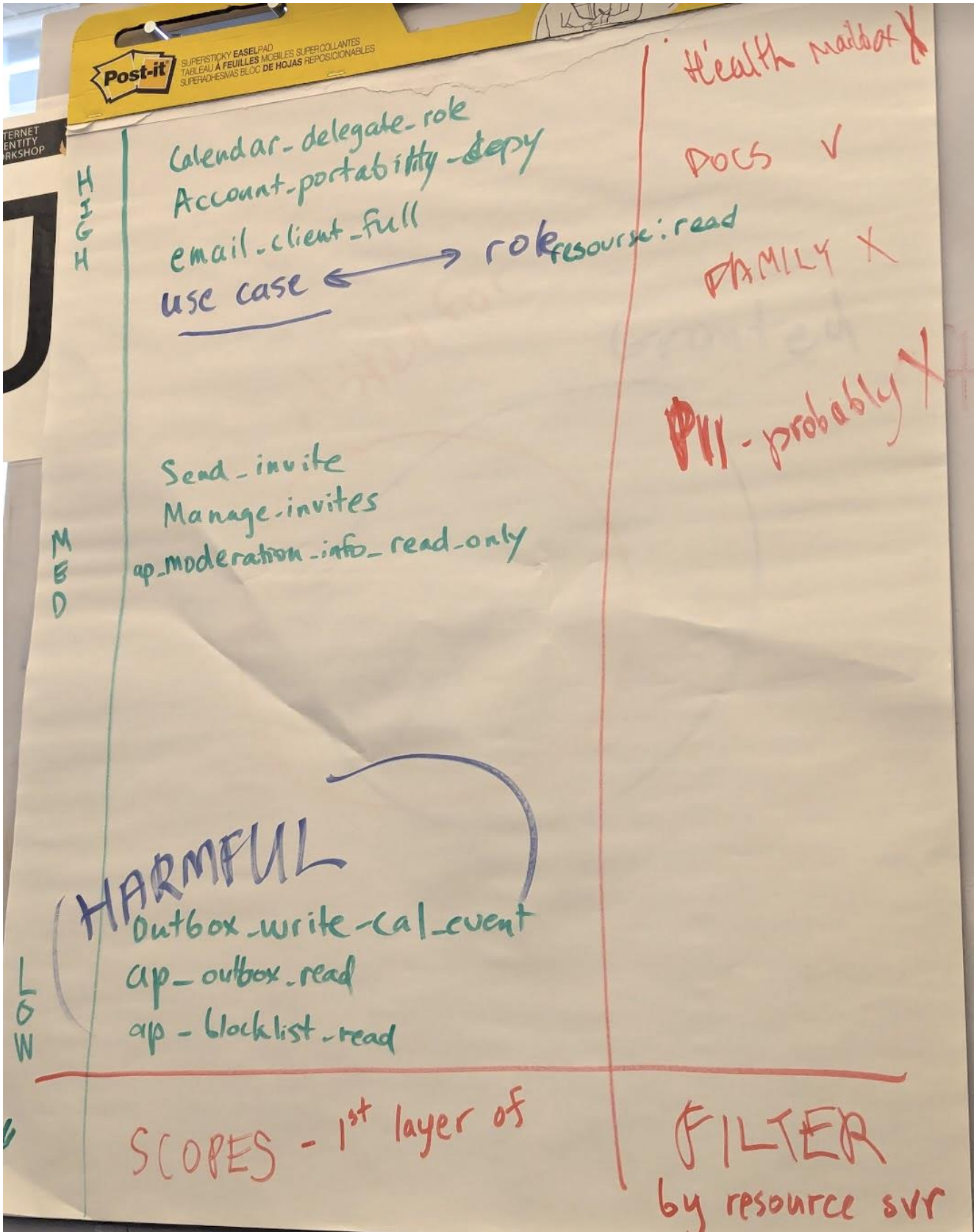
**Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:**

# Scopes and Roles Granularity for Usability

At what levels do you need to give access rights to satisfy different use cases?

- Email access to cofounders?
- Moving a profile across decentralized social networks?
- How do you ask a user for the scopes when there's scope explosion?
- How do you implement?
- If we don't do this, then people are going to build tools to simplify them and impersonate.
- How many of us actually look at the scopes that are asked for during a federation request? About half.
  - How many have declined a scope?
- A bit of history from Parecki.
  - OAuth started intentionally by not defining scope.
  - Scope Interop is usually not relevant because they're RP specific.
  - OIDC defines scopes (profile, email, address, etc.) and a re fine because we need cross RP Interop.
    - But the actual implementation is vague.
  - Scopes are strings without space, which means that they need to be predefined. Granular scopes
    - make for rapid scope explosion. (Health industry implemented a scope language).
- Then there's RAR, which is a scope-like mechanism.
- Was there ever any effort to document different scopes?
  - The closest we've gotten to is a colon separated string `resource:action`
  - In iOS they're getting pretty good about authorizing individual photos to an app.
  - On native devices this is all custom course, but Google and Apple have built an oauth based interop
    - mechanism.
- Scopes are there for a the client only, but the server MUST be the one that makes access decisions.
  - If a request from the application wants a family photo, but the server can reject that, and the resource owner can always revoke that permission.
  - Google Drive as an example: Which documents are evaluated on a request, not at authorization time.

- Tokens are intended to be consumed by the client, and should include enough information for the client to know what they can do.
- Concrete example: Expensify
  - First iteration lets you pick emails.
  - AI version will scrape things from email.
    - AI Engineer doesn't want to have too much access.
    - Customer does not want to give too much access.
- You cannot use scopes to control FGA.
- Email example:
  - Level one: You have no scopes, full access.
  - Level two: You can offer read or write access.
  - Level three: You can offer access per email, label, category, etc.
  - An email app doesn't need calendar access.
- Enterprise software has grown to raise roles to the level of well understood personas and use cases. Use case is a payroll system.
  - Can we quantify and create a registry of roles like this? HR Manager role, etc...
  - Are we conflating interop and roles?
  - The lower level you go, the less usable it gets because things are too specialized by use case.
  - Roles tend to gather finer grained permissions.
- What is the median number of scopes observed in the wild?
  - 3 or higher?
- If you have an FGA system, why do you need scopes at all?
  - You might not.
  - As a communication to the client on how the token can be used.
- How does this then apply to the enterprise example.
  - Am I logging in as an employee or manager? Which hat do I want to wear, as a scope?
- Nobody's arguing to include fine-grained scopes in the token.
- Every application has a way to create custom roles, allowing an admin to remix permissions.
- An internet draft can be written with more guidance? Like a BCP?
- Where do you draw the line between OAuth and AuthZen?
- You don't always want to run with all of your permissions/roles/etc at all times.
  - Can you do selective scope expansion?
- What about regulation?
  - We don't do use-case based scopes because we don't want to be slapped by a regulator.
  - The actual implementation pattern for engineers is that they keep adding more permissions, which means that a regulator will need to keep up with things.
  - If you offer a finer-grained scope, business competition will pick you apart in lawsuits on what you can or cannot do.
    - There's a balance - if you go too fine grained, your competition will call that out. If you are too coarse, then there's permission bleed.
- Scopes are a first layer of protection.



## ***SSB Intro to Secure Scuttlebutt (10+ years and more)***

**Session Convener:** Christian Tschudin  
**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 First Person Credential***

**Session Convener:** Drummond Reed, Andre Kudre, Marcus, Brad Degraf, ...  
**Session Notes Taker(s):** Darius Dunlap

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

Why we need first person credentials on the net - Doc Searls  
<https://projectvrm.org/2014/03/19/why-we-need-first-person-technologies-on-the-net/>

Personhood: The Killer Credential? - Eve Maler  
<https://workshop.vennfactory.com/p/personhood-the-killer-credential>

Personhood credentials:  
Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online (Research Paper with multiple authors)  
<https://arxiv.org/pdf/2408.07892>

First Person Credentials: Solving Proof of Personhood with Verifiable Relationship Credentials and the GAN - Drummond Reed, Brad deGraf and many other contributors  
[First Person Credentials: Solving Proof of Personhood with Verifiable Relationship Credentials and the GAN](#)

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

How do we tell we're a real person online, without a massive privacy problem.

MDL Drivers licences and Government IDs are being adopted. Concern that "give me your MDL" will become a standard ask, which has all kinds of privacy problems.  
Need a strong proof of personhood, with privacy preservation.

“We have 18 months before the web is completely unusable, so we need a solution.”

- Paper is under revision (See Above)

Core DNA of a “verifiable relationship credential”

- We already have the social ceremony we need. Person-to-person using methods as simple as a QR code (WeChat, LinkedIn, et. al.)
- See whiteboard diagram snapshot for the flow

Any DID-based protocol could use these VRCs for connection between these two “people”.

There is a paper on this, about 35 pages long currently, talking about how it all works, [here](#).

Then, through the GAN, these users can register their relationship and establish an FPC (First Person Credential)

Liquid Democracy

Delegation of voting power / Representation

See demo at: <https://greencheck.world>

THOUGHTS

Could this facilitate the “current best way to reach me” lookup that Tantek has through his website?

- Yes, and more

More notes from Eric S at: [Session 6L: First Person Credentials](#).

## ***UR CODES Turn “BEARER” Documents -> Biometric-Bound Documents!***

**Session Convener:** Andrew Hughes

**Session Notes Taker(s):** Andrew Hughes

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

URCodes.com    dev.facetec.com

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

- UR Codes are a new product from FaceTec.com undergoing market discovery now
- Andrew gave an overview of what UR Codes are and what they can represent
  - UR Codes are plain old QR codes that contain name-values (hopefully including a licence number, record number or similar), a 72 byte face biometric template - all the data is signed by the issuer

- This means that the person can prove that the UR Code matches their face and because of the digital signature, the person is linked to the licence number and the issuer.
- Lots of good challenging questions and discussion about the nature of biometric systems (they use machine learning and neural network models)
- MOSIP and Tech5 have created similar approaches except they use a small low res picture of the person instead of a biometric template
- Discussed potential scenarios

## What are UR<sup>®</sup> Codes?

They may look familiar, but these QR codes contain digitally signed biometric data and enable privacy-preserving Identity Verification. UR Codes enable codeholders to prove, with high confidence, their legal identity, age, and right to access their accounts or privileges, both in-person and remotely. Because they store unique, signed face data, personal info, and legal identity data, UR Codes enable secure, low-cost, two-party identity verification at unlimited scale.

UR Codes can be used in ANY identity-related scenario and from ANY Issuing Authority (DMVs, passport issuers, schools, employers, etc.) to immutably bind Anyone's biometric data to their identity data.



**UR<sup>®</sup> Driver License**



**UR<sup>®</sup> Passport**



**UR<sup>®</sup> Business Card**



**UR<sup>®</sup> Student ID**



UR Codes provide similar privacy-protecting biometric security to e-Passports, but without the usability/durability problems, or the exorbitant costs associated with scannable NFC chips. UR Codes can also store additional biometric data, along with the face data, including fingerprint data or iris data.



Encode your own Demo UR Codes Here: [encode.urcodes.com](https://encode.urcodes.com)

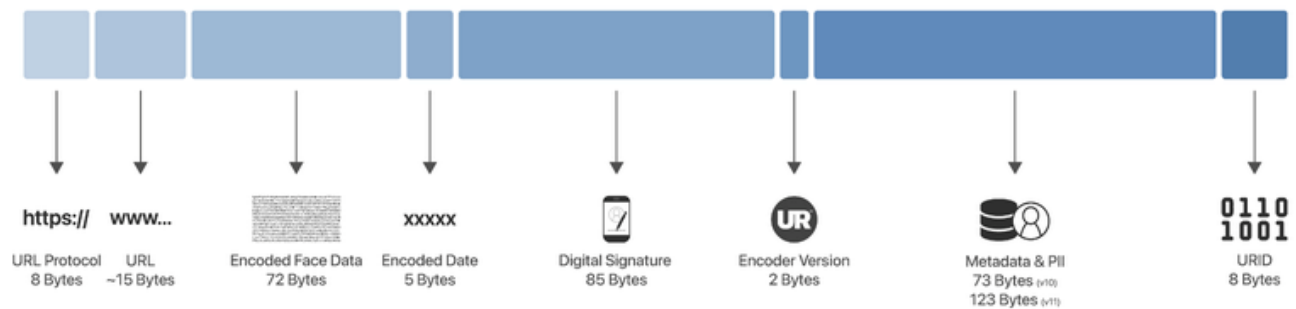
More information on UR Codes can be found here: [Facetec.com/Intro\\_to\\_UR\\_Codes.pdf](https://Facetec.com/Intro_to_UR_Codes.pdf)

Additional Technical Information can be found here: [dev.facetec.com/urcodes](https://dev.facetec.com/urcodes)

## How are UR<sup>®</sup> Codes Created?

UR Codes are generated by Issuing Authorities using secure UR Encoder software that runs inside the firewall of that Issuing Authority. Using a unique Public/Private Encryption Key pair, the software cryptographically signs each UR Code, making them provably immutable.

## What's inside a UR<sup>®</sup> Code?



## Typical UR<sup>®</sup> Code: 61x61 Matrix

Digital Signature = 85B  
Encoded Face Data = 72B  
URL = Average Length ~15B  
Unique URID# = 11B  
URL Protocol (https://) = 8B  
Encoded Date = 5B  
Encoder Version = 2B



**Required UR Code Bytes = ~198**

**Characters Available for User PII = ~123**

(Name, Address, Driver License #, Passport #, Email, 2nd face data, etc.)

If fewer than 73 Characters of User PII are required, the UR<sup>®</sup> Code will be 57x57 (v10). If more storage is required it will be set to 61x61 (v11) and store up to ~123 Characters of PII.

## ***OpenID Foundation FAPI 101***

**Session Convener:** Nat Sakimura, Joseph Heenan, Daniel Fett

**Session Notes Taker(s):**

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

OpenID FAPI working group:

- <https://openid.net/wg/fapi/>

Recorded talk on the same topic: <https://danielfett.de/talks/2024-04-01-fapi2-high-security-oauth-whats-the-latest/>

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

About 20 people attended the session.

The session used the slide deck [1] to explain that FAPI is a prescriptive profile of OAuth for interoperability and security. It has been formally verified for its security property and is now deployed in many countries. It also comes with a conformance test suite. FAPI 1 Final was published in early 2021. Since 2020, the WG is working on FAPI 2, which is close to being published as Final as well in Q1 2025.

[1]

<https://docs.google.com/presentation/d/1CvGFvHQL4VY5pScGdUXejCisaLieTue7ATJX7A4R8u4/edit?usp=sharing>



## SESSION #7

### *FedID / FIDC*

**Session Convener:** Ben Curtis  
**Session Notes Taker(s):** JIm Fournier

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

<https://fedid.me>  
<https://www.jlinc.com>

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

An online representation of you, that you own and control.

**FedID** is the root technology behind **FedID Connect (FIDC)**, which leverages the portability of OpenID Connect (OIDC) and distribution of ActivityPub to provide usernames and identifiers that individuals own and control, no matter what happens to the site they signed up on.

We took attendees through the creation of a **FedID** on a mobile device, and its use to login to an existing tool that already supports OIDC, and thus, **FIDC**.

**Available as of the first day of IIW:**

- Detailed documentation, DID format, and protocol overview: <https://fedid.me/about>
- Flutter library: <https://fedid.me/libraries/flutter>
- Containerized server infrastructure: <https://fedid.me/server>

**We have released the FedID DID server / DID resolver under an MIT + no surveillance licence**

## The Laws of Externalized Authorization

Session Convener: Omri Gazitt

Session Notes Taker(s): Omri Gazitt

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

Presentation [slides](#)

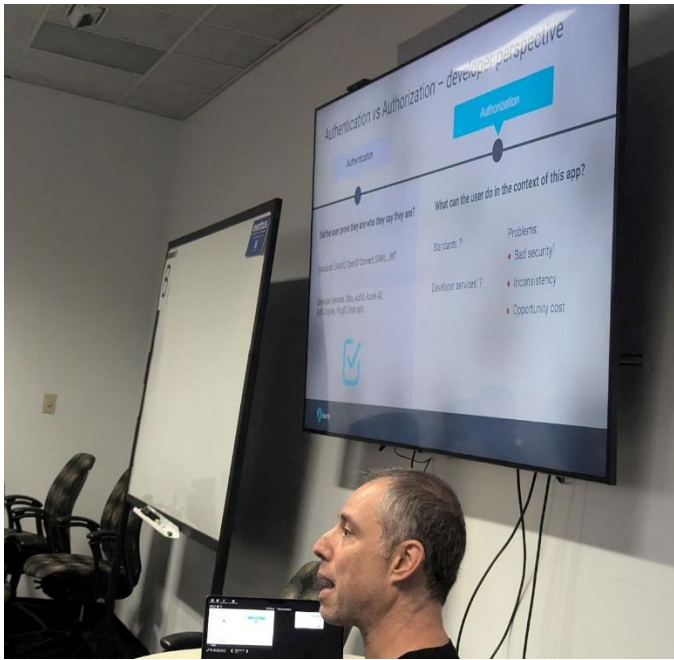
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

5 laws of authorization

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

Rohit's photos:





## Trust Network Design Session

Session Convener: Andor Kesselman

Session Notes Taker(s):

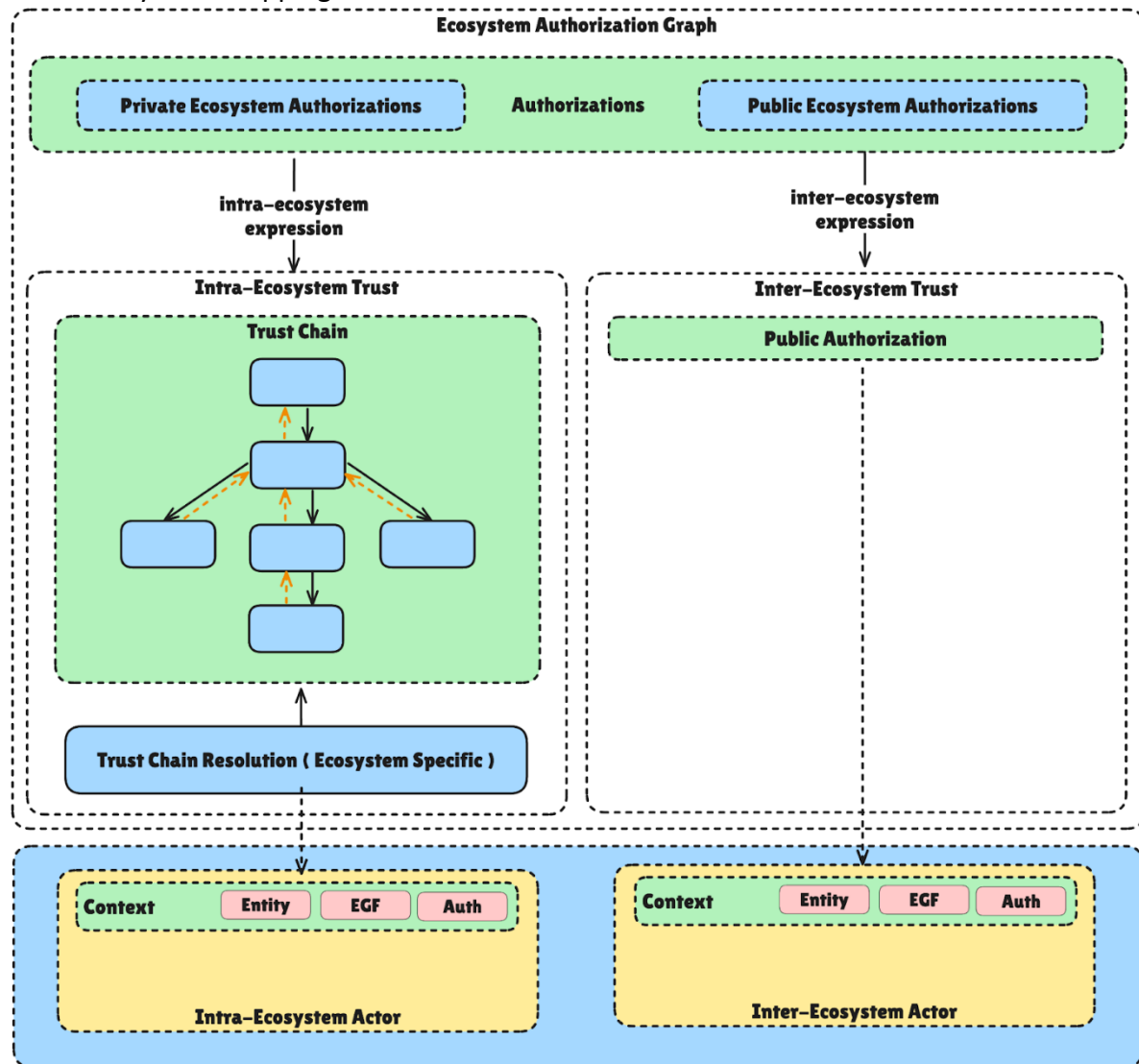
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

We discussed Trust Network Design. Reference diagram shared on whiteboard.

Ultimately, what is the data model for a query into a trust network:

Subject, Predicate, Object + Authentication Context

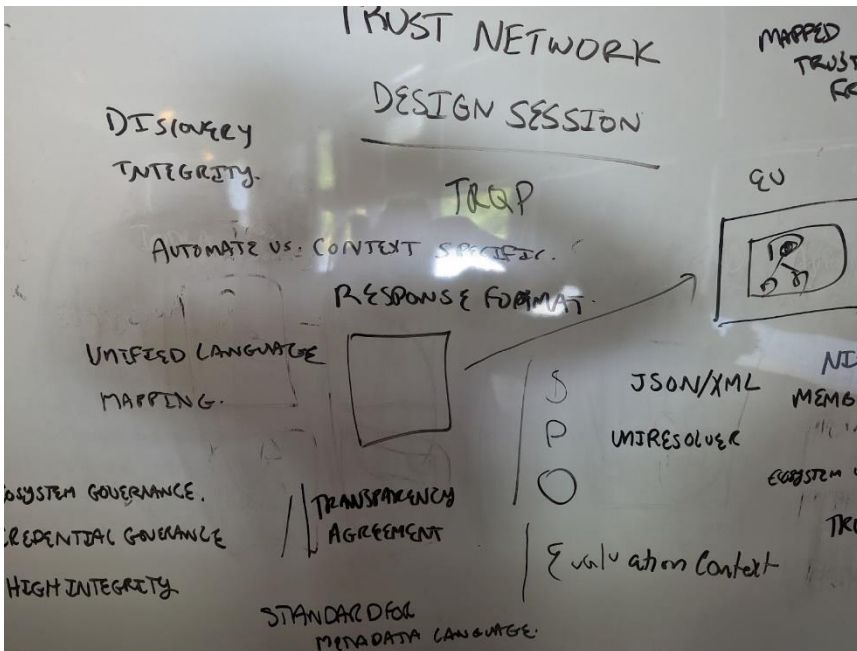
Cross Ecosystem Mapping :



Public v.s Private Authorization Space is not the same.

Discussed multiple problem statements:

- discovery
- integrity
- unified governance mapping
- ecosystem governance
- credential mapping
- Similar work is happening in uniresolver.
- Automatic vs. Context Specific.
- Work that NSTIC did:
  - transparency
  - agreement
  - Standard metadata governance
- Request vs. Response Forms
  - We may need to focus on response forms.



## SESSION #8

### *Google's ZKP for MDOCs*

**Session Convener:** Abhi Shelat / Matteo Frigo

**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 and Agent Overview @ OWF*

**Session Convener:** Mirko Mollik

**Session Notes Taker(s):** Mirko

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

<https://openwallet-foundation.github.io/digital-wallet-and-agent-overviews-sig/#/>

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

Presentation of the general overview

- showing the new features like wallet and agent dependencies and case studies
- It should help visitors to find the best fitting wallet based on their requirements
- Table is based on objective comparison values

Explanation of the generation of it

- IIW session from 3 years ago -> Credential Format comparison SIG at the OpenWallet Foundation
- TNO and Findynet started with an excel overview -> moved it to a SIG at the OpenWallet Foundation
- Both SIGs got merged recently because of their overlapping
- Multiple providers submitted pull request to add or update their wallet or agent for the overview.

## ***Dude (Person), Where's Your DID? (An update on how individual and organizational identity fits into the C2PA ecosystem)***

**Session Convener:** Eric Scouten

**Session Notes Taker(s):** Eric Scouten

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

Slides: <http://ericscouten.dev/2024/iiw39/#session-8c-dude-person-where-s-your-did>

(scroll down for PDF link)

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

I gave a brief overview of the C2PA data model and then explained the CAWG (Creator Assertions Working Group) framework for allowing content creators to add their own identity attestations to content they create.

The framework roughly translates as: “The actor described by  $\${credential}$  using a credential issued by  $\${issuer}$  produced the content described by  $\${signer\_payload}$ . Signed by:  $\${credential\_holder}$ .”

These placeholders can be filled in with different data types depending on the kinds of credentials available to the content creator. We spent most of the discussion talking about the recently-introduced model of identity claims aggregation which allows a trusted third-party to gather identity claims (proof of control over social media accounts and web sites as common examples) and link them to the content created by the same actor.

**“Verifiable AI”: Content credentials, proof of personhood, proof of “approved AI agent” and more**

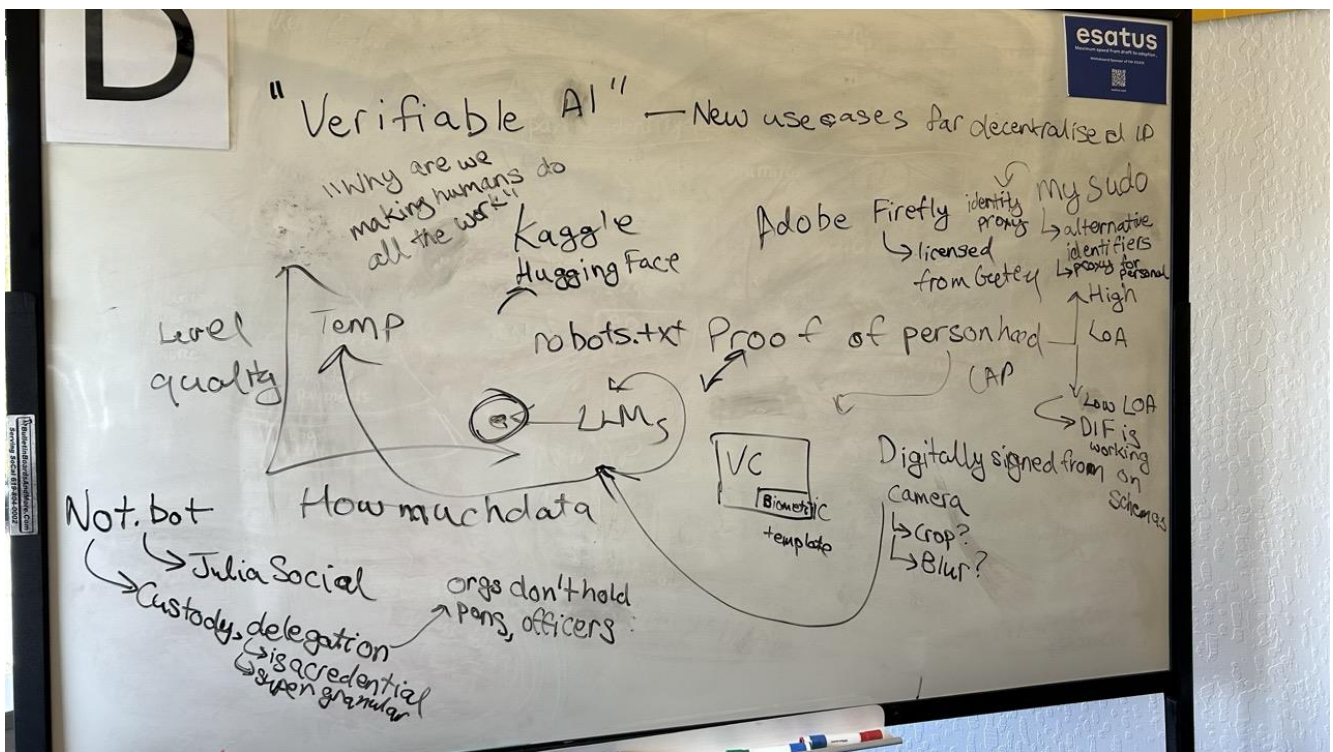
Session Convener: Ankur Banerjee, [Kim Hamilton Duffy](#), Linda Jeng, [Steve McCown](#)

Session Notes Taker(s): [Ankur Banerjee](#)

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

[DIF Hackathon: Verifiable AI](#)

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





## *Personalized AI*

**Session Convener:** Jim Goodell and Neil Thomson  
**Session Notes Taker(s):** Jim Goodell, Neil Thomson

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

[Hospitality and Travel Wallet & AI.pdf](#)  
[Personal Data “Shipping” Considered Harmful.pdf](#)

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

Multiple models:

- Federated query (so API access to personal data stored elsewhere)
  - Rather than Services storing all their customer data on their servers, query for customers data profile directly from their Digital Wallet on an on-demand basis.
- Time-limited access (used for individual interactions or a session but must be discarded after)
- Distributed processing (some decisions on local machine or personal space / processing, some on GPT)
- Send only personal data needed for the decision.
- Agent model: The agent is in your own sandbox and issues a request to the big AI and there is an agent firewall
- “Focused lending of data” – the contract is when the session is over to drop the data
- Privacy Obligation Document (POD) metadata sent with data including perishability
- GDPR implementations need to evolve to forgetability and to minimize the attack surface. Minimise risk of hacks/breach of personal data
- Ari: Question– What are the use cases?
  - Selective health data disclosure (accessibility needs, vaccinations, etc.)
  - K-12 Education – parents concerned about tutor bots (e.g. ChatGPT-based) having personal info, other kinds of non-LLM data may also apply
- Sam Johnson (piAI): Hard part is if the human needs to control access, but if the AI agent can decide based on some rules
- Categorization intelligence gives “temperature” about what each variables need or helpful, then ask for the variables based on the potential value
- Sam from (Qui(sp?) – piAI-OS) piAI pre-run self-controlled cosign similarity search – need to have arms around your full learning experience than use what’s needed.
- “Data Guardian” is specifically trained to protect personal data on your own device or in your private cloud space.
- Another important factor, we don’t try to be the system of record (e.g., if AI is based on email conversations we don’t copy the emails, just create the vector based on the source).
- Adding personal data for an LLM is known as “embedding.”

## Device Profile as a VC for Device Recognition

Session Convener: Rudra Pandrap  
Session Notes Taker(s):

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

Type Here

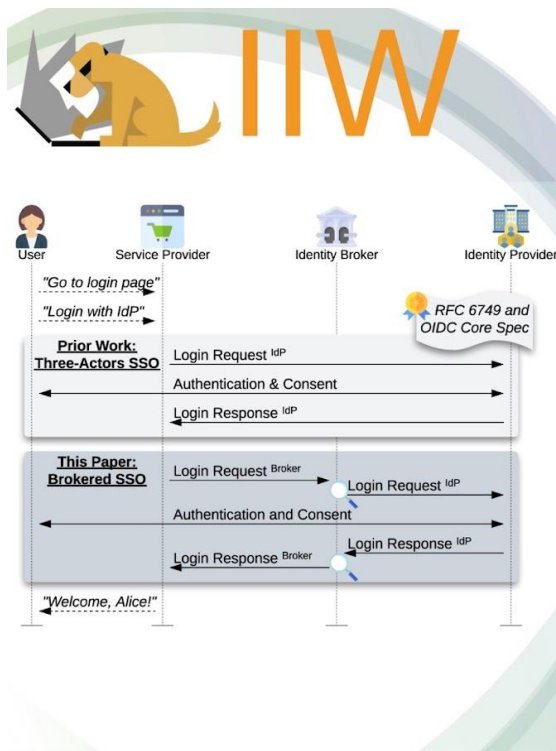
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

NO NOTES SUBMITTED

## Identity Brokers in OAuth

Session Convener: Tommaso Innocenti  
Session Notes Taker(s):

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



IEEE S&P

**“Only as Strong as the Weakest Link”:**  
On the Security of Brokered Single Sign-On on the Web

*Tommaso Innocenti, Louis Jannett, Christian Mainka, Vladislav Mladenov, Engin Kirda (Appearing in S&P'25)*

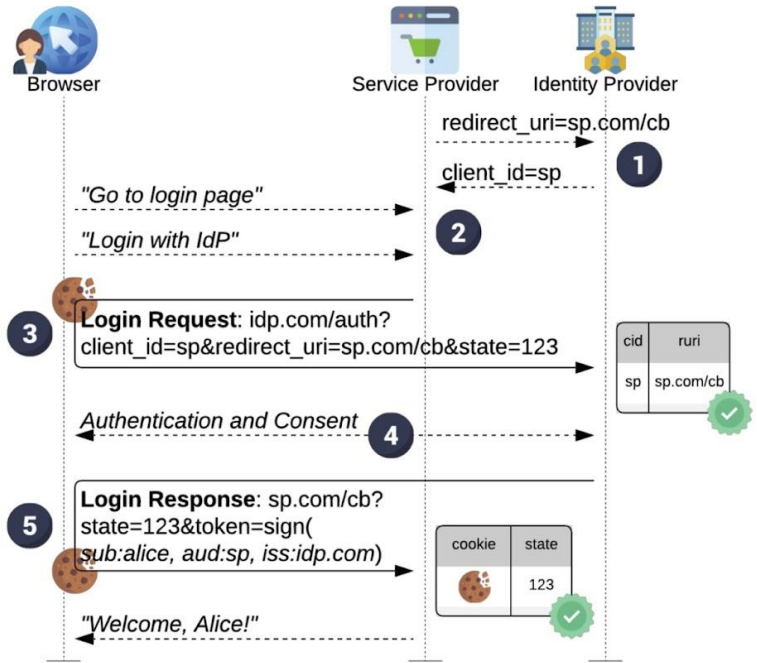
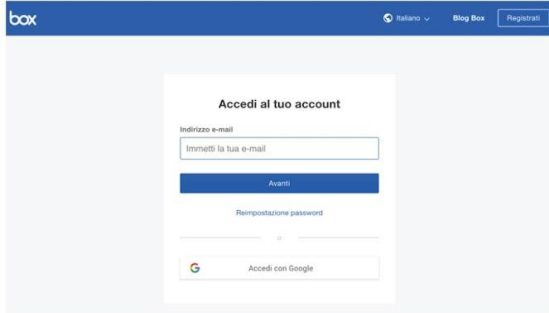
# Traditional SSO Flow:

Registration phase

1

Login flow

2 3 4 5

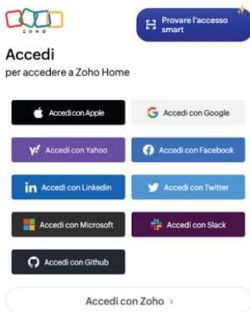


# Traditional SSO Flow

vs.

# Brokered SSO Flow:

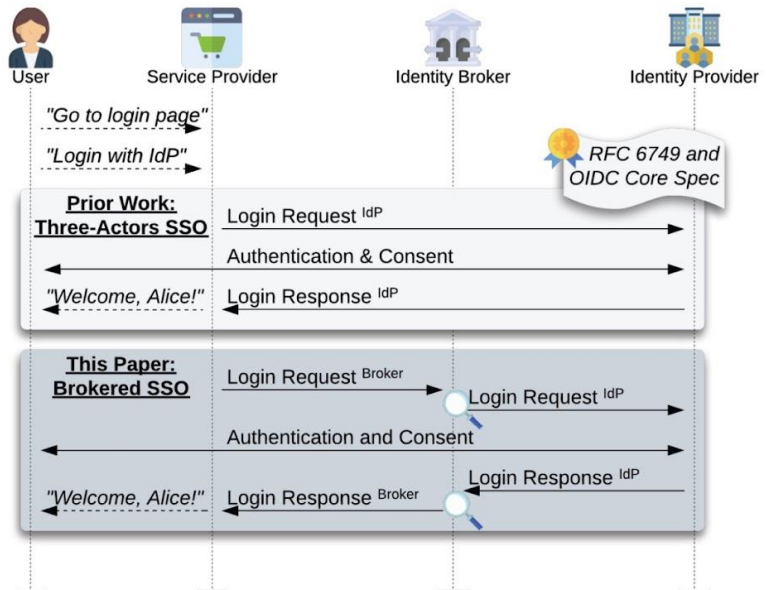
- Identity Brokers in the login flow



Autenticazione a più fattori per tutti gli account

Proteggi gli account online con l'autenticazione a due fattori OneAuth. Effettua il backup delle OTP segrete e non perdere mai accesso ai tuoi account.

Ulteriori informazioni



# Methodology



## Identity Brokers Systematization

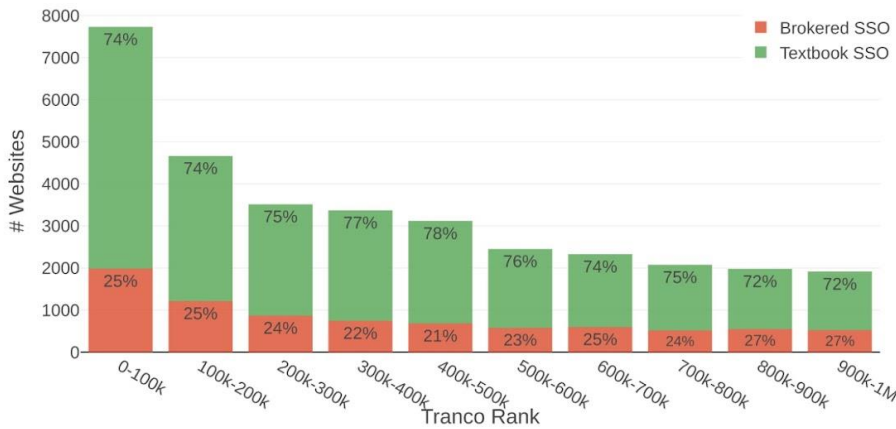
SP relation: First-party or Third-parties

Audience: Public or Internal

		# Brokers		# Flows		# Websites	
<b>Three-Actors</b>		-	-	39,870	72%	24,880	75%
<b>Brokered</b>	Public	64	26%	10,911	71%	5,944	72%
	Internal	117	47%	3,442	22%	1,635	20%
	Unknown	68	27%	1,139	7%	686	8%
		<b>249</b>	<b>100%</b>	<b>15,213</b>	<b>28%</b>	<b>8,241</b>	<b>25%</b>
<b>Three-Actors or Brokered</b>				<b>55,083</b>	<b>100%</b>	<b>33,121</b>	<b>100%</b>



## Brokered SSO adoption



The percentage of websites using a brokered SSO is constant among the Top1M Tranco list (~25% of SSO)



## Brokered SSO Flow Major Problems:



One Consent for 4 Actors



Client ID Reuse

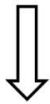


Login Request / Response Confusion

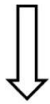


### One Consent for 4 Actors

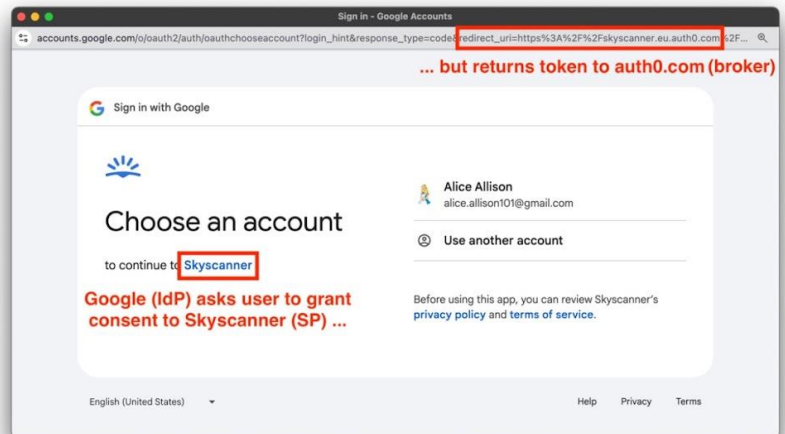
Two logically chained OAuth flows  
but only one consent prompt



Two consent prompts introduce  
friction in the login flow and can  
confuse the users



All consent prompts in Brokered  
SSO hides the presence of the Identity Broker



# Client ID Reuse

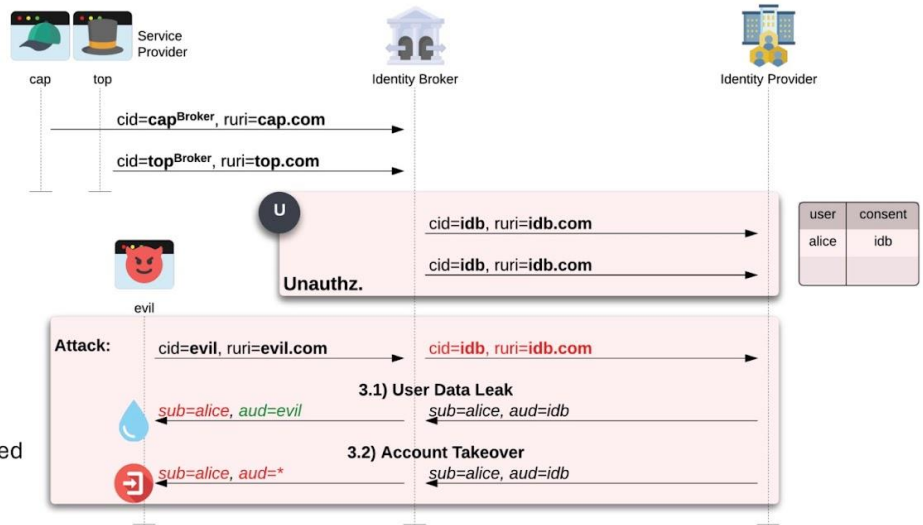
Identity brokers only use one Client ID for all SPs



- User's information Leak
- Account Takeover

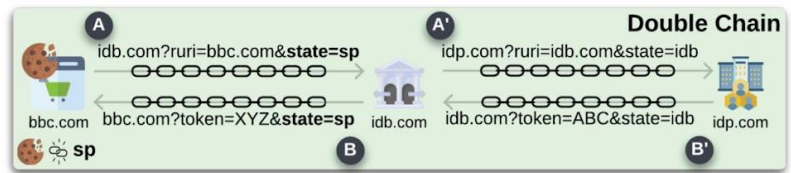
15 Identity Brokers vulnerable to user's information leak

6 Identity Brokers issued unscoped authorization token



# Correct chain scheme Brokered SSO

The double chain scheme allows a correct implementation of the Brokered SSO

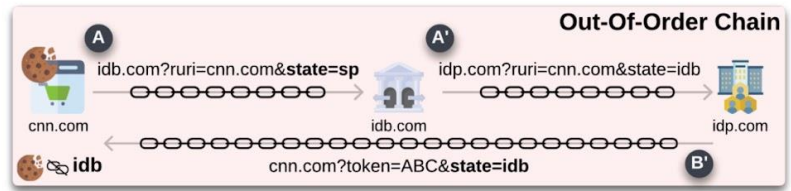


## Login Request / Response Confusion

Out-Of-Order chain scheme blocks the correct parameter validation, exposing the login flow to the LoginCSRF attack



69 Brokered SSO flows used the Out-Of-Order chain scheme

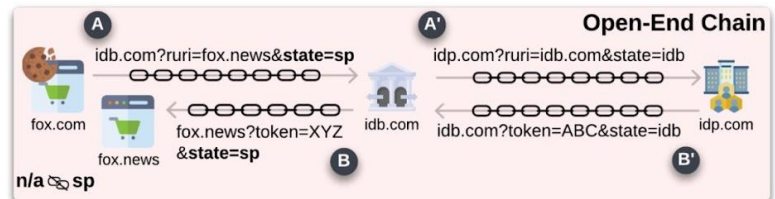


## Login Request / Response Confusion

Open-End chain scheme blocks the correct parameter validation, exposing the login flow to the LoginCSRF attack



57 Brokered SSO flows used the Open-End chain scheme



# Best Current Practice

- 1,872 violations on 2,780 websites
- Identity brokers remove PKCE, exposing brokered SSO to LoginCSRF and token leak



Identity Brokers actively downgrade the security of the login flow.

	# Flows (Total: 5,668)			# Websites (Total: 2,780)		
	IdB	SP	Secure	IdB	SP	Secure
❶ Insecure Flows	0	1,034	4,634	0	545	2,235
❷ Secret Leaks	0	0	5,668	0	0	2,780
❸	Missing PKCE	2,954	2,698	16	1,505	1,273
	Invalid PKCE	0	89	5,579	0	41
	→ no code	0	17	5,651	0	9
	→ reuse	0	84	5,584	0	36
	→ entropy < 128 bit	0	35	5,633	0	13
→ invalid method	0	39	5,629	0	17	
❹	Missing state	7	1,021	4,640	7	543
	Invalid state	8	704	4,956	4	306
	→ reuse	8	697	4,963	4	300
	→ entropy < 128 bit	0	141	5,527	0	78
❺	Missing nonce	93	2	5,573	93	1
	Invalid nonce	305	1,866	3,557	263	858
	→ no id_token	304	1,786	3,578	262	846
	→ reuse	1	138	5,529	1	67
	→ entropy < 128 bit	0	25	5,643	0	18
<b>Σ Total Violations</b>	<b>3,367</b>	<b>7,415</b>	<b>-</b>	<b>1,872</b>	<b>3,568</b>	<b>-</b>



## Improving the OAuth 2.1 and OAuth Security Best Current Practices can mitigate the presented issues

- The consent page in the presence of Identity Brokers should inform the user of this intermediary actor in the login flow
- Introduce the requirement of using separate Client\_ID for each Service Provider when the intermediary (Identity Brokers) obtains a Client\_ID from an Identity provider.

Workgroup: Web Authorization Protocol  
Internet-Draft: draft-ietf-oauth-security-topics-29  
Updates: 029, 030, 031 (if approved)  
Published: 3 June 2024  
Intended Status: Best Current Practice  
Expires: 5 December 2024

T. Lodderstedt  
SPRIND  
J. Bradley  
Public  
A. Lawares  
Independent Researcher  
D. Jett  
Authlete

**OAuth 2.0 Security Best Current Practice**

**Abstract**  
This document describes best current security practice for OAuth 2.0. It updates and extends the threat model and security advice given in RFC 6750, RFC 6758, and RFC 6759 to incorporate practical experiences gathered since OAuth 2.0 was published and covers new threats relevant due to the broader application of OAuth 2.0. Further, it deprecates some modes of operation that are deemed less secure or even insecure.

**Discussion Venues**  
This note is to be removed before publishing as an RFC. Discussion of this document takes place on the Web Authorization Protocol Working Group mailing list (oauth@ietf.org), which is archived at <https://mailarchive.ietf.org/arch/browse/oauth/>. Source for this draft and an issue tracker can be found at <https://github.com/oauthlist/draft-ietf-oauth-security-topics>.

**Status of This Memo**  
This Internet-Draft is submitted in full conformance with the provisions of RFC 79 and RFC 78. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress." This Internet-Draft will expire on 5 December 2024.

**Copyright Notice**  
Copyright (c) 2024 IETF Trust and the persons identified as the document authors. All rights reserved. This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/permissions/>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Workgroup: OAuth Working Group  
Internet-Draft: draft-ietf-oauth-v2-1-11  
Published: 16 May 2024  
Intended Status: Standards Track  
Expires: 16 November 2024

D. Hagg  
Mellon  
A. Paretz  
Oleks  
T. Lodderstedt  
jps.com

**The OAuth 2.1 Authorization Framework**

**Abstract**  
The OAuth 2.1 authorization framework enables an application to obtain limited access to a protected resource, either on behalf of a resource owner by authenticating an approval interaction between the resource owner and an authorization service, or by allowing the application to obtain access to its own behalf. This specification replaces and obsoletes the OAuth 2.0 Authorization Framework described in RFC 6750 and theBearer token usage in RFC 6757.

**Discussion Venues**  
This note is to be removed before publishing as an RFC. Discussion of this document takes place on the OAuth Working Group mailing list (oauth@ietf.org), which is archived at <https://mailarchive.ietf.org/arch/browse/oauth/>. Source for this draft and an issue tracker can be found at <https://github.com/oauthwg/oauth-2-1>.

**Status of This Memo**  
This Internet-Draft is submitted in full conformance with the provisions of RFC 78 and RFC 79. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress." This Internet-Draft will expire on 16 November 2024.

**Copyright Notice**  
Copyright (c) 2024 IETF Trust and the persons identified as the document authors. All rights reserved. This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/permissions/>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the

## A specification extension (specific use case) can confidently outline the correct implementation of Brokered SSO.





# Identity Brokers facilitator....at what cost?

## Standards have two “customers”: end-user and companies

- Identity brokers are the result of failing one standard’s “customer”.

→ **companies**

## Identity brokers help companies, but at what cost?

Open the discussion of the alternative and what we can do as a research community to solve the problem.



Thanks for your attention.

Our research artifacts:



<https://zenodo.org/records/13918427>



### “Only as Strong as the Weakest Link”: On the Security of Brokered Single Sign-On on the Web

Tommaso Innocenti  
Northeastern University  
Boston, MA, USA  
innocenti.t@northeastern.edu  
ORCID: 0000-0003-0247-806X

Louis Jannett  
Ruhr University Bochum  
Bochum, Germany  
louis.jannett@rub.de  
ORCID: 0000-0001-5448-5929

Christian Mainka  
Ruhr University Bochum  
Bochum, Germany  
christian.mainka@rub.de  
ORCID: 0000-0002-4273-645X

Vladislav Mladenov  
Ruhr University Bochum  
Bochum, Germany  
vladislav.mladenov@rub.de  
ORCID: 0000-0001-9208-9281

Engin Kirila  
Northeastern University  
Boston, MA, USA  
ek@ccs.nyu.edu  
ORCID: 0000-0001-9988-6873

**Abstract**—Single Sign-On (SSO) is an authentication process that allows users to access multiple services with a single set of login credentials. Although SSO improves the user experience, it poses challenges to developers to implement complex authentication protocols securely. External services, called brokers, simplify the integration of SSO. In this paper, we shed light on the emerging brokered SSO ecosystem, focusing on the security of the newly introduced actor, the broker. We systematically evaluate the landscape of brokered SSO, uncovering significant blind spots in previous research. Our study reveals that 25% of the websites with SSO integrate brokers for authentication, an area that has not been covered by any previous research. Through our comprehensive security evaluation, we identify three categories of threats associated with brokered SSO: (1) insufficient validation of redirect chains enabling injection attacks, (2) unauthorized data access enabling account takeovers, and (3) violations of security best current practices. We expose vulnerabilities in over 50 brokers, compromising the security of more than 2k websites. These findings represent only a lower bound of a critical situation, underscoring the urgent need for improved security measures and protocols to safeguard the integrity of brokered SSO systems.

**1. Introduction**  
Single Sign-On (SSO) is a widely used and extensively adopted user authentication technique for websites. Each year, more websites adopt SSO services to manage user identities, in order to reduce the significant burden of signing up and signing in on their sites. This trend is reflected in the forecast of the market share of identity management services, which is expected to reach 43 billion US dollars by 2029 [30]. Prominent providers of SSO services include

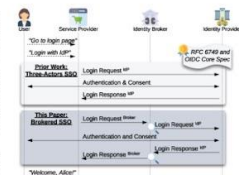


Figure 1: Three-Actors SSO vs. Brokered SSO. Three-actors SSO involves a user who wants to log in to an SP’s website by using their account at an *IdP*. Brokered SSO involves an additional actor called *linker* that mediates between the SPs and *IdPs*. This way, SPs implement only one broker while supporting SSO logins with multiple *IdPs*.

social networks such as Facebook, Twitter, and Snapchat, as well as large enterprises such as Apple, Google, and Microsoft. Together, these SSO services are utilized by more than 45k websites within the Franco top 1M sites [34]. The research community also recognizes the importance of SSO and is continually working to detect and mitigate security issues [24, 31, 33, 34, 48, 51, 64]. Additionally, the IETF regularly updates the Security Best Current Practices (SBSPs) to address the state-of-the-art research [39, 59].

**Three-Actors SSO.** Until now, the SSO security re-

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

Notes from nicole:

<https://www.igtf.net/snctfi/>

<https://www.economyofmechanism.com/office365-authbypass.html>

SAML proxies/brokers, check out the “AARC Blueprint Architecture”, CILogon <https://cilogon.org>, eduTEAMS, etc.

email: [nroy@internet2.edu](mailto:nroy@internet2.edu)

[https://openid.net/specs/openid-federation-1\\_0.html](https://openid.net/specs/openid-federation-1_0.html)

<https://technical.edugain.org>

“Try it out for yourself” - sign up for an account on <https://spaces.at.internet2.edu>

## ***Identity and the Social Web***

**Session Convener:** Johannes Ernst <https://j12t.org>

**Session Notes Taker(s):** Chris Messina

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

<https://fediforum.org>

<https://fedidevs.org>

<https://dazzlelabs.net>

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

A re-occurrence of a meta network is emerging (e.g. after AOL, eBay, etc in the 90s)

Identity isn't working well in the modern context

Use cases for identity on the social web:

- shareable/discoverability: @Cocacola on a billboard
- recognizable: distinguish people in various contexts, like Amazon reviews
- provable: attribution

What do we need to identify?

- IRL: people, groups, places, organizations...
- Virtual: accounts, groups, places, agent, "AI"
- Something in both: "Amazon"

## Solutions:

- DNS
- domains (costs)
- subdomains
  - challenges: longevity, re-use, sale, historical record, a kind of deadnaming
- Cryptographic identifiers
- DIDs
- Public keys (nostr)
  - challenges: illegible
- QR Codes
- Email addresses
- Bridges mangle identifiers
- WebFinger & discovery
- Graph of identifiers (Linktree etc)

## Other challenges

- public vs private vs semi-public or semi-private identities
- forward-linking content
- payments, ads
- name collisions
- name squatting
- group vs individual identity
- disposability
- contextual identity; probabilistic identity based on "vectors", assertions
- behavior-based identity
- opt-in vs opt-out
- scalability
- IPv6 vs usernames
- home addresses — street address vs w/o locality
- how do I assert my own identifier(s) vs applied to me
- biometric
- sovereignty
- inverse identity: blocking as reverse connecting
- opt-in follows
- social web as system of record or as live medium?
- chat groups vs feeds
- private groups vs public contexts
- network of network sprawl
- cautionary tale: XMPP, Spokeo
- how essential is the usability of identifiers?
- federated systems spend too little time on cross-system user stories
- two big problems: key recovery and economics
- incentives
- how to decentralize user engagement data (in order to create ad-sponsored media)?
- how much do people pay each month for internet access/cell phone bill?

***Why is the OpenID Foundation hopping right now? An overview of the 14 work groups and community groups on now***

**Session Convener:** Nat Sakimura + Gail Hodges

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

***DWeb Deep Dive and Web 5 / OWN Updates + Wallet***

**Session Convener:** Daniel B and Liran Cohen

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

## ***Portable Communities***

**Session Convener:** Brad DeGraf

**Attending:** Christian Tschuxdin , Joseph Huntsinger, Jeff D HumanOs, Grant Bierly internet2, Charles Lanahan,

**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:**

Brad:

- Membership rules by smart contract
- Scuttlebutt edges
- Governance mechanisms between groups
- Keri acdc
- computer language constitution  
crdt conflict free replicated data types
- email [bdegraf@gmail.com](mailto:bdegraf@gmail.com) if you want to continue in a working group
- on [Linkedin](#)
- DSL - domain specific language

## ***Adopting OAuth2.0 for First-Party Applications - Building the Authentication Layer***

**Session Convener: Janak Amarasena**

**Session Notes Taker(s): -**

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

Slide deck:

- View: [https://github.com/janakamarasena/iw-sessions/blob/main/IIW39/OAuth2\\_FiPA-Authentication-IIW39-2024B.pdf](https://github.com/janakamarasena/iw-sessions/blob/main/IIW39/OAuth2_FiPA-Authentication-IIW39-2024B.pdf)
- Download: [https://github.com/janakamarasena/iw-sessions/blob/main/IIW39/OAuth2\\_FiPA-Authentication-IIW39-2024B.pdf?raw=true](https://github.com/janakamarasena/iw-sessions/blob/main/IIW39/OAuth2_FiPA-Authentication-IIW39-2024B.pdf?raw=true)

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

- The session focused on how you build the authentication layer required when adopting the OAuth 2.0 for First-Party Application (<https://datatracker.ietf.org/doc/draft-ietf-oauth-first-party-apps/>)
- Talked about an interactive authentication API capable of handling any authentication mechanism in a generic manner. (API details available in the slide deck)
- Expectations of the API
  - Describe what data is needed to proceed with user authentication
  - Provide info for the app to build the UI representations
- Discussed the following aspects of the API
  - Generalizing the authentication requirements
  - Handling federated login
  - Dealing with multiple authentication options
  - Supporting localization for application UI representations
  - Related endpoint discovery from the API such as providing a link to user registration
- Discussed why such a complex api is needed
  - Handling the complexity at different level: app, SDK, API
- Discussed the benefit of getting early feedback when designing such a API
- Showed a recorded demo of the user experience in an application which has incorporated the API
- Went through a end to end example incorporating the authentication API with the OAuth 2.0 for First-Party Applications specification

## Secure Technology Alliance - Mobile Driver's License (mDL) Jumpstart

Session Convener: Carolyn Manis Sorensen, Tony Loprieto  
Session Notes Taker(s): “

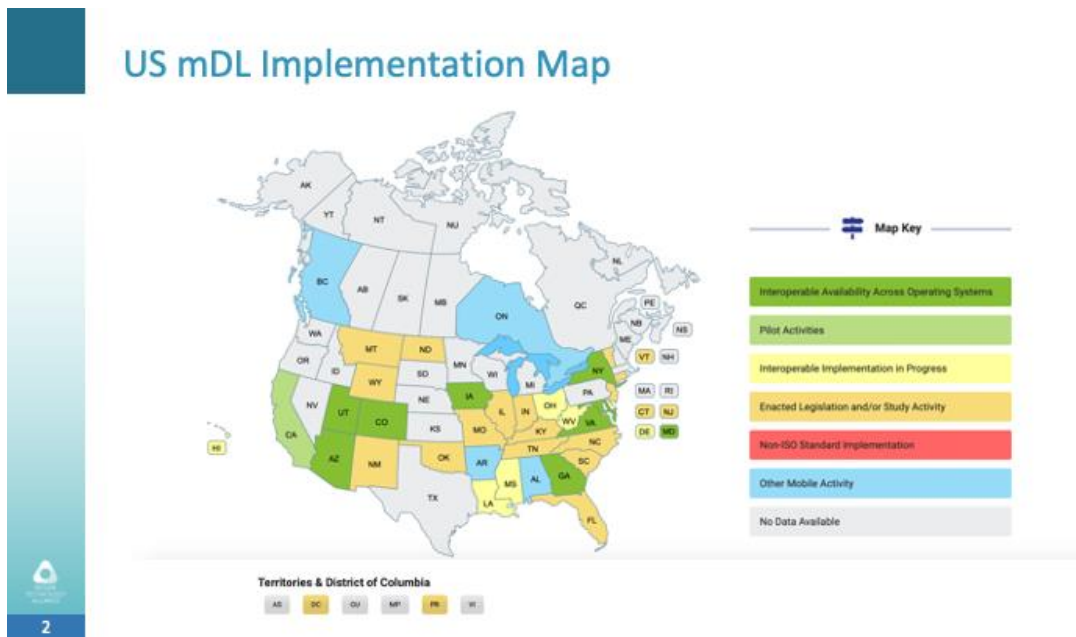
Tags / links to resources / technology discussed, related to this session:

Mobile Driver's License (mDL) Resources: <https://www.mdlconnection.com/>  
STA Identity & Payments Summit - Feb 24-26 in San Diego CA: <https://www.stasummit.com/>

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

Some Discussions:

1. Why mDL? Isn't that for "can you legally drive"? But in the US, is the generally universal identity document (or id card issued by the DMV/DLD)
2. Should there be a federal digital ID program, and what is the relationship between the state-issued mDLs and acceptance at federal government institutions
  - a. NIST NCCoE support for use cases and demonstration of value, working with Issuers, Tech Providers and Relying Parties



# STA mDL Technology Showcase

## STA Identity & Payments Summit

Feb 24, 2025

Demonstrate real world use cases of mDL value  
mDL Jumpstart Working Groups searching for tech  
provider and relying party partners  
Participation and demos for attendees across  
wider STA membership



6

## mDL Committee: 5 Use Cases to Jumpstart Adoption

mDL in...

01	<b>Banking &amp; FIs</b>	<ul style="list-style-type: none"><li>In-Person mDL Acceptance in the Branch</li><li>Production Implementation experiences</li></ul>
02	<b>Alcohol Age Verification</b>	<ul style="list-style-type: none"><li>Connections to NLLEA and NABCA</li><li>State Liquor Control Board participation</li><li>Quick, unforgeable age verify with privacy</li></ul>
03	<b>Online Identity Verification</b>	<ul style="list-style-type: none"><li>Account Opening/KYC</li><li>Freeze/Unfreeze Credit</li><li>High Risk Transaction</li></ul>
04	<b>Casino &amp; Gaming</b>	<ul style="list-style-type: none"><li>Real world rollouts are already happening</li><li>Demonstrate benefits to individual and business</li></ul>
05	<b>Retail &amp; Payment</b>	<ul style="list-style-type: none"><li>Integrations Into Point of Sale are possible</li><li>Privacy-preserving audit trail</li></ul>

Yes, we will encourage other use cases



7



*How does a person's agent talk to an RP*

**Session Convener:** Paul Trivithick

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

## SESSION #9

### *RP Authentication and Authorization for the EUDIW (European Union Digital Identity Wallet)*

**Session Convener:** Torsten Lodderstedt, Giuseppe DiMarco

**Session Notes Taker(s):** Nicole Roy

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

Need to be able to know who the RP is because you might have to communicate with them, potentially file a lawsuit against them, etc.

Full transparency for relying parties with users (required by law)

Critically, the RP needs to authenticate with the wallet, and the wallet must check to ensure that the data requested is within the scope of what the RP said it needed and registered with the member state.

Non-repudiation of the issuance of an RP authn request also required (RP must sign request).

Authorization Requirements

- PID & EAA providers may govern access to PID (Personal Identification Data, the state-issued ID) / EAA (Electronic Attestation of Attributes (everything else)) data through embedded disclosure policies.
- Policy must be matched to RP role/permission attestation

Goal: Enable informed decisions of users, but do not restrict the user's decisions.

Options for implementation:

- X.509
- OpenID Federation
- (SD-)JWTs as attestations

How it's done in Italy with OpenID Federation (Giuseppe):

Every entity is able to say whatever they want about themselves: "This is my configuration"

Entity is joined to the Italian federation, which is joined to the EU federation. The entity is also in federations (X) and (Y)

Other entities know who they trust (what federations they trust, etc.)

The federation publishes subordinate statements to declare stuff about entities in their federation. The subordinate statement can do things like place restrictions on subordinate entities' configuration statements.

The Italian digital identity wallet uses a trust chain that is "just the stuff in the Italian federation"

Trust chain allows policies to be changed in realtime, dynamically, without needing to revoke millions of credentials.

The request of the wallet must contain the entityID of the RP. The wallet evaluates the relevant trust chain(s) of that entityID according to the wallet's trust requirements.

Discussion of where the trustmarks need to go in order to enable the queries of RPs to succeed- needs to go in the entity configuration.

DCQL - digital credential query language

Trustmarks get sprinkled like fairy dust on entities by a third party that is authorized to do so by a superior.

(long debate about whether or not we call what the wallet does when it evaluates the RP's trust chain and trustmarks and query and it's self-asserted requirements for data use, "authorization")

It's really dangerous to assume that all RPs are legal entities - example include non-legal-entity multijurisdictional scientific collaborations. Sometimes these go beyond state or national boundaries.

### ***Interoperable, Private and Feature-rich?! Tru.net The new town center built on JLINC w/Fed DID's / Simply Sharing Credentials***

**Session Convener:** Jim Fournier, Ben Carson, Tonia Abdul, Golda Velez

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

## BYOC - Bring Your Own Use Cases - Whatever! Real or Imaginary

Session Convener: Seth Kwon

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 - Oh My! Practical 101 on RAG Architectures and what it means for Identity

Session Convener: Alex Olivier

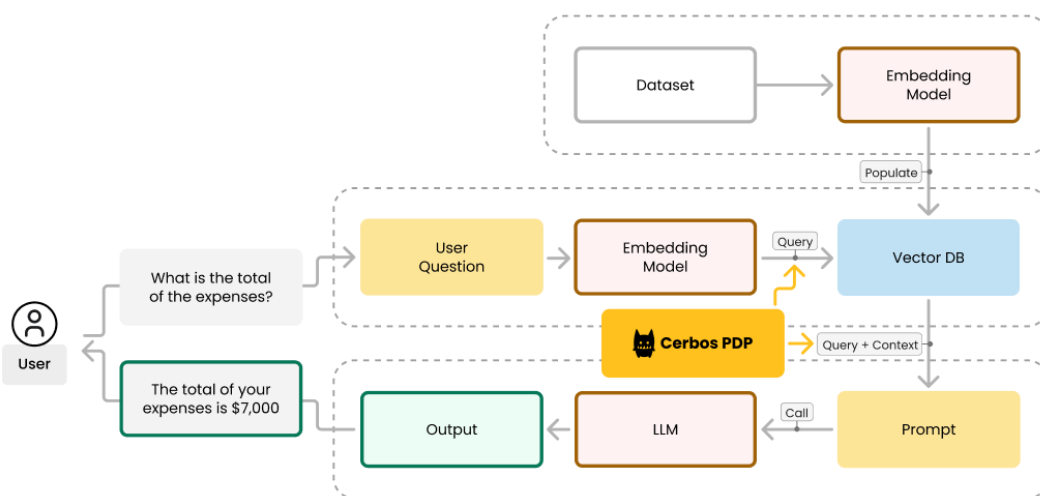
Session Notes Taker(s): Alex Olivier

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

- Cerbos
  - <https://cerbos.dev>
  - <https://github.com/cerbos/cerbos>
- ChromaDB - <https://www.trychroma.com/>
- Ollama - <https://ollama.com/>
- Llama - <https://www.llama.com/>

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

Record version <https://www.loom.com/share/024f12be6b6a4cf192e327ec5537c838>



## ***Intro to Originator Profile***

**Session Convener:** Shigeya Suzuki  
**Session Notes Taker(s):** (same as above)

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

Originator Profile: <https://originator-profile.org/en-US/>

Presentation:

[https://drive.google.com/file/d/1uLiXRjLSQxiry5kR1\\_X6uvaUwFOv3sZf/view?usp=sharing](https://drive.google.com/file/d/1uLiXRjLSQxiry5kR1_X6uvaUwFOv3sZf/view?usp=sharing)

Video: N/A (will be available at the above OP site in the future)

FAQ is now available (as of Nov 1st):: <https://originator-profile.org/en-US/faq/>.

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

Shigeya played an introductory video of Originator Profile (OP from now on), then described the project using the slides above.

There was a question and answer session.

Q: Is there a way to revoke?

A: Yes, but as it is optimized for media fragments (texts, pictures, etc.), it will have a key revocation mechanism alongside the key roll, but it will not provide a way to revoke media fragments one by one.

Q: Since this is a web site that relies on HTML and CSS, I think it is possible to inject code that pretends to be the user interface of the OP. Are there any countermeasures?

A: Currently, no countermeasures in this context are the same as other Web-based contents. Web Payment-like approach might be possible.

## ***Open Source AI***

**Session Convener:** Sam Johnston

**Session Notes Taker(s):** You?

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

Open Source Declaration: <https://opensourcedeclaration.org> (<https://osd.fyi>)

Open Source Definition: <https://opensourcedefinition.org>

Open Source Discussion: <https://discuss.opensourcedefinition.org>

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

Type Your Notes Here

## ***Accountable Wallet - A wallet can prove your legitimacy using VC's ZKP's***

**Session Convener:** Masato Yaman

**Session Notes Taker(s):**

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

[Accountable Wallet - IIW IIWXXXIX Fall 2024.pdf](#)

[BGIN Overview.pdf](#)

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

## The Business of Enterprise Identity

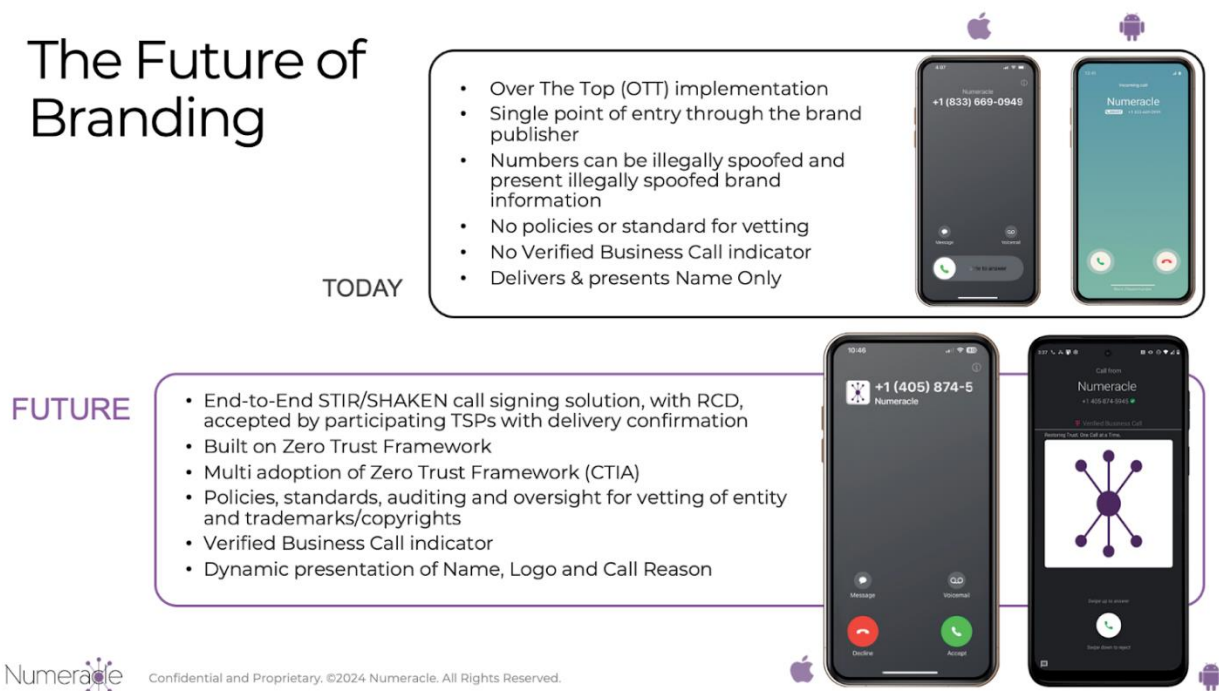
Session Convener: Sam Etler & Rebekah Johnson  
Session Notes Taker(s): Sam Etler

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

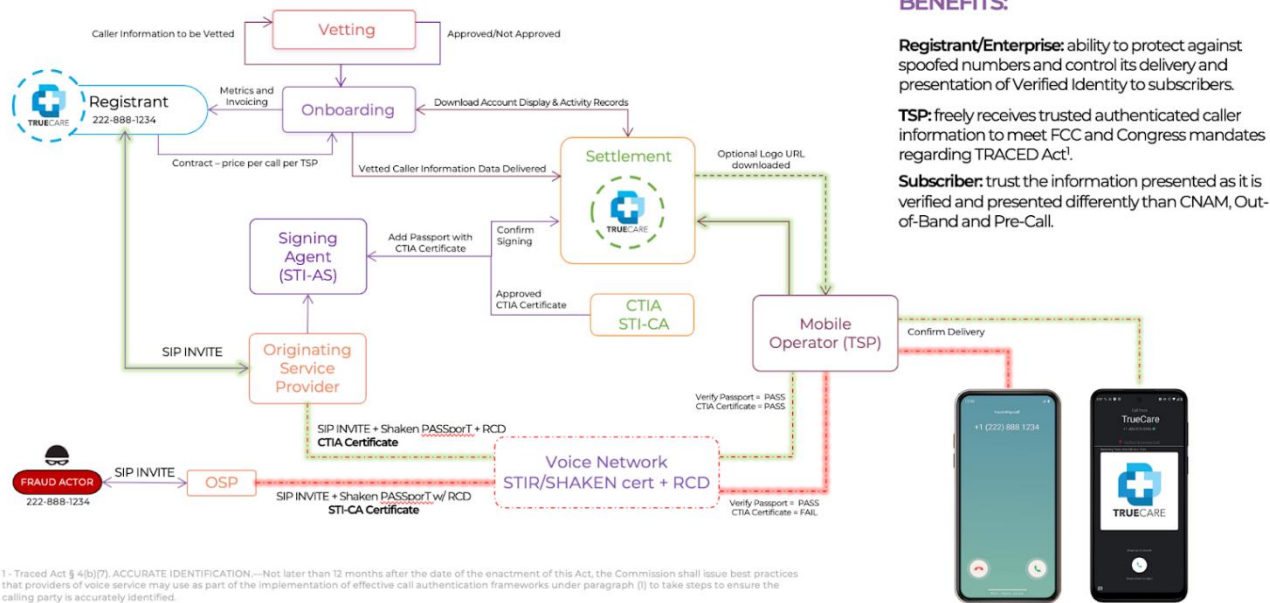
<https://www.numeracle.com/solutions/secure-verified-identity-presentation>

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

Rebekah gave a presentation describing the CTIA BCID branded calling identification ecosystem. Went into the high level reasons why business identity is needed in the telecom world (loss of trust in the network due to robocalling, traditional caller name systems are susceptible to spoofing attacks) and dove into the technical aspects and high level financial aspects. The ecosystem relies on trusted entities doing vetting of enterprises, onboarding their information such as name, logo, and reason for calling into the network, and then secure signed call headers to transmit this data to participating service providers. This allows for the display of this information on handsets along with a “verified call by...” from the terminating service provider. A live demo was performed on both an iPhone and an Android device. It was also discussed that this is relatively new technology, having gone into production at the beginning of Oct. 2024. There is a huge opportunity for end to end verified credentials for individuals.

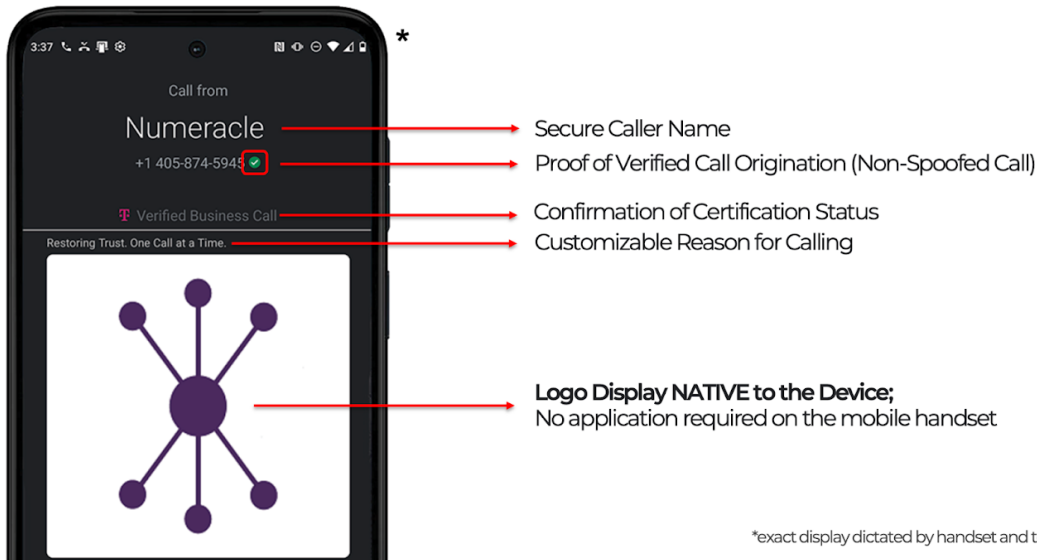


# Complete In-Band Delivery of Verified Identity + RCD



## Identity that Cannot be Displayed Without Authorization

Taking the initiative to define, establish, and transmit end-to-end verification





## ***Personal AI on Digital Public Infrastructure***

**Session Convener:** Reza Rassool

**Session Notes Taker(s):** Darius Dunlap

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

<https://www.kwaai.ai/>

See also:

<https://security.apple.com/blog/private-cloud-compute/>

<https://machinelearning.apple.com/research/homomorphic-encryption>

<https://machinelearning.apple.com/research/introducing-apple-foundation-models>

<https://machinelearning.apple.com/research>

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

Reza went through his overview presentation for Kwaai, explaining the mission, traction and growth of the community, some definitions, showing how it works, the advantages of RAG and the way they are addressing certain limitations so far. Much of this can be found at the Kwaai.ai website.

Most of the rest of the session was discussion and questions and answers.

## *World ID Proof of Human (WorldCoin)*

**Session Convener:** Adrian Ludwig, Ajay Patel

**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:**

- Want to support more than one credential type
- Not a trust protocol
- 2 questions relying party can ask today with World
  - Are you human?
  - Have I seen you before?
- How to map digital ID to national frameworks
- Anyone should be able to build an “orb”
- Orb scans and sends iris code to the phone
- Geographically, philosophically distributed secure multi-party compute so that any kind of compromise would require that all of them would need to be compromised simultaneously. Right now, there’s 7 different organisations but the intention is to increase that number.
- Being able to scan using an iPhone is really close, right now, it’s not possible because some hardware is not available, like infrared illumination
- Ticketing for concerts/events, proof of humanity for gaming
- Intention is to be 100% open source and open standards
  - Wallet is not currently open source
  - Elements that relate to keys/are proprietary

## ***UX For SSI Products***

**Session Convener:** Janet Gonzales  
**Session Notes Taker(s):** Janet Gonzales

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

- Designing UX for two KERI-based products, GLEIF's v1 Keep and healthKERI's MVP
- designspells.com = Great website for looking at simple animations

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

Creating a good SSI user experience depends on knowing your users, interaction design with your users in mind.

My slides are here, anyone is welcome to view:

<https://www.figma.com/slides/So6Wwc352FDN6jzn40wPiB/UX-Design-for-SSI?node-id=17-516&t=4otaS31vi35HhWml-1>

## ***Primer on the CEDAR AUTHORIZATION POLICY LANGUAGE - What Why How***

**Session Convener:** ?  
**Session Notes Taker(s):**

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

<https://www.cedarpolicy.com/en>

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

## ***Did:btc1***

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

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

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

NO NOTES SUBMITTED

## ***OCA Render Method for Verifiable Credentials***

**Session Convener:** Patrick St-Louis  
**Session Notes Taker(s):** Michel Sahli

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

OCA for VC visualisation: <https://github.com/e-id-admin/open-source-community/blob/main/tech-roadmap/rfcs/oca/spec.md>

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

A concern stated during the session was that with OCA, a malicious issuer could show fake information in the wallet. This can happen but the conclusion here was that information shown on a screen should not be trusted by verifiers and they must verify the actual signature and raw data.

Another discussion was which query language should be used to do the mapping between the OCA capture base and the content of the vc. Json pointer do not support array items. Json path can be dangerous because of query evaluation and another solution would be to look at something similar as in DCQL. No answer was found to that.

During the discussion, multiple brainstorming started on other use cases where OCA could also be used and it shows the flexibility that the format brings. But community work is necessary to standardize some overlays for interoperability.

BC Gov and the profile from Switzerland is not aligned yet and is one of the first steps to bring interoperability to it and hopefully will later be able to migrate to a standardisation organisation.

People from the session would find it helpful to see an OCA playground where they have an example and can play it OCA's and their representation.

## SESSION #10

### *DCQL Part 2*

**Session Convener:** Daniel Fett  
**Session Notes Taker(s):**

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

Advanced Features and Stuff

---

## Requested/Discussed Features

- More (detailed) value matching
- Support for ZKPs

---

# Value Matching Use Cases

- Age Verification:
  - Above 16? Above 18? Above 21? Under 99?
- Partial matching:
  - E-Mail ends with '@company.com'
  - ZIP code is '90210'
  - address/country is not empty
  - Nationalities contains 'JPN'

--

## What ASC does

See Advanced Syntax for Claims

--

## How we could use that

```
```json
{
  "credentials": [
    {
```

```

    "id": "my_credential",
    "format": "vc+sd-jwt",
    "meta": {
      "vct_values": [ "https://credentials.example.com/identity_credential" ]
    },
    "claims": [
      {
        "path": ["birthdate"],
        "fn": ["years_ago", ["gte", 18]]
      },
      {
        "path": ["nationalities"],
        "fn": [{"eq", "USA"}, "any"]
      }
    ]
  }
}
...

```

--

ZKP

```

```json
{
 "credentials": [
 {
 "id": "my_credential",
 "format": "vc+sd-jwt",
 "meta": {
 "vct_values": ["https://credentials.example.com/identity_credential"]
 },
 "claims": [
 {
 "path": ["birthdate"],
 "zkp": ["years_ago", ["gte", 18]]
 },
 {
 "path": ["nationalities"],
 "zkp": [{"eq", "USA"}, "any"]
 }
]
 }
]
}

```

]
}
'''

Take-aways:

- Value matching makes sense, we can enhance it (roughly as proposed here)
- It is too early to design the ZKP features right now
- We need more security considerations, see <https://github.com/openid/OpenID4VP/issues/300>

### Germany's Digital Identity History

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

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

Slides: https://docs.google.com/presentation/d/1c2PJrCRCIU96jSVL7qK7-bww03oeFE3zwLfN6EuQgWM/edit?usp=sharing

Tags: Germany, digital Identity, MDL

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

In this session Mirko gave an insight of Germany's history starting in 2002. It resulted in an over engineered way without the demand because of missing online services. Beside the development in the past for the digital identity, he also gave insights into the reaction of the civil society that criticised the current approach for the EUDI Wallet.

## *How do we get to verifiable credentials in academia and government?*

**Session Convener:** Nicole Roy, Giuseppe DiMarco, Stefan Liström

**Session Notes Taker(s):** Nicole Roy

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

We did intros from everyone, why they are interested in this topic

Interested in EU digital identity wallets - eIDAS v2 - large-scale pilots

Coming from the education space: Building services on top of existing educational identity system is complex and messy. Scaling issues.

Challenges with needing to use first-party identity (due to browser privacy changes)

Collaborate across sectors (right now academic identity is a closed ecosystem)

Wallet technologies could help us reduce complexity and increase interoperability across sectors and borders

Want to understand best current practice and stay current

Want to get universities issuing VCs for things like academic degrees, courses, etc.

Want to not have to use visitor IDs/guest IDs for campus collaboration

Google Wallet - Justin Brickell, want to understand if we can use platform wallets like Google Wallet or if we need to support third party wallets too?

Want to understand the reputational network possibilities

Giuseppe has implemented both the old model in SAML 2, as well as OAuth, OIDC solutions, collabs with research and education communities. Have implemented OIDC eGov profile for Italy, as well as developing OpenID Federation spec and running an OIDF federation for Italian gov

Student employment credentialing on campus, or internships - lots of pressure coming from alumni wishing they had had that

Help researchers make better data documentation.

Nicole posits that we need something like OpenID Federation in order to accurately represent multifederation multi-trust-path trust registries for wallets, verifiers/RPs and issuers/IdPs.

Nicole further posits that we need to profile OpenID Federation for Research, Education and Government so we know what we need to pay attention to implementing (first, or at all). Single trust anchors/trust oracles have proven to be unrealistic in the real world.



The question of what type of trust topology we need is one of governance/trust requirements modeled on the real world.

This is not a technical question, it's a governance question

Using, for example, SAML 2 with MDQ, we have a single trust anchor

Margaret brought up how to represent trust for a fictional university. Need to know how to check and trust:

- Student-ness
- Of-age
- Degrees I have
- etc.

Need trusted qualitative properties like "is an accredited degree-granting institution of MD degrees" - these are trustmarks in OpenID Federation.

VERY COOL OFFER! :: Using user journeys is really important: Story of a student, story of another subject. Give these to Giuseppe, he will help us understand what we need to deploy.

Identity matters only in relation to what others know about me, identity only exists in relation to other persons, groups and entities. It's first-party, but trusted first-party. The trust has to be introspected external to the identity. I need multiple avenues to be able to build my trust image of an entity. (Example: Fraud prevention). - Carly from University of Guelph

One principle we honor in "Next-Generation Credentials": The ability for the user to be in control of what data they release to a relying party. Trustmarks also are important there.

But can we actually make this work in the real world, with a massive RP base?

Nicole needs to know what parts of OpenID Federation we need to profile in order to run a trust registry.

oauth-status-assertion IETF draft from Giuseppe - better way to do revocation than the public token status lists that the EU mandates.

Davide Vagheti at GÉANT is task leader for the OpenID Federation profiling for research and education.

We don't want to build trust infrastructures that won't go beyond R&E. Italian government went into prod with OI DF two years ago. The EU model legislation and implementation acts reference using OI DF for RP authentication.

Boyd makes the point that moving this model into the core of university operations will bring a much greater level of funding and attention.

Another use case from Carly at U. Guelph: Being able to sign data sets as they come off the instruments. Basically research data supply-chain security.

Nicole mentioned VCs for instrument calibration attestation.

In Italy, they require the entities to store the history of their signed trust chains for provenance and auditability reasons.

## **Packet Graph**

**Session Convener:** Joe Rasmussen

**Session Notes Taker(s):** Joe Rasmussen

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

<https://www.inky.tech/>

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

Joe's session initially drew just one other participant - Larry Hamid of Bluink. Later Andor Kesselman joined the discussion.

From Joe's perspective, one outcome is that he is slowly tightening-up a reasonably concise introduction to the Packet Graph proposal, as follows:

Packet Graph - Abstract

This paper outlines a proof-of-concept to demonstrate a standard. The standard relates to entities that communicate from IP6 addresses. Subscribers to the standard would have access to a reputation system not entirely unlike the reputation system that governs Wikipedia. They would have access to a search mechanism not entirely unlike PageRank.

The proposal treats the messages sent by the entities as *species*. The word is meant both in the sense of *types*, but also in the 'lifey' sense that any message may prove to be a 'please copy me' instruction; with the fittest messages competing with, and pushing aside, messages that are less fit.

These are the three components of the system:

1. Reputation somewhat like Wikipedia
2. Search somewhat like PageRank
3. Design somewhat like natural selection.

The objective is a lofty one: To build a decentralised, general problem-solving machine at the scale of the internet.

More information here: <https://www.inky.tech/>.

## ***Better Login for the Fediverse and the Social Web***

**Session Convener:** Aaron Parecki

**Session Notes Taker(s):** Sam Goto

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

<https://indieweb.org/FedCM> for IndieAuth

<https://indieweb.org/FedCM>

<https://github.com/samuelgoto/indie-fedcm>

<https://github.com/aaronpk/oauth-fedcm-profile>

<https://developers.google.com/privacy-sandbox/cookies/fedcm>

<https://github.com/w3c-fedid/FedCM>

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

- johannes: take your blog urls and bootstrap identity system, activitypub, dazzle, personal data stuff related to activity pub, fediform, online
- jan: enterprise, architect engineer
- aaron: blog web, independent web space, interested in using your blog as your identity online, works on enterprise
- stephan: make the web usable, surveillance, works on enterprise IT, simplify identity
- nick: interested in fediverse, distributed, roadblocks
- tommaso: phd, four years in oauth, federations,
- nicolas: consulting, system integrator
- paul: also consulting, interested to understand before a corporation ruins the idea of fediverse
- venky: paypal identity,
- jonak: IAM solutions
- vel: working at paypal, remove login, trusted,
- aaron: content in distribution systems, passwords should go away,
- lisa: activitypub, account portability,
- jim: consulting, working on NIST
- aaron p: in most traditional login system, you'd email password, thankfully now we are moving away from passwords, still a lot of username based accounts, social login, enterprise login, indie auth login, use your own identity provider to login to something., historically, these have not had good UX, to the point where they use usernames and passwords. lately, i've been working on, since 2014 or so, i've been working on indie auth, taking your url as a discovery point for your oauth server, to login to something, same design goals as OpenID 1

- aaron g: neat, that's where we started
- aaron: the friction, couple points, i don't want to have a website, and 2, it is hard to enter the identity. there is a lot of work to do on advocacy side, but there is a lot of practical things that we can do with the support of the browser. if we do have the support of the browser, we could use FedCM in the browser, to completely smooth over the UX friction ...
- aaron g: they have gotten a lot better at TPMs
- aaron p: the actual credentials, and how is that tied to the person, the other is where did account originate
- johannes: different persona on social media ... everybody ...
- dazzle: you need to created a local account
- johannes: you'd want to
- aaron: the common thing is the browser, this is what we are prototyping.
- aaron: basically the idea is, if i have a mastodon server, that can register in the browser as an identity provider ... the browser then remembers ...
- stephan:doesn't SIOP work?
- paul: what if we standardized a reserved URL, say https://idp.example, and that would always return all things per user
- ?:
- johannes: the user doesn't care about the mechanism
- johannes: have the browser know this one identity that I have, and if the brose cooperates, and it works, except that, people have segmenting their personas
- extra step in here, if there a choice ....
- profiles in chrome
- aaron: walks through demo

pk Aaron Parecki x W Webmention.io x +

🔄 aaronparecki.com/settings/fedcm

**aaronparecki.com wants to** x

📁 Use your accounts to login to websites

Block Allow


Site Syndication

**FedCM**

Register IdP

Unregister IdP

Sign in to webmention.io with aaronparecki.com x

 Aaron Parecki  
aaronparecki.com

Continue as Aaron

- paul: there is a big difference between authentication here and just following ... to an end user, it looks exactly
- johannes: how does firefox feel about it?
- johannes: this is pretty cool ... have you talked to the mastodon people?
- johannes: i've been coordinating with the mastodon people ...
- aaron: they have a oauth ruby library ...
- aaron: my identity provider does not know of all of the clients in the world ...
- aaron: i wrote a separate oauth part ... for the client metadata .... useful for mastodon, bluesky,
- paul: i assume we'd need automatic client registration ....
- aaron: aha, that's exactly the draft that I wrote ... not necessary ... the OP can .... fetch the client metadata dynamically ...
- aaron: there is a oauth profile for fedcm, there is an indie auth profile for fedcm, and there is the fedcm spec ...
- ben curtis: we are working on something called FedID
- aaron goldman: there is a browser UI ... does that mean that's all that i can do ...
- aaron pk: good question ... the reason that's the only thing ...
- paul: do we want to do this only in the browser ... or both?
- aaron: for practical purposes .... you want to do both things ...
- joahannes:
- ben: mastodon, lemmy, matrix,
- paul: does facebook
- goto: should we meet again tomorrow?
- all: yes, lets kick off another session tomorrow!

## ***Customer Commons + IEEE P7012 - by which sites and services agree to YOUR terms***

**Session Convener:** Iain Hendersen + Doc Searles

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

## Bridging Trust: DIDs + DNS + X.509

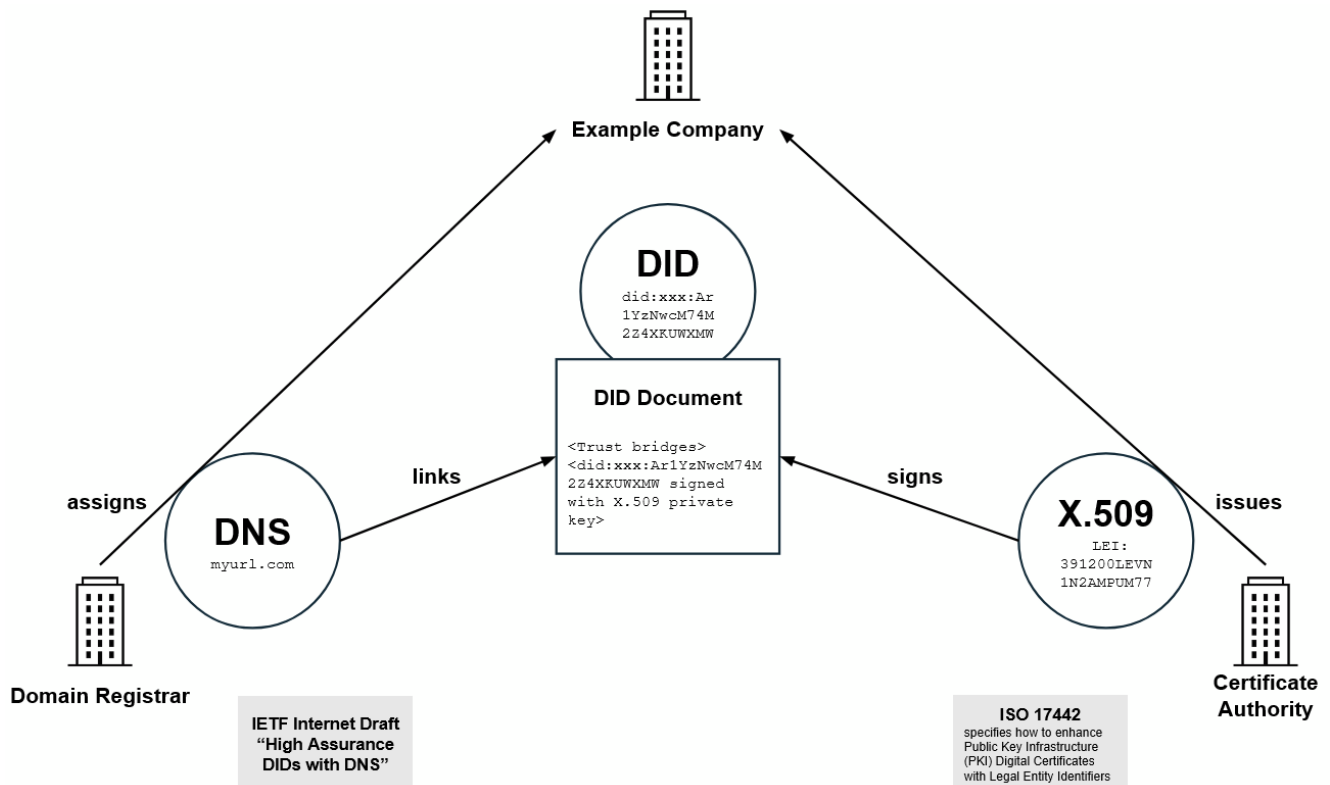
Session Convener: Andre Kudra, [Markus Sabadello](#), [Drummond Reed](#)  
Session Notes Taker(s): [Ankur Banerjee](#)

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

- <https://datatracker.ietf.org/doc/draft-carter-high-assurance-dids-with-dns/>

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

- Binding DID to LEI/vLEI
- What does having an LEI prove, besides that there's a legal entity?
- DID document
- Consider DNSSEC and HSTS (HTTP Strict Transport Security)



## ***Sneaking SSI into the Music Industry - AMA with Switchchord***

**Session Convener:** Cole Davis

**Session Notes Taker(s):** Cole Davis

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

Cole gave an introduction to Switchchord and the issues he faced as a lawyer that caused him to look for identity technology to help with legal workflows. The music industry has a lot of different *identifiers* but no functioning *identity* system. Decentralized identity provides a framework to verify and bind disparate identifiers to a single cross-platform identity. Cole showed how Switchchord uses these verified identities to then map legal relationships between songwriters, music publishers, and publishing administrators, which dictates how metadata for new music should flow throughout the supply chain.

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

Switchchord is looking at implementing the C2PA standard for recorded music. Hopefully by the next IIW we'll be able to demo the intersection of identity, legal, and data provenance in the music industry.

## ***Should the Sustainable + Interoperable Digital Identity/SISI HUB and Open Wallet Foundation/Forum converge efforts?***

**Session Convener:** Daniel Goldsneider, Gail Hodges, Elizabeth Garber

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED



## ***Unintended Consequences of Digitizing Personal Data (the impacts of Dobbs)***

**Session Convener:** Karen Studders

**Session Notes Taker(s):** Libby Brown

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

Type Here

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

Karen called this session based on community feedback. Karen spoke about the impact of the Dobbs SCOTUS decision that overturned Roe v Wade, and how it led her to fight for a state “My Health, My Data” law in Washington state. This law protects all health data, regardless of who gathers it, for residents and visitors to the state (of impact to residents of other states that have limited access to healthcare such as abortion or gender-affirming treatments.)

Conversation also ranged around other topics including: Project Liberty and their efforts to improve personal data control across social media and other sites; the rights and responsibilities of digital consumers to know and understand what personal data privacy means, and how aware/willing consumers may be to make trade offs between privacy of personal data and perceived value of the sites they visit/use.

Additional topics as well - other attendees please feel free to add your recollections!

## ***Social Media/Web - Exciting Opportunities for Collaboration in the next 6-12 months***

**Session Convener:** Brendan Miller(brmiller@cyber.harvard.edu) and Alberto Leon(aleon@cyber.harvard.edu), Applied Social Media Lab, Harvard University  
**Session Notes Taker(s):** Alberto Leon and Brendan Miller

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

Participants:

- See picture below
  - Alberto Leon
  - Brendan Miller
  - Anuja Chivate
  - Golda Velez
  - Tania Abdul
  - Jeff O
  - Benjamin Goering
- Not pictured
  - Dmitri Zagidulin
  - Day Waterbury
  - Koby Han

The goal of the group was the surface/brainstorm possible exciting opportunities to make a notable positive difference in social media through the use of identity in the next 6-12 months, and then prioritise them.

See the brainstorm and the score/ranking from the group on the most exciting opportunities in the pictures below.

The group expressed interest in staying in touch and following up.

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

Tania Abdul

- Mentioned the social graphs and its importance in making it portable.
- She mentioned that adoption should be EASY and it's something that the group agrees on.

Golda Velez:

- Has experience on decentralised trust and is very familiar with bluesky.
- Mentioned an idea of involving influencers to make the adoption easier.
- Talked about how to involve someone with a podcast to try all the different platforms.
- Mentioned a future use case where AI can become something that people social with and can publish to your social platforms

Jeff O:

- Tech anthropologist and has passion for the social media realm.
- Mentioned the aspect of making the new era of social media as “yummy” and then getting people to open their mouths.

Tania Abdul:

- Also involved in trunet, the same as Golda and is dedicated to interconnecting networks.

Koby Han:

- Is part of a business based on decentralised identity in Korea called HOPAE.

Benjamin Goering:

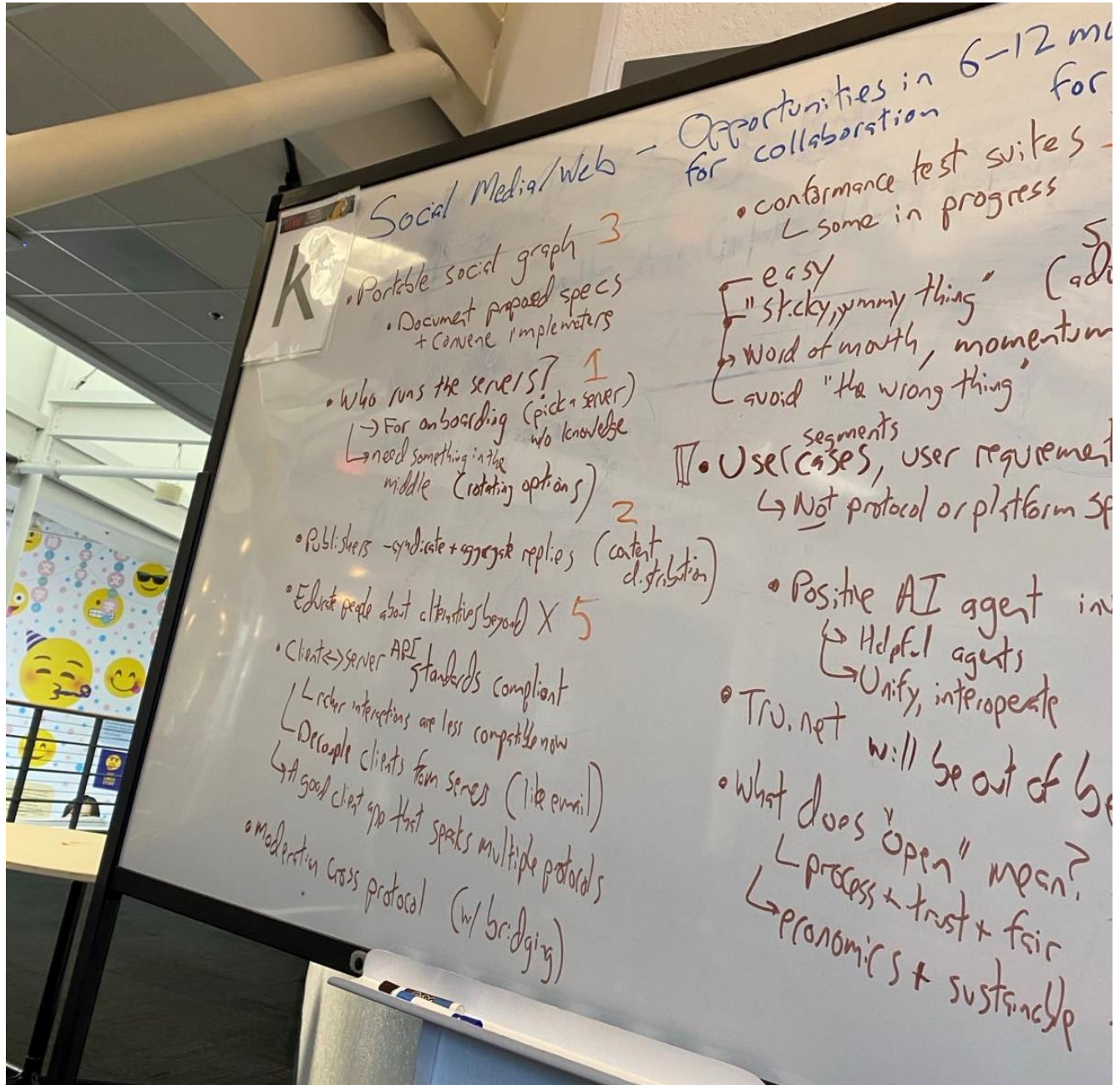
- He has worked on test suites around Fediverse. Knows Darius from the open standard group.
- Mention during the session the option of creating things that are standard compliant.
- Brainstormed the idea of test suiting some of the standards.

Demitri Zagidulin:

- Has a focus on social web, participants a lot on the open standard group for social web. Has experience working with social issuers, and wallets also.
- Mentioned mainly two problems he sees:
  - Who controls the server?
  - Onboarding experience. -> mentions the UX experience, something is needed in the middle



Brainstorm whiteboard:





Media/Web - Opportunities in 6-12 months for impact!  
for collaboration

col graph 3

+ proposed specs  
one implementers

series 1

diag (pick a server)  
no knowledge

in the  
rotating options)

regis replies (content  
d. strabian)

beyond X 5

compliant

op-still now

s (like email)

multiple protocols

bridging)

• conformance test suites 3  
↳ some in progress

easy  
"sticky, yummy thing" (adoption) 3  
↳ word of mouth, momentum  
↳ avoid "the wrong thing"

work in open  
engage influencers

II. User cases, user requirements, reference designs 4  
↳ Not protocol or platform specific

• Positive AI agent involvement?  
↳ Helpful agents  
↳ Unify, interoperate

credentialing  
issues?

• TRU.net will be out of beta

• What does "open" mean? 1  
↳ process + trust + fair  
↳ economic + sustainable

platforms  
creators

## *JSON-LD VC with BBS, OID4VCI, OID4VP, and Pseudonymous DID Key*

**Session Convener:** Dan Yamamoto

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

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

Verifiable Credentials, JSON-LD, BBS Signatures, OID4VCI, OID4VP, Pseudonym, did:key  
Slides: [JSON-LD VC with BBS, OID4VCI, OID4VP, and Pseudonymous DID Key - Speaker Deck](#)

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

In this session, we discuss the use of JSON-LD BBS VC (Verifiable Credentials) with OID4VCI (OpenID for Verifiable Credential Issuance) and OID4VP (OpenID for Verifiable Presentation), focusing on the pseudonymous did:key approach. After the discussion, the presenter shows a demonstration using their prototype wallet, which is a work-in-progress web application without a hardware security module or native mobile implementation.

### **Technology Stack**

- Utilizes OID4VCI and OID4VP for issuing and verifying credentials.
- Employs the W3C verifiable credentials data model with data integrity.
- Uses the blind BBS signature scheme to issue credentials that are blindly bound to the holder's secret key.
- Implements the ZKP (zero-knowledge proof) system of BBS for realizing selective disclosure and unlinkable presentation
- Pseudonymous DID Key: Generates multiple public did:keys from a single user secret key.
- (Extra feature) Wallet-Initiated Presentation: Unlike the standard verifier-initiated presentation, the wallet can initiate the presentation.

### **Standardization Status**

- Some technologies are not yet standardized but are planned to be in the future.
- The methods of blind BBS signing and ZKP differ from those in the [W3C Data Integrity BBS Cryptosuites](#).
  - The most significant difference is the way JSON-LD data is transformed into BBS input messages (a sequence of field elements).
  - **Pros:** Our scheme can be extended to use zk-SNARKs for predicate proofs for each attribute in the credential.
  - **Cons:** Proof size can be three times larger than the W3C DI-BBS.
- Our scheme is inappropriate for some proximity use cases where transmitting large data over BLE (Bluetooth Low Energy) is required.
- There are still a few other differences, making implementation not straightforward at the moment. We plan to document and publish the details later.
- Pseudonymous did:key and wallet-initiated presentation are also works-in-progress and not yet standardized.

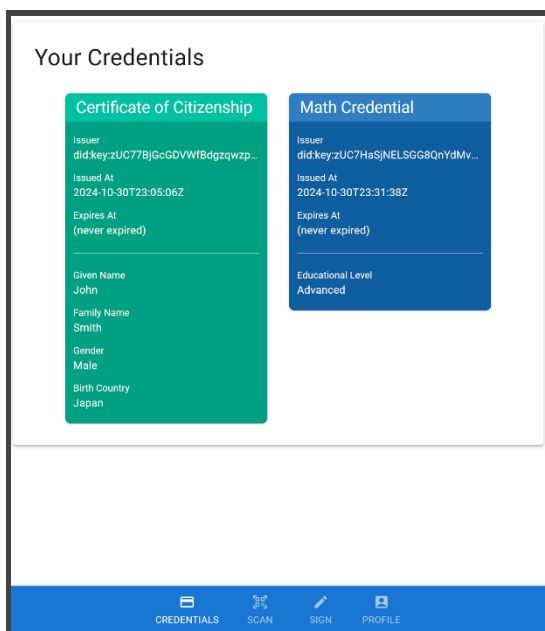
### **Pseudonymous did:key**

- Generates multiple public keys from a single secret key for different domains or content, enhancing user privacy.
- It functions as a usual did:key, resolvable using a DID resolver (e.g., `did:key:z3tEFvdbfSRva1mkyFDvgocAf8AASbXhEet6tVz51AFAp9TwnL7hGJKNsmtxrRFucQrXCT`).
- It is similar to a Schnorr public key, except that while a Schnorr public key is generated as `gsk` where `g` is a shared public parameter, our key uses a domain-specific base like `Hash(domainID)sk`.

## Demonstration

- Shows the process of issuing and verifying credentials.
- Demonstrates obtaining a credential from a government site and presenting it to another site for verification.
- Demonstration Steps:
  - The user obtains a digital citizenship certificate from the government site using OID4VCI and a pseudonymous did:key specified for a government site.
  - The citizenship certificate is then used to prove the user's identity on another skill-checking website.
  - After verification of the citizenship certificate, the skill-checking website issues a skill credential to the user's wallet over OID4VP and a pseudonymous did:key specified for the skill-checking website.
  - The process includes scanning QR codes and selectively disclosing credentials and attributes.
- The Implementations are a work-in-progress and have not been published as open-source yet, but they will be published once they are ready.

## Screenshots Below:



### Certificate of Citizenship

**Issuer**  
did:key:zUC77BjGcGDVWfBdgzqwz...

**Issued At**  
2024-10-30T23:05:06Z

**Expires At**  
(never expired)

---

**Given Name**  
John

**Family Name**  
Smith

**Gender**  
Male

**Birth Country**  
Japan

### Credential Information

**Credential ID:** <http://did-vc-core.test/credentials/51946f90b6711cf31a9a9b59ee116bda>

**Credential Type:**

- CertificateOfCitizenshipCredential
- VerifiableCredential

**Issuer:**

did:key:zUC77BjGcGDVWfBdgzqwz3uuWkoWuRMe8pnx4dkncia5t9LKHVt96BPG

**Issuer ID:** <BizeSU7BKiv35h1tsuVwHUVt4arZuckxGCb2tTsB3fsY66mQNs5Bwoac2w2iyYFe8uenBUYdAiveEr>

**Issued At:** 2024-10-30T23:05:06Z

### Credential Subject

**type:**

- Person

**Given Name:** John

**Family Name:** Smith

**Gender:** Male

**Birth Country:** Japan

**Birth Date:** 1980-05-03T00:00:00Z

// Example of Verifiable Presentation

```
{
 "@context": [
 "https://www.w3.org/2018/credentials/v1",
 "https://www.w3.org/ns/data-integrity/v1",
 "https://zkgp-ld.org/context.jsonld",
 "https://w3id.org/citizenship/v3"
],
 "type": "VerifiablePresentation",
 "proof": {
 "type": "DataIntegrityProof",
 "created": "2024-11-03T09:20:08.253Z",
 "challenge": "f347878abf00cd9b76328de20c9472a2",
 "cryptosuite": "bbs-termwise-proof-2023",
 "domain": "http://did-vc-core.test/verifier/verifier3.test/response",
 "proofPurpose": "authentication",
 "proofValue": "uomFhWQReAgAAAAAAAAAAj2pm0hdZE1BFqYoETM301jXhxDI62N1Jg6jlaAsJr-Iln-
B5MHZz9TH40mZhcMv5iT7ZW6VRUgwVZe1J3KqkE954bgwQp9G2mt6i6jUNWA5k9m43SdqRBB2OShuwx48aijK58AcLh8uhH
K5CFXdvphszVPdtVNnEkkyfwBEE0httX66_SWifCL9ba6LiFohkV5IYozTKMMQe1118xUO3bPFtHVyeJzoTBPntswH4fPu5S0QsiM
e7o60J1VMK5Kih7PIb6pN6qxIRZQE1wv2O2I8e8aTbJzEjBODJu6APATFWxb5mZt45xiMtx0oj6EmtLWZUY2vxfwzOZFvKHNEqQ
d7VOF5SdL9cReXxpb3EEr16XoNnEKoue7soLGV2SGBY-
PSj9aLC4KbMaqjqtTAABEGAA
oU92H0SkQmAQAAAAAAAAAACpg1Mkd02gHJwDnet6qelshOfiqJKe6qpqbzPDzGuZXAQAAAAAAAAAAD-
WqV6T28bF12OFw4AqtfA6-
96fK1In6rJuqISFdyBoIAAAAAAAAAAFHVQxHwwhbownd_M7VRbxVcQgb9rEw3ziB2wiBlaUBMCQAAAAAAAAAasmuejaTOueHUZ
Kzz1WR8qnx-pq4IXYFZEx3A-
3FYVPwoAAAAAAAAAYOGrdeJsPbFo3hNOglMdxRQMIhFzr1XwFAVt6KwC24LAAAAAAAAAIdMIAYrHZJYU1uHdwTmrMTCWR
_iZxiOzTE2nKQILUODAAAAAAAAAADvDK_UX-99xWVHYAQ_Om4_-
L597QlmRhBWVw9SrGM0DA0AAAAAAAAAAc1cq9vp8yC7zmF7XR8r-O8C1bFC26M8Oy6TmwYHr30cOAAAAAAAAANmFOF-
I_ot27Ro-RkGi46j_edNvTSpCI9rJL2cO-wHDwAAAAAAAAADHIB0pXMiLcC06kHxgNh1TzAP6wMbh8iLnOeTu-
```



```
geKRBAAAAAAAAAAHODRKCQAw1AQgF2V9LA-
gm4YCWfkKIfvoHh8Q4r7SlkRAAAAAAAAAAEo8NWzfXphpSDowU6leWEZfIAAmvA7c5IVKYLLcfqheEgAAAAAAAAAcbaAu2bWJ1i
obz7laQeDoAmCgA4fO5rmMIASR6AjU-
KBMAAAAAAAAAAnBV8ps_ohn8X2YHXC_1yXdgbKXK3UegWMTMh4geW520VAAAAAAAAAAlipF0n8BRI2SNxn7rbLsj2xqrzuLD9
vkrFbXjSu58DGgAAAAAAAAAB5qT5mEMbMLMhxnUu_BeKqICnGAeuvciCWvxt06imPHBsAAAAAAAAA4SvwI6F7819Z6831nvbB
Dk9bYOcnj0BKIFPlw3vVDgwcAAAAAAAAACCQVC1FOwgXRqxMFQqNQTCAONwF6Me8WISBtVyOQO0xGZCT__exs_fwsYO8r1
OhVQgAAAAAAAAAAEAAAAAAAAAABhYoGkYWGHBQoAAQIDBGFIC2FjhQABAgMEYWQF"
},
"holder": "did:key:z3tEFvbdFSRva1mkyFDvgocAf8AASbXhEet6tVz51AFap9TwnL7hGJKNsmtxrRFucQrXCT",
"verifiableCredential": {
 "type": [
 "CertificateOfCitizenshipCredential",
 "VerifiableCredential"
],
 "proof": {
 "type": "DataIntegrityProof",
 "created": "2024-10-30T23:05:06Z",
 "cryptosuite": "bbs-termwise-bound-signature-2023",
 "proofPurpose": "assertionMethod",
 "verificationMethod":
"did:key:zUC77BjGcGDVWfBdgzqwzp3uuWkoWuRMe8pnx4dkncia5t9LKHVt96BPGBizeSU7BKiv35h1tsuVwHUVt4arZuckxGcb
2tTsB3fsY66mQNs5Bwoac2w2iyYFe8uenBUYdAiveEr#zUC77BjGcGDVWfBdgzqwzp3uuWkoWuRMe8pnx4dkncia5t9LKHVt96B
PGBizeSU7BKiv35h1tsuVwHUVt4arZuckxGcb2tTsB3fsY66mQNs5Bwoac2w2iyYFe8uenBUYdAiveEr"
 },
 "credentialSubject": {
 "type": "Person",
 "birthCountry": "Japan"
 },
 "issuanceDate": "2024-10-30T23:05:06Z",
 "issuer":
"did:key:zUC77BjGcGDVWfBdgzqwzp3uuWkoWuRMe8pnx4dkncia5t9LKHVt96BPGBizeSU7BKiv35h1tsuVwHUVt4arZuckxGcb
2tTsB3fsY66mQNs5Bwoac2w2iyYFe8uenBUYdAiveEr"
}
}
```

## Delegated Authorization with AI

Session Convener: Adrian Gropper

Session Notes Taker(s): Adrian Gropper

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

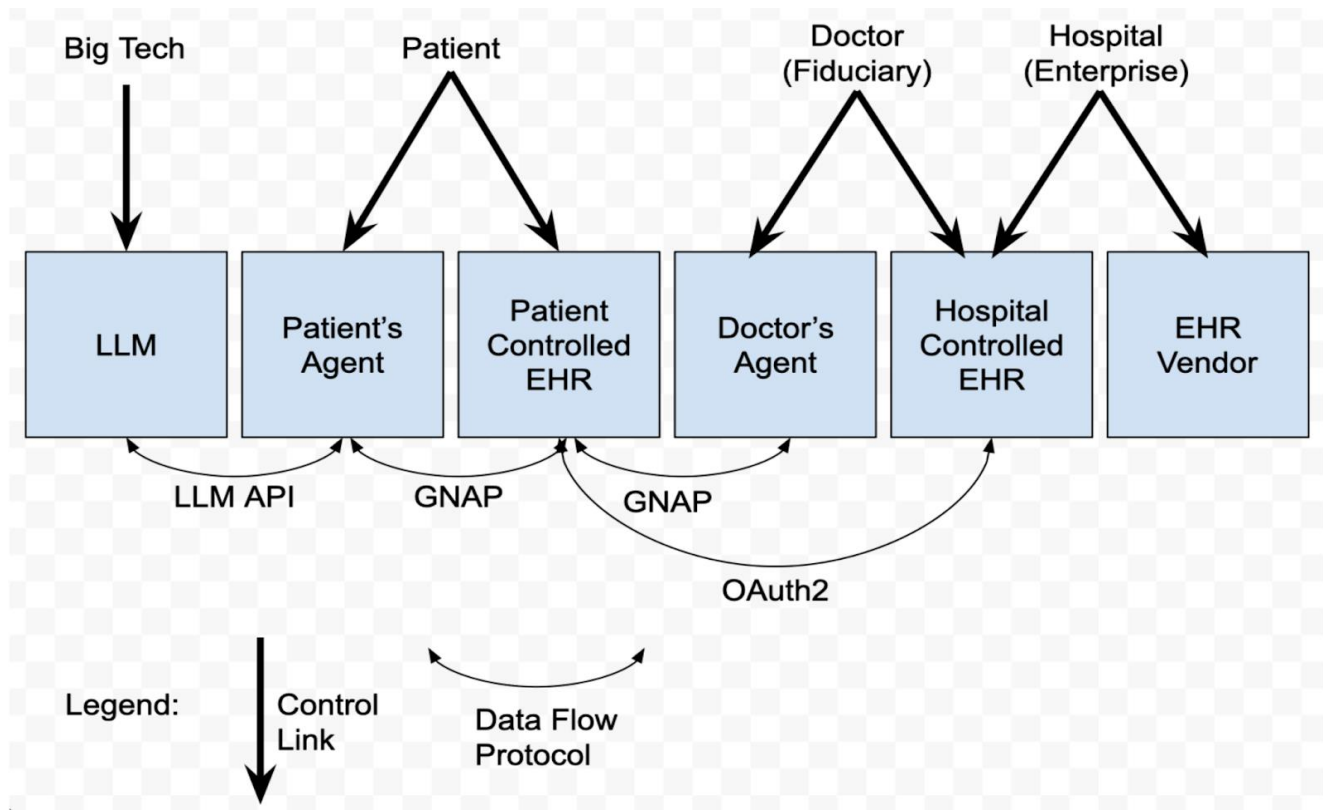
[IETF GNAP RFC 9635](#)

[HIE Of One](#) (obsolete, to be replaced by some version of:

<https://hieofonestatic.netlify.app/demo/>

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

A discussion of the benefits of GNAP over OAuth in healthcare and other domains....



# Standards enable choice and agency

## Demo standards:

- IETF GNAP - Delegated Authorization Protocol
- Containers and App Platform - Hosting Choice
- Free and Open Source Software - Community Support Choice
- Passkeys - Encourages delegation instead of password sharing
- HL7 FHIR - Service Resource Ontology and Scoping
- Markdown Chat UX - Consistent User Experience avoids lock-in
- Email - Messaging choice
- Verifiable Credentials - Verifier choice
- IETF GNAP - Enables separation of:
  - Document storage (NOSH)
  - Policy storage (Trustee®)
  - Personal AI as user agent (GNAP client library on GitHub)
  - Document update by delegate's personal AI (Signed markdown)

## Discussion Notes:

**M** 10 Delegated Authorization for AI

- RS → New OS Health.
- Client → AI enhance personal Agent
- OAuth tokens are opaque strings. → no responsibility tracks for attribution  
GNAP is Certificate Based → nonrepudiation  
RS is in the token vs OAuth in the URL → security risk  
GNAP is capability based.
- Protecting the patient against themselves → same as OAuth.
- Signing documents is important - must capture delegation chain
- We're not dealing with policy expression
- GNAP allow for out of band patient notification if policy says its ok

***Personal knowledge management & tolls for thought: 5C of knowledge management framework (an optimal method to learn metacognition)***

**Session Convener:** Michael Becker

**Session Notes Taker(s):**

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

NO NOTES SUBMITTED

***Key recovery using secret location entropy comparison with seed phrase***

**Session Convener:** Matt Vogel

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

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

Trying to compare the entropy in a 24 word seed phrase ( $2048^{24}$ ) to Matt V's location-based recovery system.

We threw some numbers up on the board—thankfully we had Christian Tschudin to keep us honest with the math and apply his methodical mind to the problem.

**Some observations:**

-Several of the session attendees believe there are way more possible locations than locations that someone would reasonably choose, so the entropy is lower than it could be.

-In a 24 word seed phrase words can be repeated—if locations can't be reused that also lowers the entropy (basically it gets easier to guess the next value as you move along the recovery path).

-Christian pointed out humans are notoriously bad at being random.

I think the conclusion was that you would need to remember "quite a few" locations to approach the entropy of the 24 word seed phrase.

Christian recommended letting the computer generate the seed phrase and protect the seed phrase with the location based recovery. Matt added maybe add some kind of offline component to that....e.g. the seed phrase is encrypted with the location based recovery scheme, and then stored offline.

Matt V also mentioned the app uses AI to see if the clues are too easy. He mentioned that he avoided putting in the clue and the answer in the query because he didn't want that info to potentially end up in the model. But a way around that could be to ask the AI for the top 10 guesses given the location prompt, and then compare those to the answer outside the AI engine.

Powered by

# OPEN SPACE TECHNOLOGY

## 5 Principles:

- 1 WHOEVER COMES ARE THE RIGHT PEOPLE
- 2 WHEREVER IT HAPPENS IS THE RIGHT PLACE
- 3 WHATEVER HAPPENS IS THE ONLY THING THAT COULD HAVE
- 4 WHENEVER IT STARTS IS THE RIGHT TIME
- 5 WHEN IT'S OVER, IT'S OVER



## THE LAW OF MOBILITY



### *Motion and Responsibility*

If you are not learning or contributing, move yourself to somewhere that you will.

*Capture the Power of Self Organizing  
to Engage Your Most Pressing Issues*

## Notes Day 3 / Thursday October 31 / Sessions 11 - 15

### SESSION #11

#### *Revocation/Status mechanisms Comparison*

**Session Convener:** Paul Bastian & Mirko Mollik

**Session Notes Taker(s):**

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

Slides here: [https://docs.google.com/presentation/d/1pIZCRbVaODI5KaBt0kh8l9k9vvlZkt\\_QkX--szY3QkQ/edit?usp=sharing](https://docs.google.com/presentation/d/1pIZCRbVaODI5KaBt0kh8l9k9vvlZkt_QkX--szY3QkQ/edit?usp=sharing)

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

- we presented the current mechanisms and their developments, standardisation roadmaps
- the audience was very interested in the experience and also the demand like the architecture reference framework from the EU
- the perfect mechanism does not exist, but we were able to define criterias that can be used to find the best fitting approach for each use case

#### *KERI as a Service health KERI's KaAs Platform*

**Session Convener:** Phil Feairheller

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

## Decentralized reputation and social attestation

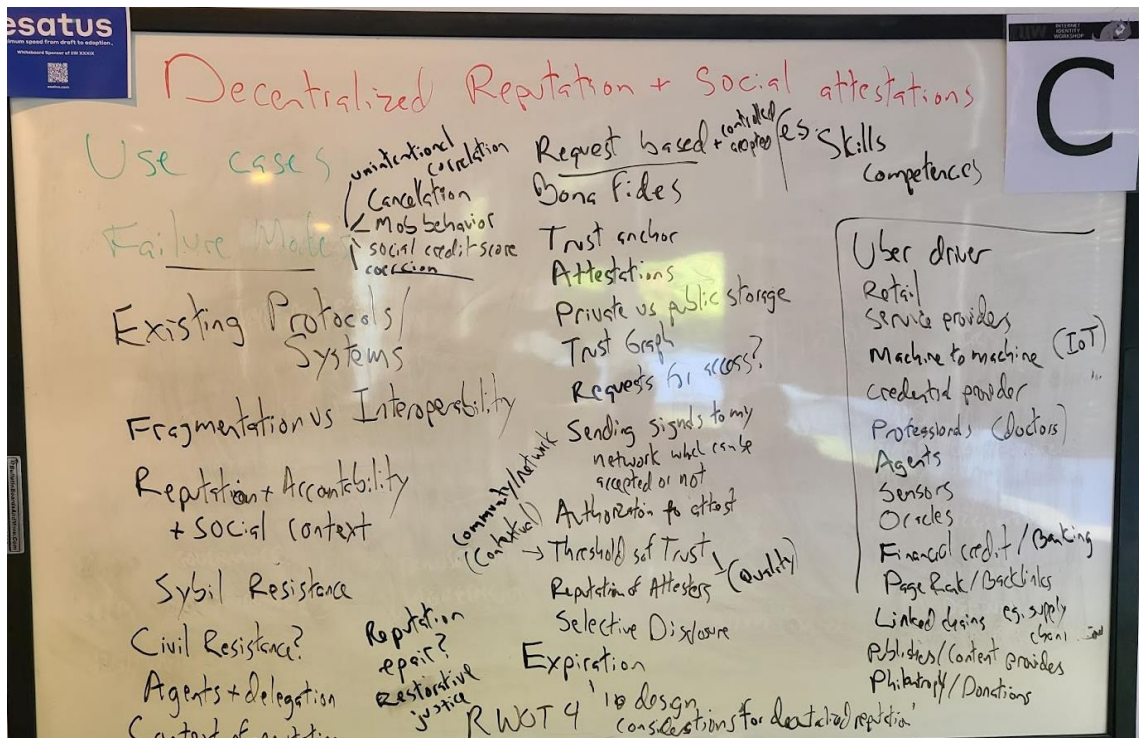
**Session Convener:** Brendan Miller (brmiller@cyber.harvard.edu), Applied Social Media Lab, Harvard University

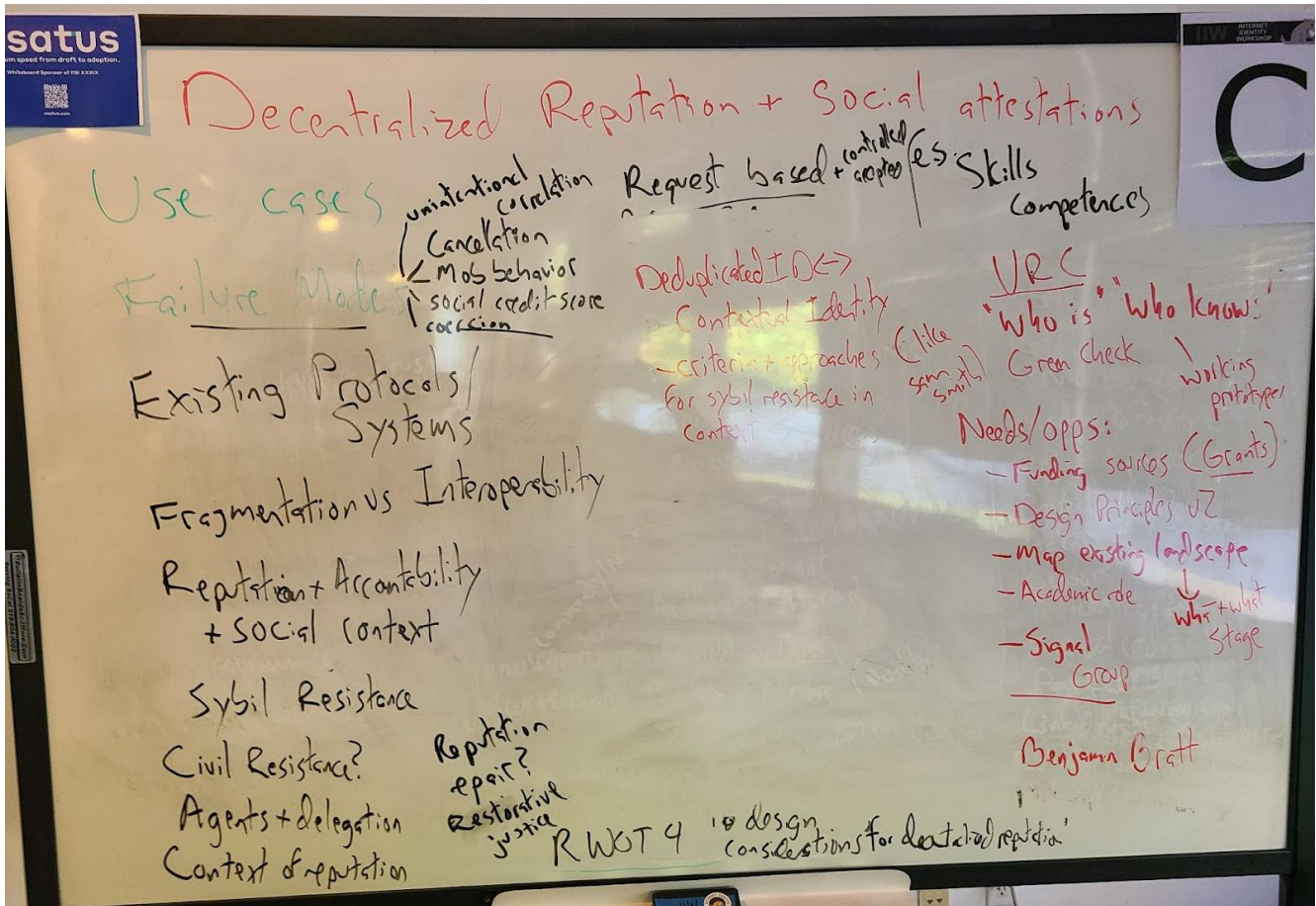
**Session Notes Taker(s):** Alberto Leon and Brendan Miller

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

- Signal group for discussion and coordination:  
[https://signal.group/#CjQKIFNplmUVDdgbVA38p1EflOGuKc9p5qfMGmZKtN8DCmvFEhDAIJT\\_PQ-Y\\_6esU3thDns6](https://signal.group/#CjQKIFNplmUVDdgbVA38p1EflOGuKc9p5qfMGmZKtN8DCmvFEhDAIJT_PQ-Y_6esU3thDns6)
- References to previous and existing work (*please add links if you have them*):
  - Verifiable Relationship Credentials (Drummond and Andre)
  - Phil Long Reputation System
  - RWOT 4: [Design Considerations for Decentralized Reputation Systems](#)

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





- Introduction to the subject and open discussion for ideas, interests, background, and brainstorming.
- Partly inspired by Drummond and Andre's Verifiable Relationship Credentials proposal regarding person to person social attestations
- Jerry: trying to learn about the subject.
- Adrian: healthcare use cases. May allow doctors to work on their own reputation
- Masato: Research Exclude bad actors from the economy, he has the idea to be focused on the reputation
- Apply decentralised reputation
- Josh: Important and has a black mirror episode. People are rating each other and are worried about what it can turn into. System of context of who reviews who and what context is important.
- Building trust.
- Students are doing research on different use cases.
- Nonprofit for blockchain identities.
- Can we use a social graph on who we can trust with certain content?
- Uses cases
- Failure modes
- Existing protocols systems
- Fragmentation on reputation systems



- Put it outside of the network
- Reputation is tied to reputation and civil resistance.
- There is an issue on how to provide context.
- Allow individuals to request information from a third party.
- Ideas about recommendation based on skills among other data points.
- Linked claims and open creds. -> open source
  - Civil resistance example.
  - Recommendation is coming to an individual from another through email.
  - Its removable
  - it's like a google drive in which you request access.
- Agent centric model and own sovereign data. make unilateral decisions within its own frame and propagate the signal which can be listened to or not.
  - Assess certain information and then send the signal to choose or not.
  - Broadcast the signal to certain communities and other to not allow in certain communities.
- Uber example. One social context to another and is it transferable.
- Examples:
  - Uber
  - Retail
  - Service provider
  - Machine to machine
  - Credential provider
  - Professionals
  - IoT
  - Agents
  - Sensors
  - Oracles
  - Financial credit score
  - Aggregate attestation of things -> like a supply chain.
- Invisible hand example, cost and benefits are dif to order of magnitude to the attestation.
- Tech design design consideration for decentralized reputation RWOT
  - Context
  - Value generation
  - Life cycle
  - Resilience
  - Legal
- Banker wants to open an account and need to do KYC -> fintech
  - not related to the anti social organisation
  - Thresholds of trust
- Prevent social credit score by design
  - Example: keybase enterprise
    - Method was to cross the reputation from dif social networks with a number to each social media platform and the keybase reputation was based on an effect aggregated in an identity.
    - Result was negative.

- Timing -> expiration
- Positive and negative attestation
- VRC -> verifiable relationship credentials
  - Who is
  - Who knows
  - Working prototype
  - LinkedIn endorsements.
  - Govern reputation systems
- Matrix of grant money -> where does the money come from.
  - VC type? Blockchain
  - Give money back?
  - Misalign with the infrastructure and must be focused on the social public interest
- Rol academic with similar to KERI
- Crypto link between deep implicated ID and contextual identity to your reputation
  - ZKP
    - Techniques for civil resistance
- Who is doing what at what stage

The group requested the creation of a signal group for ongoing coordination.

## ***Expanding ACA-Py support for DID Methods using DIF's DID Registrar Drivers***

**Session Convener:** Ankur Banerjee, [Markus Sabadello](#)

**Session Notes Taker(s):** [Ankur Banerjee](#)

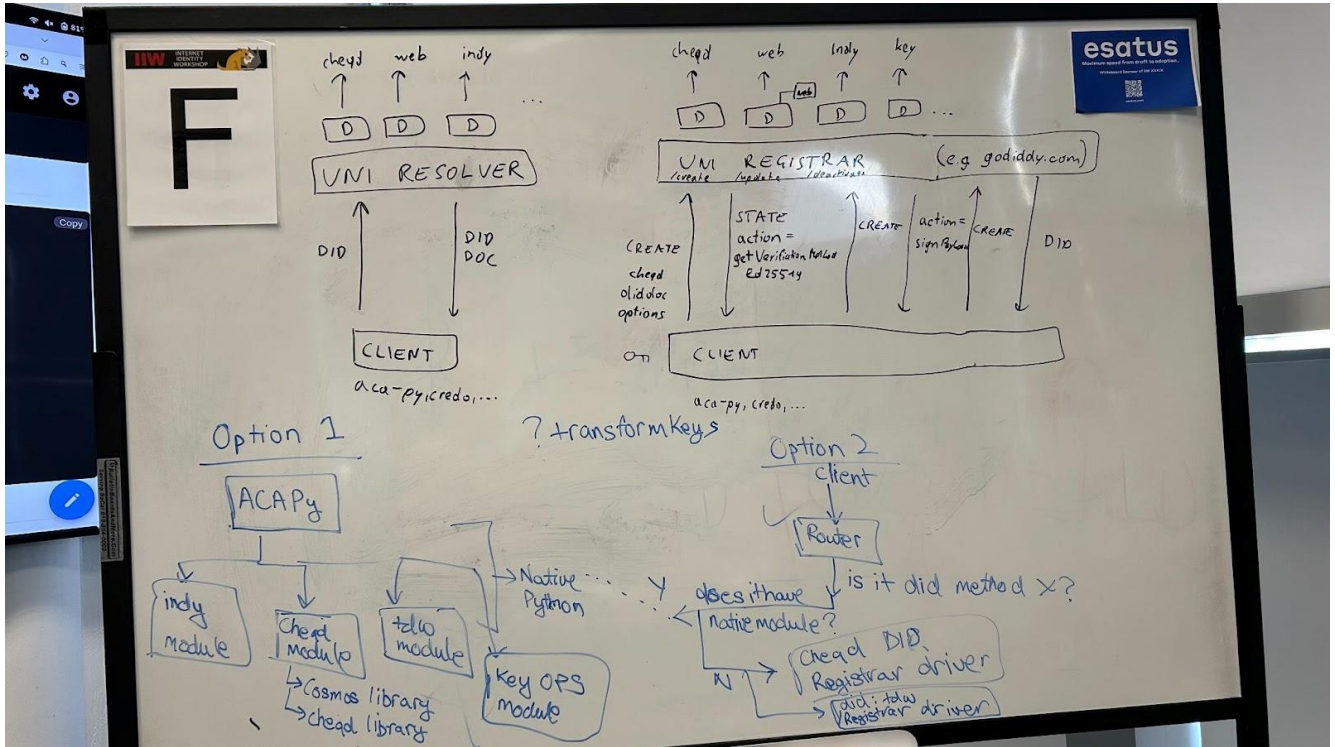
**Tags / links to resources / technology discussed, related to this session:**

- [Universal DID Registrar](#) and [DID Registration specification](#)
- [ACAPy](#)

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

- ACA-Py maintainers [Stephen Curran](#) and Daniel Bluhm attended
- Challenge 1: maintaining libraries in multiple languages is a problem for many DID method maintainers
- Challenge 2: ACAPy wants to support additional DID methods and credential formats, but doing this in native libraries is very heavy in terms of engineering resources
- There was some discussion about how having independent implementations in different languages is good
- [Markus Sabadello](#) explained the concepts on how DID Registrar works

- Does NOT mean sending requests to uniregistrar.io, instance should run own Registrar servers
- Conclusion: using pre-existing DID Registrar drivers did pass the initial sniff test of being a potentially viable approach for expanding DID method support.



## ***DOCUMENTARY Film - the Legacy of the Identity Industry - open idea brainstorm***

**Session Convener:** Oliver Mellan

**Session Notes Taker(s):** Oliver

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

Commons Movement

Self Governing is nice and refreshing. A lot of things are over designed.

Group trust created.

Making and having fun vs. being entertained. The creative act of being a part of the fun.

This is the most leveraged meeting place.

“COLLABITITION” Collaboration and competition. All boats rise together.

When we can let go of our identity, we can find who we really are. Letting go.

Some groups go and leave and miss out on the development. It is always changing.

This event feels like a music festival. It is what you make of it. The connections you make and the potentials that exist by the diversity of attendees. Lots of ideas.

People coming together to fight the man.

### **DIVERGENCE CONVERGENCE**

#### **FILM MUST-HAVES**

- Opening Circle. The process of aligning on topics and timing of discussions.
- Acronym Apocalypse. What are these letters stuck in our alphabet soup.
- Sticky notes, just everywhere!
- Low and high tech solutions for contextual consent
- Structured lack of Structure
- Diversity and Inclusion or perspectives and experiences
- San and unsung influences and achievements
- Open Spaces -ness
- The Basic problem: Digital Identity is hard to solve (which is why we've had 39 of them)
- Urgency of the topics warranted a twice a year meeting cadence. Still is needed and expected.
- Competition - from the Roman origin - getting somewhere together.
- The founding story
- Organic nature of the process
- Open Space low tech format - puts value on people's ability

- Variety of community attendee members and organizations.
- Founding story of synchronicity and immediate action - still represented in the meetings

## INTENDED EMOTIONS

Story flow [ confused - grounded - inspired / \ ]

Hopeful, moved to participate, eyes opened, thoughtful about implications for trust, commence, human values, individual agency, digital death.

Motivated, inspired, hopeful, shocked, enlightened, scared, purpose, urgency,

Challenged, uplifted, hopeful, inspired, concerned - almost scared.

Surprised, curious, concerned (will digital ID ever get solved?) Respectful (of what's been done)

Inspired and moved to be a part of something beyond themselves and their usual.

Intrigued to find out more

Visually fulfilled by beautiful cinematography and people and textures and story editing delight.

Urgency to think about these topics.

Laugh! Find the cosmic comedic moments.

## ***Policy As Code - The practical magic of Authorization development.***

**Session Convener:** Gert Drapers

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

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

Topaz: <https://www.topaz.sh>, <https://github.com/aserto-dev/topaz>

Git repository for session: <https://github.com/gertd/iw39>

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

Pointer to the "Laws of Authorization" [presentation](#)

Discussion notes:

- Q: Policy as code being a textual representation: don't you need a high-level / graphical representation so that users can understand the policy?

- A: yes, it's useful to have an isomorphic graphical representation of a policy, but you need a textual rep to be able to check in to source control and diff it
- Rohit: "policy" is typically expressed by business analysts, who don't understand code. And developers "HATE" policy.
  - A: in this context, the "policy" represents the domain objects, and how permissions are granted to subjects (users/groups) through relationships
- Q: How does an application tell the relationship database about relationships?
  - A: very domain-specific. Sometimes this is done through a service bus architecture (changes in the system raise events, and there is a subscriber that will create or delete relationships in the relationship database)
- Mike Schwartz: What are the most common questions about going to a policy-as-code model?
  - Where to start? (templates that you can modify)
  - How to model? (teaching people to view roles as "edges" (relationships), not objects in and of themselves)

Photos:





John Henderson notes:

- Policy-as-Code aspects
  - Use version-able artifacts
    - Git is your friend
  - A text editor is your main tool
    - This is the litmus test
  - Automate:
    - Testing, Deployment, Analysis
    - Can build tooling. CEDAR is an example of this.
- From discussion: Other key aspects of Policy-of-Code:
  - Serializable
  - Human-readable
  - Reviewable
    - Human and Machine reviews
- Following along: <https://github.com/gertd/iiw39>
  - Modelling Google Drive in manifest.yaml (see the `doc` and `folder` sections)
  - Use directory/model to visualize the model
  - data:
    - can express everything as relation until we have properties
    - e.g. a user can be an object
    - subjects have relations to objects

- there is IDP and domain data
- There is tooling to read from common IDPs
- How to get application data in?
  - It's a spectrum:
    - stateless, where each call defines the relations
    - keeping a copy of the relations in the authorizations systems
      - This is the Zanzibar model that Google uses
- ReBAC:
  - Roles are edges, not objects themselves
  - E.g. a group objects is a relationship

Link to the slides:

- [IIW39-Policy-As-Code.pdf](#)
- [IIW39-Policy-As-Code.pptx](#)

The demo followed the steps documented in the [README](#) file in the accompanying GitHub repository.

The core objective of **`Policy-As-Code`** is to externalize the authorization policy. This ensures that the policy is external to the application or Policy Enforcement Point (PEP) and allows it to evolve independently of the application.

Although practitioners often frown upon the **`as-code`** part, its main objective is to track and document change in a structured manner, using the lowest common denominator toolchain: version control!

When the as-code part is embraced, additional benefits, such as repeatability and automated verification of authorization policies, can be unlocked. Don't make this the starting goal when the core objective is unmet!

Having authorization policy artifacts that are versionable in a version control system does NOT assume consumers of the artifact must be able to read code. It is key to be able to visually represent the content in a meaningful manner, similar to exploring the authorization policy and verifying its behaviors.

The **`as-code`** part is an enabler, not a goal itself!



## *HomeAssistant as an example for Identity*

**Session Convener:** Sam Curren

**Session Notes Taker(s):** Wendy Seltzer

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

<https://www.home-assistant.io/>

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

HomeAssistant (HA) is a brand-agnostic smart-things platform. Sam sees parallels with the identity space.

Demo/walkthrough of HA.

HA has dashboards. Default lists all device. You can make custom dashboards.

Runs on a Raspberry pi device in the home. Nabu.casa offers a tunnel hosting service.

You can build automations around geolocation (with phone app),.

Scenes, e.g. "movie time". Monitor TV time. Dog walk reminder with tracking dog collar and step counter. The house can notice when the dishwasher needs to be run. Halloween lights schedule.

Heat tape on the roof.

Double tap a (remote) switch to turn on the hot tub exterior lights.

Integrations, devices, entities with state.

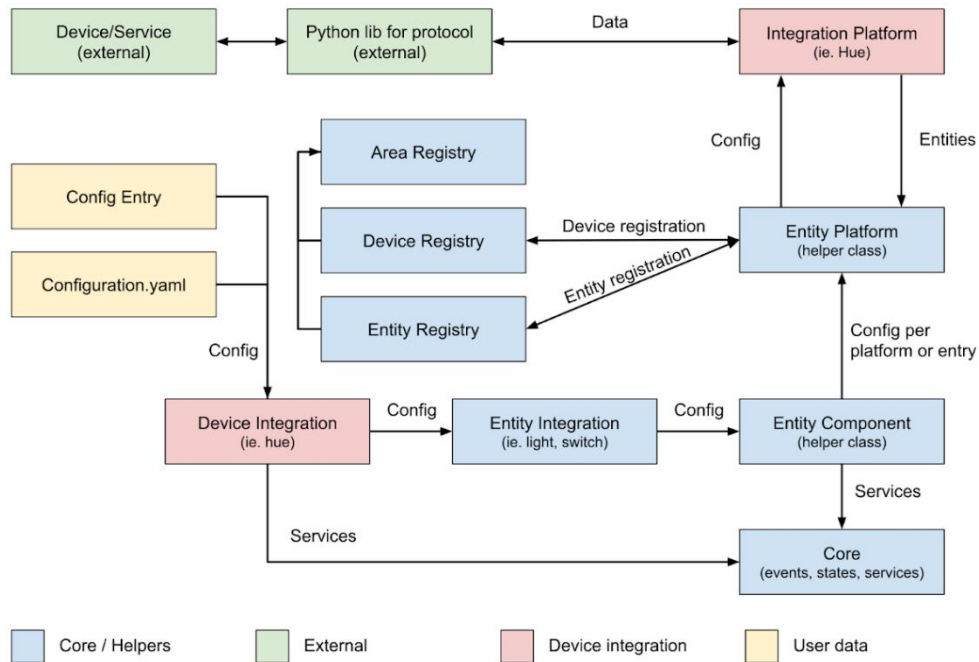
Zwave, zigbee. Lots of these for lots of smart switches.

Fade up the nightstand lights 30mins before the alarm goes off. (cool light in the morning, warm in the evening)

Activity log shows state changes.

HA as a project doesn't care if it's a cloud API, local device on your network,

<https://developers.home-assistant.io/img/en/architecture/integrating-devices-services.svg>



Example: a door open-close sensor switch on a medicine case can record the timing of daily medication, turn on a light to note missed dose. The system stays quiet when meds are taken on-schedule, alerts only on exception. (System can also watch for batteries getting low.)

Highly configurable via UI and YAML, without programming.

Question:

Here's a system demonstrating it can bring the factions of home automation together across ecosystems. (Nest, Ring, Zwave, Zigbee, Chamberlain...)

We have identities around the Internet, local and non-local. Are there parallels we can draw from the Switzerland of home automation?

Neil: travel. building on 30-year-old systems. overlay opportunities.

Sam shows a folder of 4x4 icons of apps he doesn't use anymore because he can control them through HA.

Roomba can avoid cleaning while people are home.

Paul: system of systems, as Reilly showed. Federated. It can be messy underneath. "collect the private systems under one umbrella"

Sam with HA, some integrations are cooperative, some are adversarial ("unpermissioned"), mimicking the app's wifi signal.

Steve: some other systems, if you read their TOS, they'll tell you how they use the data, even when the technologists won't

This works because we can intercept the transport layer. because it's too costly to add cell chips to all the devices we have an architectural cord to cut. We don't always see that in identity systems.

Architectural controls.

The interop draw? "works with identity assistant" ?

HA has won the protocol war by supporting all of them. Like Novell.

Brainstormed a HA app that takes VCs as credential to grant access

imagine public service credentials for the fire department or police, with access to the front door in case of emergency.

Mandated interface, build an adaptor. e.g. to RTBF.

What data-stores should we be able to mine:

Receipts, Payments, Shared PII, location history,

Connected devices, bills, utilities, e.g. solar panels, predicted charge/discharge/map of connected drive.

begin with an interface, extend from there

need delegation, designated agent.

Work with CU's Permission Slip?

Utah or Cal law has legal right to data access, deletion.

Can you use that to negotiate a better API? we don't want to delete our data, we'd rather have better access.

Open Banking. "consent hubs"

"Focused loaning" of data

Random notes:

RATGDO (rage against the garage door opener) vs Chamberlain

## **GOV'T GO FAST Part 2: Challenges + Ways Forward**

**Session Convener:** Tchaikawsky “Troy” Samuels and Shannon Johnson

**Session Notes Taker(s):** Otto Mora and Nara

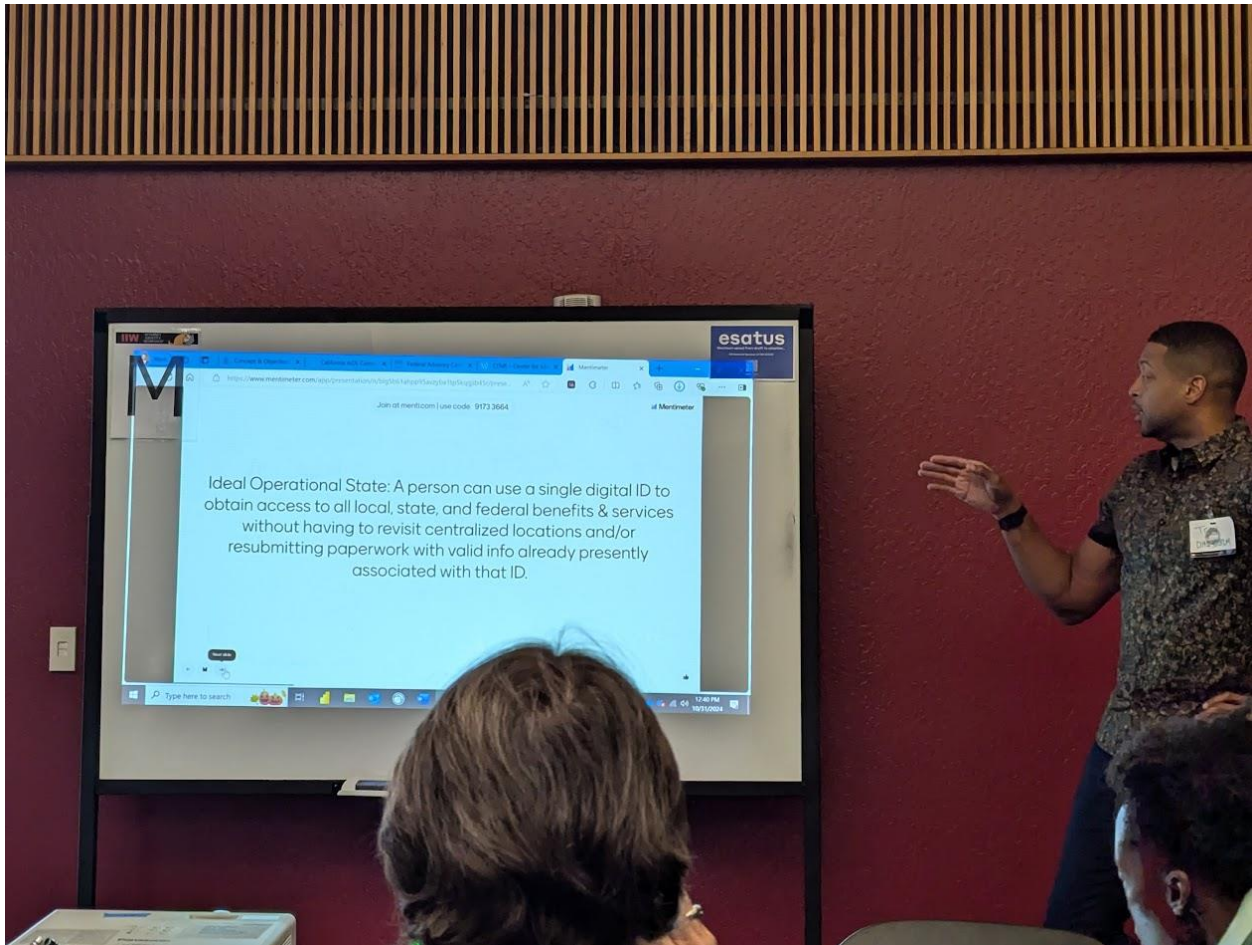
**Tags / links to resources / technology discussed, related to this session:**

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

The US DHS facilitated a workshop around discovery of platforms and standards organizations that can help create the following “Ideal Operational State”: A person can use a single digital ID to obtain access to all local, state, and federal benefits & services without having to revisit centralized locations and/or resubmitting paperwork with valid info already presently associated with that ID.

The DHS is planning to hold a symposium in Virginia in April to discuss this further. The output of the symposium will be a lessons learned document that will be presented to US legislators in order to fund the initiative.





**Why are you failing as president (once asked by a reporter to unknown nation state leader)?**

“The issue is that we are failing to build an institution that can outlive the personalities within it”

- a. Institutions are built without boundaries and borders ensuing in chaos.
- b. Balance between going fast and going slow to go fast
  - a. Strategic slowness? Some bureaucracy is helpful. Preferably as little as possible to find a balance between cost, assurance, and convenience.

**Mentimeter**

A lot of people who are experts that are introverts do not share their knowledge and expertise. This platform is for introverts to share their thoughts.

Slides:

<https://www.mentimeter.com/app/presentation/n/blg5b61ahpp95avzyba1tp5kqgjib45r/edit?source=share-modal>

Results:

<https://www.mentimeter.com/app/presentation/n/blg5b61ahpp95avzyba1tp5kqgjib45r/edit?source=share-modal>

Homeland Security – scan this to be added to email list

Join Digital Identity conversation

**DHS Goal:** Streamline the acquisition and use of centralized credentials by leveraging the convenience of biometrics.

Government as issuer and verifier of VCs.

**Concerns:**

Architectural difference is about digital VCs that phone home to the government (surveillance concern) versus paper VCs (passport) that don't phone home.

**Ideal operational state:** Person can use single digital ID to obtain access to all local, state, and federal benefits & services without having to revisit centralized locations and/or resubmitting paperwork with valid info already presently associated with that ID.

**Word Cloud Activity**

What are the challenges/needs standing in the way of an ideal state? If you see a word and agree, add it again.

Interoperability

Privacy

Decentralization

Standards

Usability

Wallet

Schema

Trust

Legislation

Bureaucracy

What percent increase in fraud is expected for this level of convenience nationwide? Enter a numeral from 0-100.

10

40

-100

Digital credentials actually mitigates fraud, so it is expected to increase authentication, which reduces or eliminates fraud.

“Road to Hell is paved with good intentions”

**Comment:** Europe as an inspiration for US Identity VC development

Concern/Rebuttal: US not like EU, have 50 states with their own rights

Place top challenges where you think they belong:

1. Interoperability

2. Privacy

3. Standards

4. Usability
5. Decentralization
6. Offline
7. Wallet
8. Schema
9. Bureaucracy
10. Legislation

**Comment:** Govt Go Fast doesn't seem to be happening as fast due to these challenges. Maybe it's not a good idea to go fast, because it might not happen the right way.

Time horizon – pilot within 2 years.

Concern: It's too close to the end of the internet, per AI.

Comment: AI solutions to help with force multiplier to go faster

What are the top 3 solutions/organizations currently best suited to address priority #1 (interoperability)

1. Government
2. Legislators
3. IETF
4. Kantara
5. W3C
6. TOIP
7. OpenID foundation

Bureaucracy is useful in some purposes such as mitigating too much centralized power amongst department agencies. When serving the public, it may be important to go faster when working with distributing SS payments.

**Comment:** Late mover advantage, after other countries have developed their identity programs.

**Comment:** Slow and fast in terms of psychology, how we handle disagreements. Slowing down to think about everyone and inclusion and its effects, pulling back to a conservative, slow approach.

**What are the top 3 solutions/organizations currently best suited to address priority for #2 Privacy?** Symposium with privacy papers for government review:

**Comment:** Privacy is a pain point for companies and that's why they are looking after themselves, but otherwise they don't care about privacy.

**What are the top 3 solutions/organizations are currently best suited to address priority #3 Standards**

TOIP, DIF, ETSI, ISO, digital fiduciary assoc, cen, mdl

### **Top 3 for Usability**

IETF TOIP DIF

UI/UX

ECOS

Comment: QR codes create a lot of attack vectors

### **#7 Wallet solutions**

Comment: Wallet is least important part of the whole system.

Government of the City of Buenos Aires – Quark ID, open source

### **#8 Schema**

Properties needed

Use 1 digital application

Selective Disclosure

Progressive elision

Minimum standards

Scheme dot org – open source

Comment: role of nlp and ai, mapping to scan natural language in fraudulent application

Response: agreed, it is a major concern. 1 to many situation, where multi-state fraud is being committed, where federal database of fingerprints can help mitigate.

### **Support for #9 Bureaucracy**

Management of bureaucracy –

Singapore

EFF

Blockchain

Taiwanese government – centralized

### **Support for #10 Legislation**

Linda Jeng

Kim Duffy

Chris Allen

Texas

DAO framework

State or Country that has launched a digital ID and changes they are dealing with past launch

Colorado

Estonia

CA

India

Utah

Wyoming

Singapore



Bhutan  
City of Buenos Aires  
Czech Republic

### Slide 1

<b>Date</b>	2024-10-31
<b>Session</b>	1
<b>Type</b>	slide
<b>Title</b>	Slide with Text
<b>Respondents</b>	1

No votes for this session

### Slide 2

<b>Date</b>	
<b>Session</b>	1
<b>Type</b>	slide
<b>Title</b>	Slide with Text
<b>Respondents</b>	0

No votes for this session

### Slide 3

<b>Date</b>	2024-10-31
<b>Session</b>	1
<b>Type</b>	slide
<b>Title</b>	Gov't Go Fast:
<b>Respondents</b>	6

No votes for this session

### Slide 4

<b>Date</b>	2024-10-31
<b>Session</b>	1
<b>Type</b>	slide
<b>Title</b>	Slide with Text
<b>Respondents</b>	1

No votes for this session

## Slide 5

<b>Date</b>	2024-10-31
<b>Session</b>	1
<b>Type</b>	slide
<b>Title</b>	Please join the DHS- Office of Biometric Identity Mgmt. (OBIM) mailing list
<b>Respondents</b>	1

No votes for this session

## Question 6

<b>Date</b>	2024-10-31
<b>Session</b>	1
<b>Type</b>	wordcloud
<b>Question</b>	What are the challenges/needs standing in the way of an ideal state? If you see a word and agree, add it again. Also try to add a unique challenge.
<b>Respondents</b>	13

### Responses

---

Fraud  
Identity\_theft  
Wallet  
Communication  
Readers  
Verifiers  
Value  
Interoperability  
Funding  
Planning  
Schema  
Decentralization  
Institutions

Bureaucracy  
Privacy  
Adaptability  
Trust  
Wallet  
Privacy  
bureaucracy  
privacy  
Legislation  
Decentralization  
Privacy  
interoperability  
offline  
Identity\_is\_hard  
privacy  
Usability  
decentralization  
interoperability  
privacy  
Trust  
interoperability  
Schemas\_for\_non\_mdI\_ID  
Interoperability  
standards  
offline  
privacy  
Interoperability  
interoperability  
Decentralization  
Usability  
Resilience  
Legislation  
usability  
Standards  
Principals\_of\_federalism  
Offline  
Wallet  
Schema  
Credential  
Interoperability  
overthinking  
delegation  
usability  
interoperability  
standards

Trust\_registry  
standards  
standards  
Offline  
standards  
standards  
Usability  
standards  
schema  
schema  
schema  
schmea  
schema  
Privacy

**Question 7**

**Date** 2024-10-31  
**Session** 1  
**Type** wordcloud  
What percent increase in fraud is expected for this level of convenience nation wide? Enter a numeral from 0-100.  
**Question**  
**Respondents** 14

**Responses**

---

Government 10  
40  
-100  
25  
-100  
-40  
-101  
-25  
-98  
-25  
-50

DHS\_SVIP

**Question 8**

**Date** 2024-10-31  
**Session** 1  
**Type** rating  
**Question** Place the top challenges where you  
**Respondents** think they belong  
 9

**Choices**

**Order of implementation**

---

Interoperability	4.333333333
Privacy	1.444444444
Standards	3.444444444
Userability	4.555555556
Decentralization	3.222222222
Offline	4.111111111
Wallet	5.555555556
Schema	4.888888889
Bureaucracy	3.111111111
Legislation	5.888888889
Add item 11	0

**Question 9**

**Date** 2024-10-31  
**Session** 1  
**Type** wordcloud  
**Question** What are the top 3  
**Respondents** solutions/organizations currently best  
 suited to address priority #3 Standards?  
 9

**Responses**

ISO ToIP

DID\_Foundation DIF DIF  
Itu Etsi Cen  
toip ietf dif  
Digital\_Fiduciary\_Assoc DIF W3C  
mDL VC DIF  
W3C  
iso ietf openid\_federation  
Lei Vlie

### Question 10

<b>Date</b>	2024-10-31
<b>Session</b>	1
<b>Type</b>	wordcloud
<b>Question</b>	What are the top 3 solutions/organizations currently best suited to address priority #1 Interoperability?
<b>Respondents</b>	12

### Responses

Government Legislators Government  
IETF Kantara OpenID\_Foundation  
toip ietf w3c  
Aamva  
Digital\_Fiduciary\_Initiat  
Works\_Wide\_Web\_Consortium  
Internet\_identity\_worksho  
DHS\_SVIP  
Iso Oidf NIST  
tan\_tan OpenID W3C  
DID\_Foundation DIF DIF  
openid\_foundation ietf iso  
Bhutan\_NDI IIW Identity\_Wowan  
IETF Global\_Acceptance\_Net EUDI\_Large\_scale\_pilot

### Question 11

<b>Date</b>	2024-10-31
<b>Session</b>	1
<b>Type</b>	wordcloud

**Question**  
**Respondents**

What are the top 3  
solutions/organizations currently best  
suited to address priority #2 Privacy?  
8

**Responses**

---

eff keri toip  
Privado\_ID did-iden3  
Enisa  
Digital\_Fiduciaries Lynn\_Parker\_Dupree Scott\_David  
Selective\_Disclosure Liability\_Limiting Legislation  
openid\_foundation keri eff  
PIMS Education Legislation  
Ctr\_fr\_democracy\_and\_tech EFF

**Question 12**

**Date**  
**Session**  
**Type**

2024-10-31  
1  
wordcloud  
What are the top 3  
solutions/organizations currently best  
suited to address priority #4 Usability?  
7

**Question**  
**Respondents**

**Responses**

---

toip dif ietf  
ToIP UI\_UX\_experts  
Privado\_ID Altme\_Wallet  
Legendary\_Requirements DIF  
Interoperability\_plugfest  
User\_testing Focus\_groups Ecoes  
tan\_tan  
openid\_federation ietf ui\_ux\_experts

**Question 13**

**Date**  
**Session**  
**Type**

2024-10-31  
1  
wordcloud  
What are the top 3  
solutions/organizations currently best

**Question**

suited to address priority #5  
decentralization?  
5

**Respondents**

**Responses**

---

KERI  
Digital\_Fiduciaries DIDs Verifiable\_Credentials  
DID\_Foundation Ethereum\_Foundation DIF  
LACNet EBSI  
keri toip ietf

**Question 14**

**Date** 2024-10-31  
**Session** 1  
**Type** wordcloud  
What are the top 3  
solutions/organizations currently best  
suited to address priority #6 offline?  
**Question**  
**Respondents** 5

**Responses**

---

Nfc Ble Adhoc\_wifi  
keri verifiable\_credentials  
Altme\_wallet Privado\_ID\_mobile\_app  
MOSIP QR  
QR\_Codes

**Question 15**

**Date** 2024-10-31  
**Session** 1  
**Type** wordcloud  
What are the top 3  
solutions/organizations currently best  
suited to address priority #7 wallet?  
**Question**  
**Respondents** 5

**Responses**

---

tan\_tan  
Open\_wallet\_Foundation KERI\_compatible\_wallets  
Altme\_wallet Privado\_ID\_wallet Quark\_ID  
CA\_DMV Veres\_Wallet Ledger



### Question 16

**Date** 2024-10-31  
**Session** 1  
**Type** wordcloud  
What are the top 3 solutions/organizations currently best suited to address priority #8 schema?  
**Question Respondents** 7

#### Responses

---

Selective\_disclosure Progressive\_elision  
schema\_dot\_org Minimum\_standards  
DL\_Edu\_I\_and\_W\_forms  
Basic\_person\_schema\_DIF  
Did\_foundation\_schemas\_wi  
did selective\_disclosure ssi  
Human\_centric\_schema MyData\_Global  
Did selective\_disclosure  
Predii

### Question 17

**Date** 2024-10-31  
**Session** 1  
**Type** wordcloud  
What are the top 3 solutions/organizations currently best suited to address priority #9  
**Question Respondents** 7  
bureaucracy?

#### Responses

---

eff  
Christopher\_Allen Kim\_Hamilton\_Duffy  
Diego\_Fernandez\_-\_Argenti  
Digital\_Fiduciaries IETF Singapore  
ietf Singapore eff  
Bhutan\_Digital\_Identity\_i  
DHS\_for\_National\_ids EUdi

Question 18	
<b>Date</b>	2024-10-31
<b>Session</b>	1
<b>Type</b>	open
<b>Question</b>	Name a State or Country that you know has successfully launched a digital ID and changes they are dealing with post launch.
<b>Respondents</b>	8
Responses	Upvotes
Estonia	0
City of Buenos Aires, Argentina. Supporting older smartphones.	0
India	0
Bhutan NDI integrating with other countries, so adjusting for localization modules	0
California. Dealing with multiple standards and presentation. Relying party adoption is limiting citizen value.	0
Bhutan - citizen ID in progress; organizational credentials to come	0
Utah and Wyoming are working digital ids	0
United States. PIV card. Too expensive. Too limited.	0
State of Colorado	0
India's implementation of digilocker ( wallet by central gov) but has only xml and pdfs. Many states of India are struggling to get customisations done leading the states to drop off the initiative	0
Belgium itsme	0
Us piv card	0
Digital Bazaar	0

Question 19	
<b>Date</b>	2024-10-31
<b>Session</b>	1
<b>Type</b>	wordcloud
<b>Question</b>	What are the top 3 solutions/organizations currently best

suitied to address priority #10  
legislation?  
7

**Respondents**

**Responses**

---

Christopher\_Allen Kim\_Hamilton\_Duffy  
eff toip  
Aamva EUDI  
California Texas eff  
EFF ACLU Dazza\_Greenwood  
Cftb\_fines  
CFpb algorithmic\_law

**Slide 20**

**Date**  
**Session** 1  
**Type** slide  
Please join the DHS- Office of Biometric  
Identity Mgmt. (OBIM) mailing list  
**Title**  
**Respondents** 0

No votes for this session

**Question 21**

**Date** 2024-10-31  
**Session** 1  
**Type** open  
Shout-out! Post your (or someone  
else's) website, company, name, and  
which challenge they can help with.  
**Question**  
**Respondents** 6

**Responses**

---

**Upvotes**

Diego Fernandez - Quark ID -  
fernandezdiego@gmail.com 0  
National Association of Convenience Stores - TruAge  
age verification program 0  
Jorge A. Ortiz  
tan tan  
jorge@tantan.solutions 0

1-USCIS for immigrants documentation  
 2-National Students Clearinghouse for Education  
 credentials 0  
 JFF 0  
 Jobs for the Future 0  
 jorge@tatan.solutions 0  
 DataSapien, Shane Oren at id\verse for document and  
 liveneas testing, PRIVO for age compliance and  
 assurance, jobs for the future, 0  
<https://digitalfiduciary.org>

Can help establish decentralized identity assurance  
 protocols that fundamentally respect individual  
 privacy while achieving 100% post facto  
 accountability. 0  
 DIF - Otto Mora - Privado ID - otto@privado.id 0

**Slide 22**

**Date**  
**Session** 1  
**Type** slide  
**Title** Slide with Text  
**Respondents** 0

No votes for this session

End of notes.

## SESSION #12

### RP Auth & EUDIW Part 2

Session Convener: Torsten Lodderstedt

Session Notes Taker(s): Dima Postnikov

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

Requirements (from the legislation)

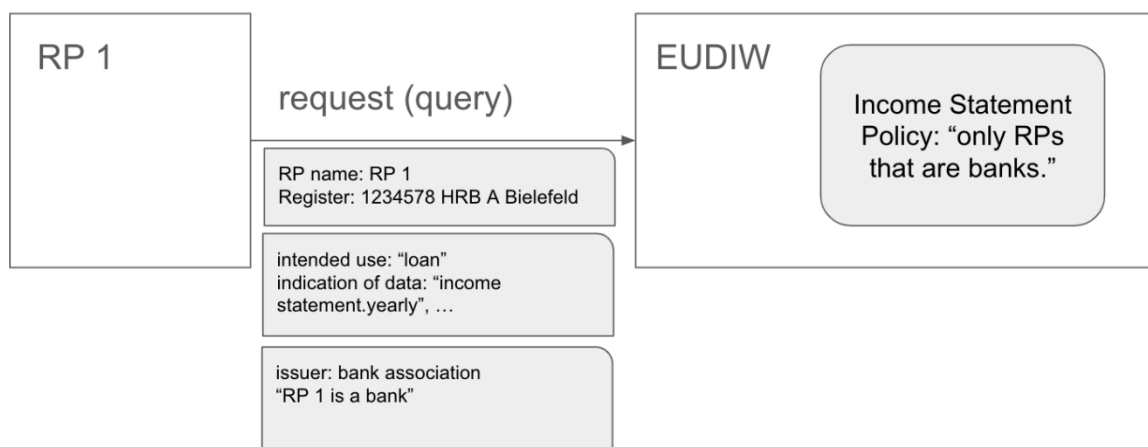
#### 1. Authentication

- RPs shall register with Member State
  - Name, register number
  - Intended use + indication of the data to be requested by the relying party from users
- Member state publishes RP data
  - allows inspection by interested third parties
- RP needs to authenticate with the EUDIW
- Wallet needs to check whether a certain presentation request matches the registered “indication of the data to be requested by the relying party from users”
- Objective: creation of transparency

#### 2. Authorization

- PID & EAA Providers may govern access to PID/EAA data through embedded disclosure policies.
- Policy must be matched to RP role/permission attestation

## RP Authentication + Authorization

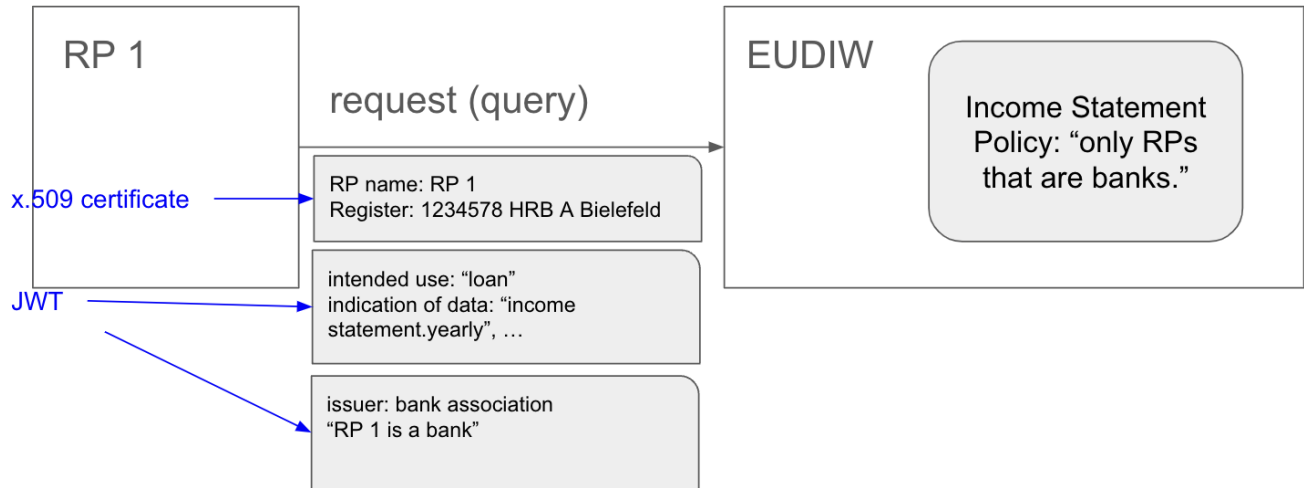


1 and 3 are verified  
 2 self declared but signed by the register  
 protocol - openID4VP

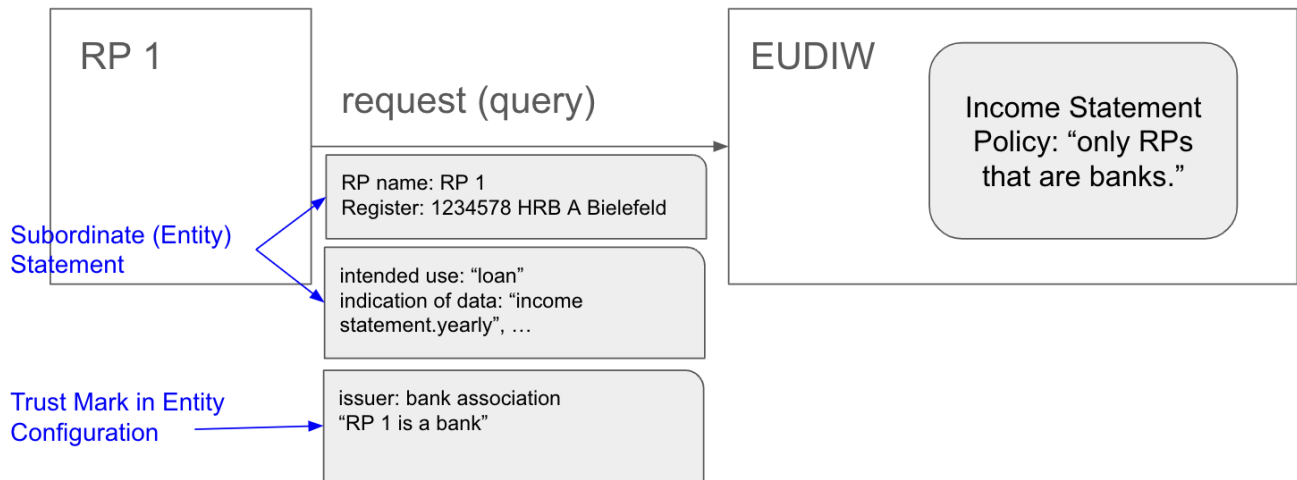
RP has a certificate to authenticate

Proposal 1 based on x.509

Proposal 2 based on x.509 and JWT



Proposal 3 based on OpenID Federation



<https://github.com/openid/federation-wallet/issues/39>

### Comparison

- X.509
  - Access Certificate and Authorization Certificate are both x.509 certs
  - Need extension to x.509 cert to include intended use, and most likely, for roles and permissions of the RP

- requires extensions x.509 scheme, OpenID4VP and 18013-5 to pass a second x.509 cert
- OpenID Federation
  - Access Certificate
    - name, register number, ...: entity configuration + entity statement
    - intended use: entity configuration
  - RP Authentication either with entity id in client\_id (OID4VP) or in x.509 cert (18013-5)
- (SD-)JWTs as attestations
  - client id scheme verifier attestations
  - Access Certificate and Authorization Certificate are (SD-)JWTs
  - ISO 18014-05

	<b>Option A) x.509</b>	<b>Option B) OpenID Federation</b>	<b>Option C) (SD-)JWTs as attestations</b>
<b>Access Certificate</b>	x.509 cert	<ul style="list-style-type: none"> <li>• name, register number, ... in entity configuration + entity statement</li> <li>• intended use in entity configuration</li> </ul>	(SD-)JWT passed in client id scheme verifier attestations
<b>Authorization Certificate</b>	x.509 cert	Trust Mark	(SD-)JWT passed in client id scheme verifier attestations
<b>RP Authentication</b>	client_id_scheme: x509_san_dns	either with entity id in client_id (OID4VP) or in x.509 cert (18013-5)	client_id_scheme: verifier_attestation

<b>other</b>	<ul style="list-style-type: none"> <li>• Need extension to x.509 cert to include intended use, and most likely, for roles and permissions of the RP</li> <li>• requires extensions x.509 scheme, OpenID4VP and 18013-5 to pass a second x.509 cert</li> </ul>		
--------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

***The 7 Privacies or How our misconception of Privacy Preserving Tech prevents a full solution. - Ugly Baby Pagent***

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

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

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

NO NOTES SUBMITTED

***A gentle CRDIs into to (the foundation of local-first SW)***

**Session Convener:** Christian Tschudin  
**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



## *Data Coops with JLINC*

**Session Convener:** Brad deGraf + Jim Fournier

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

## *Exploring Remarkable Regenerative Patterns of IETF: What do its governance practices have to teach us for our ID communities protocol work.*

**Session Convener:** Kaliya Young, Day Waterbury

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

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

Kaliya and Day were funded by the Summer of Protocols which is a project of the Ethereum Foundation to study the IETF and its protocols for protocol creation.

Slides for the Session:

[IIW Preso IETF Research](#)

Paper about the IETF:

Exploring the Remarkable Regenerative Patterns and Practices of the Internet Engineering Task Force (IETF)

[IETF - Research Almost Complete Draft](#)

## ***Identity in Telecom 101: STIR/SHAKEN, Rich Call Data & Authenticated Communications***

**Session Convener:** Pierce Gorman

**Session Notes Taker(s):** Pierce Gorman & Sam Etlar

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

RFC 8224 Authenticated Identity Management in the Session Initiation Protocol (SIP)

<https://datatracker.ietf.org/doc/rfc8224/>

RFC 8588 Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN)

<https://datatracker.ietf.org/doc/rfc8588/>

ATIS-1000074 Signature-based Handling of Asserted information using toKENs (SHAKEN)

[https://access.atis.org/apps/group\\_public/download.php/67436/ATIS-1000074.v003.pdf](https://access.atis.org/apps/group_public/download.php/67436/ATIS-1000074.v003.pdf)

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

Reviewed slides (below). Discussed that STIR/SHAKEN is voice call authentication technology applied to Session Initiation Protocol (SIP) as required by the US Traced Act and several US Federal Communications Commission (FCC) mandates. Mentioned that SHAKEN has been largely ineffective in terms of providing a source of automated traceback or as an important input to anti-robocalling analytics designed to combat illegal robocalling. i.e., anti-robocalling analytics largely ignores STIR/SHAKEN call authentication. Regardless, STIR/SHAKEN has provided a foundation for more interesting use cases such as authenticated content in so-called “branded calling” which uses a Rich Call Data (RCD) Personal ASSertion Token (PASSporT) to carry “claims” such as company name, logo, and reason for calling, to be displayed on the dialer application of mobile phones, for example. There are multiple PASSporT types including shaken, div(ersion), Resource Priority Header (RPH), msg, rsp, and Rich Call Data (RCD). There are challenges to including trust attribute information with PASSporTs and X.509 certs which may be better supported using Verifiable Presentations. Mutual authentication and authentication for RCS messaging are important use cases which remain outstanding.

# Identity in Telecom 101

STIR/SHAKEN, Rich Call Data, & Authenticated Communications

## STIR/SHAKEN – a very short primer

- Secure Telephone Identity Revisited (STIR) working group in IETF
  - Revisited RFC 4474bis “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)”
  - Defined a “base” STI Personal ASsertion Token (PASSporT) JWT
  - Later defined extensions to the base...
    - SHAKEN ppt
    - DIV ppt
    - RPH ppt
    - MSG ppt
    - RSP ppt
    - RCD ppt
    - Verified Sti PERsona (VESPER) in progress based on SD-JWT

## STIR/SHAKEN – a very short primer continued

- Alliance for Telecommunications Industry Solutions (ATIS)/SIP Forum Joint Task Force on IP-Network-to-Network Interconnection (IP-NNI)
- ATIS-1000074 “Secure Handling of Asserted information using toKENs (SHAKEN)”
- STIR defined the IDENTITY header in Session Initiation Protocol (SIP), and the “shaken” PASSPORT
- SHAKEN defined how the IDENTITY header and “shaken” ppt would be populated
- RCD (IETF Internet-Draft) defined how Rich Call Data should be represented
  - <https://datatracker.ietf.org/doc/draft-ietf-stir-passport-rcd/26/>



# Enhancing STIR/SHAKEN with Rich Call Data

```
{
 "alg": "ES256",
 "typ": "passport",
 "ppt": "shaken",
 "x5u": "https://cert.example.org/passport.pem"
}
{
 "attest": "A",
 "dest": {"tn": ["12125551213"]},
 "iat": 1471375418,
 "orig": {"tn": "12155551212"},
 "origid": "123e4567-e89b-12d3-a456-426655440000"
 "nam": "Numeracle"
 "rcd"
 {
 "crn": "Calling about your invoice"
 "icn": "https://logo-repository.Numeracle.com/acctspayable-logo.bmp"
 }
 { signature }
```

## Beyond STIR/SHAKEN...

- Plethora of PASSporTs (shaken, rcd, div, RPH, msg, rsp)
- Layered Identity Problem
  - Companies hire robocallers
  - Robocallers call for lots of companies
  - How do you know the robocaller is an authorized agent of the brand?
  - How do you know the robocaller has consent to call the subscriber?
  - How do you know the robocaller is licensed by the state they operate in?
  - How do you know the robocaller (and their agent) is insured with security bonds?
  - Who authorized the calling telephone number?
    - Carrier
    - TNSP
    - Brand
    - Robocaller
- What about *mutual* authentication?

# Beyond STIR/SHAKEN...

- X.509
  - STI-GA, STI-PA, STI-CAs
  - STI-GA Certificate Policy v1.4
  - Subordinate CAs and Delegate Certificates
  - Certificate Transparency Logs
- VESPER SD-JWTs
  - <https://datatracker.ietf.org/doc/draft-wendt-stir-vesper/>
  - Notary Agent, Claim Agent, Claim Graph, Transparency Log
  - And many other things that may not belong in an IETF spec 😊
- Beyond...
  - VCs, DIDs, DNS, ISO-17442, Branded Calling, Mutual Authentication, Rich Communications Services (RCS) Message Authentication

## *Self-Describing DID Methods - OR - Decentralizing DID Method Names*

**Session Convener:** Kevin Dean  
**Session Notes Taker(s):**

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

Document and discussion on GitHub: [https://github.com/LegReq/Self-Describing\\_DID\\_Methods](https://github.com/LegReq/Self-Describing_DID_Methods)

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

- DID method name centralization through the DID extension registry goes against the ethos of DIDs themselves.
- Name conflicts present a real risk for long-lived DID methods.
- Changes to DID methods to incorporate new features or address deficiencies often require new DID method names with no way to advertise correlation between old and new names.

### ***Cloud Wallet Architecture - come discuss***

**Session Convener:** Patrick St. Louis  
**Session Notes Taker(s):**

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

NO NOTES SUBMITTED

### ***How we lose the Attention Wars?***

**Session Convener:** Aaron Goldman  
**Session Notes Taker(s):**

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

NO NOTES SUBMITTED

### ***Election / Voting System Using VCs - Let's Build One!***

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

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

NO NOTES SUBMITTED

### ***Payments & Identity: Past, Present & their increasingly linked future***

**Session Convener:** Tony Lopreinto  
**Session Notes Taker(s):**

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

NO NOTES SUBMITTED

## ***GOV'T GO FAST Part 2: Challenges + Ways Forward***

**Session Convener:** Tchaikawsky “Troy” Samuels and Shannon Johnson

**Session Notes Taker(s):** Otto Mora

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

Type Here

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

Please see session notes for “Session 11 / Space M Session Title: GOV'T GO FAST Part 2: Challenges + Ways Forward”. This session was part of that.



## SESSION #13

### *Digital Credentials API: Updates & Demos*

Session Convener: Tim Cappalli  
Session Notes Taker(s):

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

Slides: <https://tclslides.link/iw39-dcapi>

<https://digitalcredentials.dev>

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

This session was primarily level setting and a bunch of live demos. Slides are above.

### *KERI Security II - AI Safety Verifiable Agents*

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

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

Type Here

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

NO NOTES SUBMITTED

## OpenID Federation 2.0

Session Convener: [Alex Tweeddale](#), Dima Postnikov

Session Notes Taker(s): [Ankur Banerjee](#)

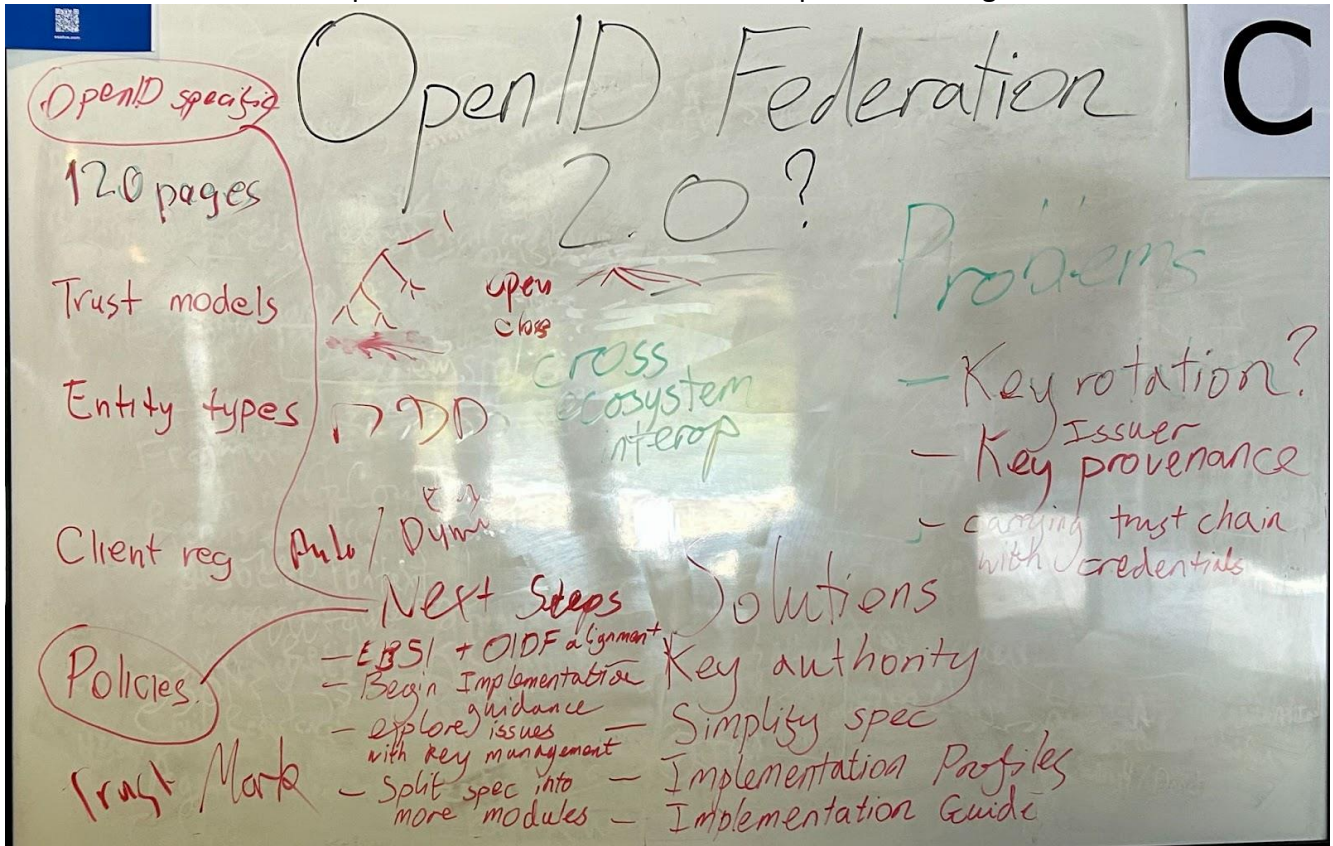
Tags / links to resources / technology discussed, related to this session:

- [OpenID Federation 1.0](#)

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

- Generic framework for bridging trust between different ecosystems
- What does the OpenID Federation have
  - Trust models
    - Open or closed systems. E.g., of such system is Open Banking
    - Usually a flat hierarchy
  - Entity types
  - Client registration
    - Automatic, dynamic
    - Some use static
  - Policies
  - Trustmarks
- Open Banking is a great example
  - Many jurisdictions like UK, Australia, Brazil doing it
  - [FAPI](#) and Security profile
- Brazil OpenID Federation
  - Open Finance and Open Insurance ecosystems interoperate with each other has a lot of advantages
  - Manual registration is hard to coordinate
- Key rotation is a problem and who keeps the keys in a tree model
  - Say there's a credential issued today, and it's checked 1 year later. How can a relying party fetch from an authoritative archive to store key rotation history
  - (Whether correct or incorrect...) this is the reason why EBSI went down using DID Documents, since it has key rotation history
  - Maybe the holder's wallet could store some sort of trust chain history which can be used to validate
  - Including entire trust chain in every verifiable credential/presentation could have scaling issues
- Not changing the text, but modularising it
  - Split up the spec, multiple profiles
  - Have a standalone implementation guide because you can then change recommendations without changing the specification itself
- "How to build an ecosystem" spec?
  - Is this even a spec or is it an implementation profile?

- In Italy, they use Federation to automatically issue X.509 certificates
  - There's a separate document created as an implementation guide? With roles?



## ***OAuth Scopes vs Dynamic Authorization - Why can't we just get along??***

**Session Convener:** Omri Gazitt

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

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

Omri's "OAuth2 scopes are NOT permissions" [blog](#)

Vittorio Bertocci's "On the nature of OAuth2's scopes" [blog](#)

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

Generally, Scopes in an access token are good for a "delegated authorization" scenario where the *user* is at the center, and the user wants to delegate access from one application (a resource owner) to another application that can act on their behalf, but with a "scoped down" set of capabilities.

Generally, dynamic authorization is good for determining whether a user has permission to perform an action on a resource at this time. It is used when resources are fine-grained, and can be shared across multiple people. It is not generally used as a mechanism outside of the scope of a single application.

Some rules of thumb:

- Don't do scopes for individual resources
- Scopes are used to "scope down" access to a smaller subset of all available resources
- Scopes need to be understandable by a human
- OAuth2 focuses on a single user sharing resources across applications they own
- Dynamic authorization focuses on sharing (entitling other users to access data you own in the app), and the application enforcing those access rules
- OAuth tokens ought to contain information about the user, less about domain-specific things about the application
- Fine-grained authorization reasons about the domain model (in addition to the user)

## ***KYC, PASSKEYS & SECURING Customer data with Trinsic***

**Session Convener:** Michael Boyd & Mahesh Balan  
**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

## ***Personal AI (not personalized AI from giant services)***

**Session Convener:** Doc Searls  
**Session Notes Taker(s):** Doc Searls

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

Twelve pieces (so far) that Doc Searls has posted on Personal AI: <https://doc.searls.com/personal-ai/>

Kwaai: <https://kwaai.ai>

The slide deck is here: <http://searls.com/talks>

Consumer Reports' future work on personal AI will start with Permission Slip: <https://www.consumerreports.org/media-room/press-releases/2023/10/consumer-reports-introduces-free-permission-slip-by-cr-app-to-empower-consumers-to-take-back-control-of-their-personal-data/>

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

Doc reviewed his writing about the space, which Claude, ChatGPT and other BigCo chatbots made clear is almost free of development work outside open source models provided by Meta, et. al., and work by Kwaai. Because it's early, and nearly all the investment money is going to the bigs, enterprise, and AlaaS in general.

There was a discussion of possible AI help with ordinary life needs, without an agent.

## 5 Alternatives to WorldID/Worldcoin

**Session Convener:** Kaliya Young

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

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

Some reference links:

- [Deception, exploited workers, and cash handouts: How Worldcoin recruited its first half a million test users](#)
- [Worldcoin Under Scrutiny in Singapore Over Account Sales and Biometric Data Privacy Concerns](#)

**We talked about why we came to the session:**

- I wanna know about worldcoin
- I wanted to go to session Kaliya was moderating
- Biometrics
- Its terrible edge Biometrics
- Digital Fiduciaries.

**We started by briefly describing WorldCoin/WorldID**

Inspired by Aadhaar's system in India

One idea behind is to give individuals a Universal Basic income

Sybil Resistance via Iris Biometrics

1:N "proof of humanity" Hardware strong <- trust devices (Shouldn't)

"Everyone on Planet" No eyeballs | Religious Believes

One key binding to you "for life"

*We did several group brainstorming exercises.*

**HARMS from WorldCoin**

What about the "Right to be Forgotten"

How to Change my ID?

Inability to be forgotten

Ambient Identification

You can't always hide your eyes in public.

A type of Super Cookie -> Over Correlation

Context Collapse is Coercive

Risk of becoming a tracking vector between public and private and government spheres

Can they “cancel” your life? (blacklist)

People Don’t understand - what the technology does or how it works.

What about Non-Human Iris Registration for Fake ACcounts?

Before we get to WorldCoin - the first step is to reduce the cost of 1:1 - make edge matching better.

Corruption is Empowered - potentially by those who control the orbs.

Exploitation by GateKeepers - forced to use and pushing people to get enrolled

Tyranny of Data - deference to the system not the human in front of them.

The team creating the device doesn’t believe it can be attacked -there is a hubris on the engineering team.

Blessed Database in the Cloud is required for deduplication (even though the team denies it)

Contract Terms are

- Unclear
- Abusive
- Changinte

Changes Identity and Self Perception

Digital Gap 3 levels for access and skills

Persons and pseudonyms allowed?

Selective Zero Knowledge disclosure available?

Eyes Change (Physical injury) loss of Access

Lose Control if Iris Changes

Do Irises change significantly over time?

Physical threats?

Mandatory use of biometrics

REquires biometric enrollment: digitization of the body cannot be mandatory

Forced Body Digitization

Exclusion and Discrimination

Privatising Public Goods as Bad

Private Entity profit pressures and trustworthiness

Do we (the world and this community) trust this sponsor?  
Surveillance and trust in instruction

What about Post Quantum.

What will happen if Hardware is compromised

Users won't know about tampered devices until it's too late

Inadequate SafeGuards about misuse of data  
Over use of identity (too easy)

Mixing  
Key Binding  
Key Recovery

Iris Data gets Hacked and sold

Healthcare providers will demand increasing attack vectors

Scope Creep required for Welfare, banking, health, social

Dehumanisation Cannot prove my humanity

"proof of humanity" is problematic we don't have a set list of attributes for "humanity"

Access and Inclusion  
Exclusion from Services (Public Service)

Discrimination

---

## **ALTERNATIVES**

Nothing Digital  
Digital Fiduciaries (A New Profession)  
Trusted Social Webs - People know other people  
Localization

Verifiable Relationship Credentials with Social Graph

Bhutan NDI

AnyWise DIDs and renewable VCs  
SSI With Biometric Binding



biometrics Hidden in your passkey?

Non-mandatory diverse, minimal biometrics

Selective Disclosure (case- tailored ID)

Good Government Trust ID Issued - by state

multi-Stakeholder Governance

Governance -> NOT Sam Altman

Efficient Key Recovery / Management Solution

Proof of Presence (go to a place)

Accept the intractability of proving humanity

Proof of humanity

pros: Genomics hash - proves humanity much higher bar of consensus

Cons - invasive maybe hair is fine

Hardware as a public good

Edge Biometrics on attested open code in trusted

ID Commons

Layered ID System

Paper Solutions/Alternatives

UX and Government

What Why now

Mr. Sovereign State Recognize Digital Colonialism

Start with PQC Quantum Resistant Algorithm

Actually Tax Billionaires instead of selling another crypto to anyone that falls for it.

***Auth Z 201 - Current developments & new ideas for policy decent IAM.com***

**Session Convener:** Rohit Khare

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

***Copy Protected credentials in Decentralized Environment using Hardware Security Modules***

**Session Convener:** Andre Roder

**Session Notes Taker(s):**

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

Type Here

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

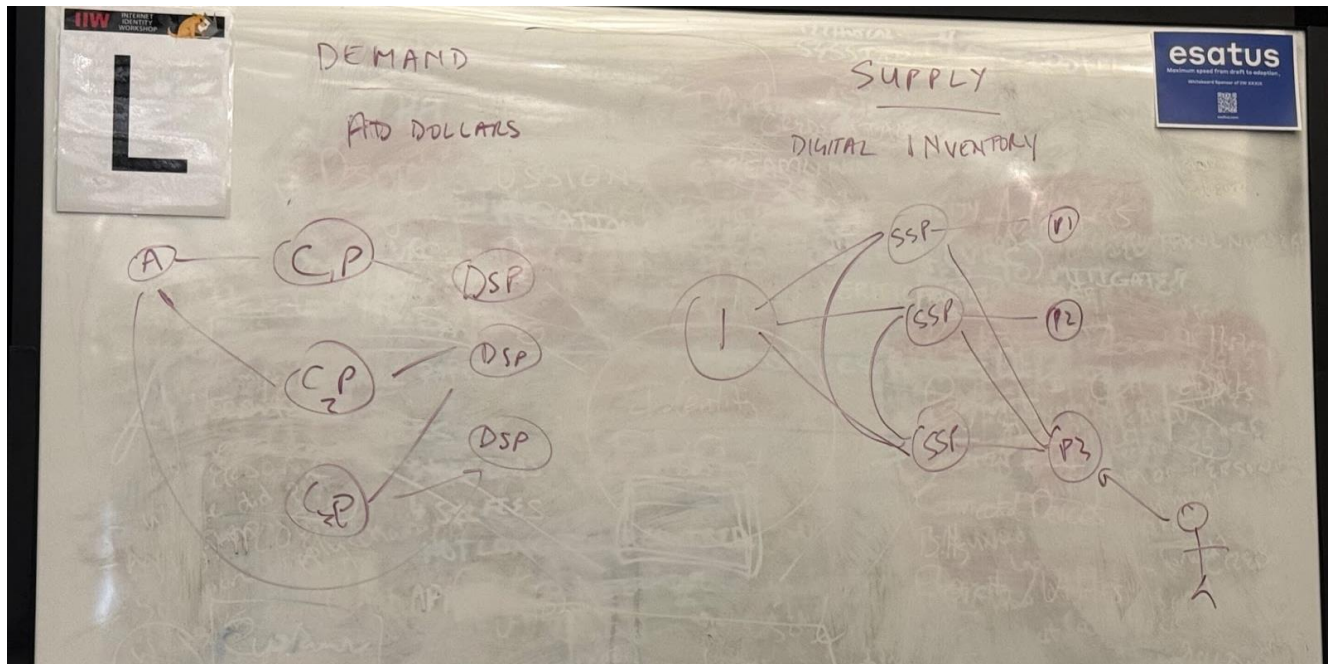
NO NOTES SUBMITTED

## Brainstorming Organizational Identity for Digital ADS Industry

Session Convener: Vinod Panicker - Amazon and Per Bjorke - Google  
Session Notes Taker(s): Phil Windley

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

Discussion started with ad network structure.



A - Advertiser

P - Publisher (web site)

CP -

SSP - Supply-side Platform

DSP - Demand-side Platform

I - Intermediary

**Key Question:** How do trustworthy parties distinguish themselves as such?

Talked about using LEIs to reduce ad fraud

1. Some ad fraud or malvertising is done by groups that aren't real businesses.
  - use LEI to prove they are real businesses
  - gives a global identifier
  - Create more transparency.
2. Digital vLEIs make this doable at scale
  - org-level credential
  - org-level plus person identity with role (campaign submitter)

3. Sign ad copy with credential to know who originated the ad
  - the signer takes responsibility for the submission
4. GLEIF relies on LEI issuers to attest that a particular org was formed in a specific jurisdiction
  - the issuer should ensure the applicant has signing authority for the business
5. This doesn't make fraud impossible, but raises the bar.
  - if specific jurisdictions are risky (allow businesses to be created cheaply with little friction) that can be taken into account in the ad network.
6. We can outsource KYC on businesses.
7. Use risk scores in the bidding algorithms.
8. LEI issuers set their own cost
  - sometimes depends on kind of entity
  - cheapest is \$50
  - renewal cost for each year and data is rechecked.
  - vLEIs have additional cost
9. Balance cost with access

### ***Did:btc1 Deep Dive***

**Session Convener:** Will Abramson

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

## ***Dazzle Update - Getting back personal data, Fediverse, what?***

**Session Convener:** Johannes Ernst

**Session Notes Taker(s):**

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

<https://dazzlelabs.net/>

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

Reviewed the original concept for Dazzle and the Data Palace concept, and how it evolved once the federated, open social web / Fediverse suddenly became viable again after the Twitter acquisition.

## Session #14

### *OIDC4 VCI Browser API Issuance Profile / OIDC4 VC presentation during issuance*

**Session Convener:** Joseph, Kristina, Sam, Mirko  
**Session Notes Taker(s):** Joseph

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

Slides used for VCI Browser API part, including two slides that contains the proposals discussed:

[https://docs.google.com/presentation/d/1MJc33dmXb2Yip2neo0gbWilmUZ1vpCDq1Ucy48GFG34/edit#slide=id.g310d3171d57\\_0\\_0](https://docs.google.com/presentation/d/1MJc33dmXb2Yip2neo0gbWilmUZ1vpCDq1Ucy48GFG34/edit#slide=id.g310d3171d57_0_0)

Slides for the presentation during Issuance: [https://docs.google.com/presentation/d/1tmCunR-HxTStLI7CS8tsre\\_LNjxr2GNO7OhfiZTlpgQ/edit?usp=sharing](https://docs.google.com/presentation/d/1tmCunR-HxTStLI7CS8tsre_LNjxr2GNO7OhfiZTlpgQ/edit?usp=sharing)

- some use cases demand to present a credential to actual get one (like presenting a student credential to receive a ticket)
- Both approaches with Pre-Authorized Code and Authorized Code Flow were presented
- Auth Code flow was chosen together with the First Party App spec since it allows as browserless user experience
- Google was able to give an answer to the problem how to talk to another wallet in case the first wallet was not able to fulfil the presentation request via the credentials apis

## ***Consumer/Service interaction in Travel is a Mesh, not a Supply Chain***

**Session Convener:** Neil Thomson  
**Session Notes Taker(s):** Neil Thomson

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

[Hospitality and Travel Wallet.pdf](#)

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

With travel and hospitality costs escalating, Hospitality (Hotels, Restaurants, Site Seeing) and Travel (Airlines, ...) needs to understand their customers better. And Travelers need to be able to capture and share their requirements, needs and wants/preferences and share that information while preserving their privacy.

The DIF Hospitality & Travel Special Interest Group is creating a travel profile, a schema, and a data exchange protocol for digital wallets to meet this need.

The presentation outlines the change in traveler/travel service interaction from a top-down tree from major on-line travel services down to the individual service providers to a mesh where both traveler and services can interact directly - decentralized - offering more choices for travelers and opportunities for specialized travel services.

The role of AI is also discussed, which points to all Parties (Traveler, Services) having their own "high level" agents ("Concierge Model"), with more specialized agents filling specific roles (e.g., personal data privacy and selective disclosure agent, personal accessibility needs agent, ...)

## ***How do we all run engineering & product teams in ID companies? Swap advice and stories on what works ("do we hate agile"), etc***

**Session Convener:** Ankur Banerjee  
**Session Notes Taker(s):** [Ankur Banerjee](#)

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

We discussed stories of what has worked and what doesn't work in our teams.

- Linear, ClickUp vs Jira, Azure DevOps/Team Foundation Server

## *The HumanOS Stack - How You Evolved Your Digital Identity*

**Session Convener:** Jeff Orgel

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

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

This session presented a thought model which intended to share and build language that could identify the various stages of relationship between human and connected information technology (IT) systems. It also looked to identify the different phases and details likely related to the different phases.

Visually this model is a pyramid type stack with five (5) levels. From the bottom up they are named @0, @1, @2, @3, @4. Each level represents a stage of the relationship. How you navigate, and the decisions you make in that journey, will form the digital DNA-building blocks of your digital identity. This will also impact on your ability to move through this landscape more in charge of, than owned by, the forces in this digital realm. In Real World (RW) we might ask;

“Who’s wearing the leash and who’s wearing the collar?” Are you taking tech out for a walk where you want to go or is IT taking you for a walk where IT wants to go?!

Over-simplified these stages would be roughly described as;

**@0: Before** - human experience with no exposure to connected systems. Examples may be newborn, deeply isolated cultures and all of us pre-1990’s. People who remember saying or hearing someone say, “Have you ever tried the web?” or “Have you been online yet?” would be what is known as a “digital immigrant”, per Marc Prensky. Those who’ve never heard such a thing said are likely “digital natives”, again per Prensky. They were born in a world where that relationship and entanglement has been a matter of fact mostly since birth. They were born into the stage of @1.

**Between @0 and @1** - is the Boundary Line of Awareness and/or Access. After this boundary is crossed in either or both senses, pure @0 is difficult to return to if not impossible.

**@1: Procreative Stage** - awareness of the digital landscape begins for many as a strong attraction which animates the idea of using connected systems. A key value of this stage may be that it delivers awareness that something new – a relationship entanglement – is in the room with you.

**@2: Developmental** – here the inevitable relationship with active systems forms. The Give & Take relationship surfaces rules, strengths and weaknesses present themselves.

Here the Real-IT<sup>®</sup> and the HumanOS<sup>™</sup> bloom more or less so based on numerous idiosyncrasies. Real-IT is the relationship we choose to have, or not to have, with information technologies and connected systems. *Your Real-IT relationship choices will reflect into your*



*Reality*. The Key value here is understanding the synergy between the @0 world designed by nature for people, and the forces impacting and influencing in your life @1. The HumanOS is reviewed in the next stage @3.

**@3: Maturation** – the refinement of the relationship begins. Crafting of your digital You begins to manifest driven by better understanding of the Real-IT<sup>®</sup> relationship and the HumanOS<sup>™</sup> perspective. Whether your digital twin will be more in your control - or more of a system's marionette - will reflect what does or doesn't happen at this level. Actionable sensibility is key here. Additionally, this level stays in touch and responds to the Give & Take relationship occurring @2. This is because systems are often changing and how we choose to respond affects choices we may make. At this level a person is ideally able to put their relationship choices, referred to as one's Real-IT<sup>®</sup>, into a proportion and balance that will allow for comfort and control and reflect comfortably into their Reality. The balance and degree of comfort achieved is related to the HumanOS's<sup>™</sup> alignment with the individual's wants and needs and how those intentions deliver positive outcomes to one's life.

**@4: Outcome** – How is Your Real-IT<sup>®</sup> reflecting Into Your Reality? How is your You-X\*<sup>™</sup>! The You as a Human having an eXperience related to technologies touching your day, and night - here and there...more or less... Key elements are;

**Control** – owning communication and command of the space

**Safety** – sense of Privacy, Security and respectfulness of those technologies

**Comfort** – how is the pace of the relationship considering all your feeds and accounts, etc.

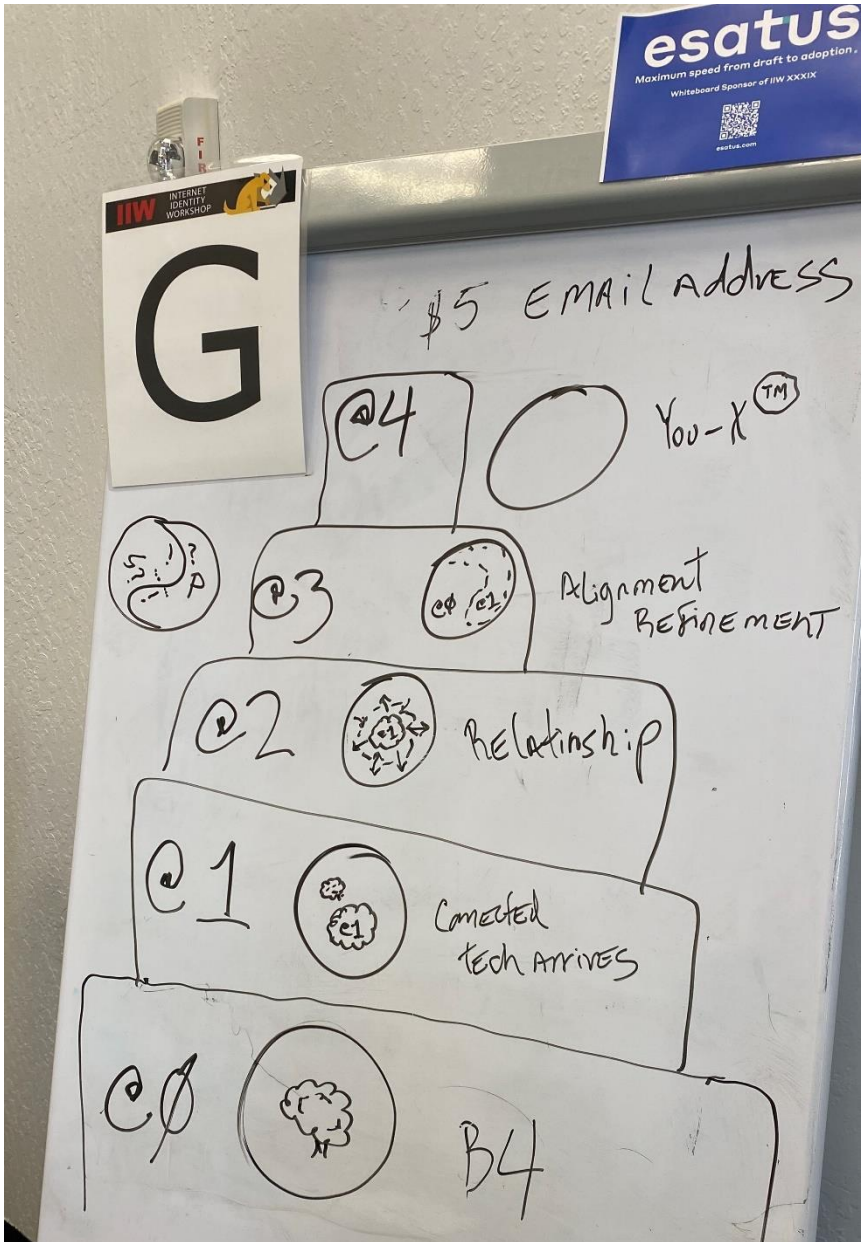
How does the load feel? *Are you feeling accomplishment of your intentions without dodging or being impacted by hazard, loss or harm?*

Expanded Language Definitions:

\* **Real-IT<sup>®</sup>** – the relationship we choose to have, or not to have, with information technologies (connected systems) *Your Real-IT relationship choices will reflect into your Reality.*

\*\* **HumanOS<sup>™</sup>** – represents *the idea of an emulator mode in the sense that people try to align real world experience/wisdom with their Sense of Self (SoS) on the other side of the glass, @1.*

\*\*\* **You-X<sup>™</sup>** – The You eXperience (You-X) How you are doing having a leg on both sides of two different worlds. One world appears as wind, light, earth and gravity and another world on the other side of glass, which appears as a device screen. One side is a world that is built for us by nature, and one world is built for us by us and only accessible via crossing glass. The UX (User eXperience), a common phrase in software design, is regarding studying how people feel using IT systems. The You-X focuses on the experience of being a human with a foot in two different realms – the realm of natural world and a realm of human built system forces - on the other side of glass.



## Trust Registries 101

**Session Convener:** Dmitri Z  
**Session Notes Taker(s):**

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

A trust registry is a governed, authoritative list defining how entities are authorised to perform specific actions within an ecosystem's governance framework.

In the session, participants explored trade-offs and challenges related to the longevity of Verifiable Credentials and their representation within a trust registry.

For a comprehensive list of trust registry technologies, visit: [Awesome Trust Registries](#).

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

#### Trust Registries 101

*VC Longevity and Lifecycle planning*

#### Goal of this talk

- 1) explain trust registries
- 2) explain longevity: what to do when government or institution goes away

#### Basic Definitions/concepts

- *Trust Registries (TR)*: an attestation authority (hierarchical tools apply)
- *Verifiable Credential (VC)*: a claim
- *Longevity*: verifying a credential after the issuer no longer exists

#### I.3 components of VCs

- 1) Meta tag: about VC
- 2) Some claims: (Fields) about subject
  - - Things we can claim: passports, drivers licences, etc.
- 3) Digital signature (seal)

#### Types of VCs - a spectrum of different values

Low value (Bearer VCs, coupons) <-----> high value (Holder Bindings, passports, etc.)

Low Threat

high reproducibility

50 cent off coupon

non-binding

High Threat

low reproducibility

passport, green card

binding

#### Non-binding (Bearer VCs) vs Holder Binding VCs:

- Bearer VCs (no holder ID) - those that can be copied (ie, coupons)

- VCs good at guarding against being stolen but not willingly shared therefore need one time use policies, revocation, etc.
  - No set correlation between Bearer vs and low value, just is
  - High value: linked to legal identity = Holder Binding
  - High level/high threat have additional binding requirements: hardware brand of device, manufacture of wallet, ensure that keys live on trusted wallet
  - Holder binding: options: legal identities (3-4 fields like name, birthdate, etc. for differentiation) to be bound to legal identity
- Bound to some holder key

### **Pseudonymous bindings: middle ground**

*Bearer VCs <—| pseudonymous binding |—> Holder Binding (Legal)*

- 1) Pseudonymous bindings: no legal requirement for legal binding, but still of value
- 2) Pseudonymous bindings: Examples
  - Learner credentials : not so high value BUT, still bound to legal identity

### **TR Dependence on signatures**

- TRs: dependent on signatures (example: signature Key “DID:ex:123”)
- DID (decentralised identifiers) >>> keys because...
  - 1) Any VC at point of verification (ex: employer verifying diploma): need to know that was signed by opaque key (gives auth and provenance)
  - 2) Entity that controls key claims authorship
  - 3) We know that claim wasn't tampered with (tamper resistant)
  - 4) VC Signed by key number did:ex:123 —> how to link that did to name of community college (but can't easily link to name of CC because it's forgeable)

Therefore, trust registries are a directory where verifier takes opaque string and says that key is controlled by CC (community college)

Trust Registry (TR): = directory = map of opaque key identifiers to known entities

TR needs to be trusted

Q. How to come up with list/mapping: (needed by verifier AND employer AND HOLDER (in order to identity the requester))

How does a holder validate which requests from employers are legit?

Need access to directory to ensure they can /should pass along a credential

### **TR Challenges:**

- 1) *Discovery*: how can verifier know that a registry exists? Sometimes it's taken care of, sometimes not (Attn web?)
  - mandated by vertical or...
- 2) *Scalability*: (running the TR)
- 3) *Governance*: Picking a data model/protocol: which spec to use: should allow us to look up opaque identifiers (any spec will need to do: Hosting, scaling, governance)
  - What does the key have to do to get on the list?
  - HOW? Reuse existing governance structures: examples: eduroam: a TR that maps signing keys to known entities; GAN. Any that already use KYC, etc.

4) *Longevity* (organisational and developmental (via rotating keys, (rotating DIDs less likely))

- What happens when the key is rotated out? And verification is requested? Registry is pulled up and keys aren't there, so history would need to be recorded in order to keep track of key rotation

- Who does this?

1) did method itself - some keep history of rotations

2) Trust registries (hopefully) - some have provisions for a rotation history

5) *Funding*: how to fund these registries?

### Comments

1) Org validation certifications only provided value to registrar

2) Domain validation: easy

3) TR's don't work on the web, but they can still work

4) Legal and cultural constraints

5) Cost is tied to legal liability

- \$ = more money for KYC = less legal liability

6) How to do TR: legal mandates

7) Can use TRs for code signing: for software packaging, bill or \_\_\_\_, OS's currently sign their own apps with their own TR's

### Questions

1) Longevity/lifespan of credentials AND registries - issuer of diploma no longer exists - still need to have diploma verified - so what happens? Where does key live?

- Provisions are needed to ensure that even if issuer goes away, needs to be held by some directory or trusted authority (needed BEFORE creating a TR)

2) How to re-issue when issuer is no longer around?

3) Incentive\$ in institutions to keep system?

4) What about automated (native) refresh: should this be VC spec or Did method responsibility

- Ex: TRUage - creds for age verification - can be auto-refresh by wallet

5) How to show TR's in UI?

6) Which specifications should be used for Trust registries?

### Considerations:

1) UI patterns

2) How authority can check via TR (a TR of TRs could be possible BUT begs the topic of decentralisation vs centralization)

- Regardless, machine readable ways needed

3) Developer considerations: If registries divide, devs will need to load both libraries

4) Endorsements from one agency to another for co-recognition (less hierarchy, more graph traversal)

### Advanced Topics

1) History/Longevity

- 2) Discoverability (medium term problem)
- 3) Fine-grain authz (filter by type by both verifier and holder))
- 4) Top-down(traditional) vs bottom up registries(ex: ORCID) (will need a mix of both)
  - has to do with whether or not you do KYC before or after you get on list
  - (Dmitri recommends getting trust AFTER (ie, accumulate legitimacy over time with verified attestations))
    - get on list, but shows up unverified until verified/identified after KYC by registry
    - OpenID AND (trusted credential trust) DIF spec allows both Top-down and bottom up
- 5) Progressive Trust Registries: <https://docs.google.com/document/d/1Rl1GsTF843aSs1kE2-BO5rIDy2yliDYeOokdmZ17r5w/edit?tab=t.0>

**Miscellaneous Notes:**

- Awesome trust registries : <https://github.com/andorsk/awesome-trust-registries>
- Contact books (phone)
  - Trust registry as address book
  - Contacts in address book have did:key field

## It's 2025, how do I set up a Digital Notary? (for a known authority)

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:

- Notary either signs a list or, preferred, signs each VC
  - They need a PKI wallet of some sort
- MD signs the Hash (content, MD name, MD identifier, Notary identifier (DID web), date, VC)
- All parties keep a copy
- Federation is separate to prove a license attribute
- Verifier is open standard and well known
- If each VC is signed by MMS, then they have less liability
- Likeness detection may be used for remote enrollment

**M 14** It's 2025, How do I set up a DIGITAL NOTARY as a trusted entity

**Diagram:** A circle containing the text: name, MMS, date, HASH, date. Below the circle, it says "Signed by MMS".

- MMS as issuer signs the list
  - public key for list
  - private key in wallet
- MD signs the HASH
- All parties keep copies
- Federation is separate to prove license attribute.
- Verifier is open standard and well known.
- VC signed by MMS instead of a public list less liability.
- Likeness Detection used for remote enrollment

**Additional notes:**

- Docusign.
- VCs
- Business case / model
- ? - Remote
- 3 - Federation scope
  - Level of Assurance
- Liveness Detection.
- Doc Format PDF

**Other notes:**

- MMS publishes a list of Members. + Public Key
- if 2 parties each keep signed copy
- Verifier.

# SESSION #15

## OID4VC Credential versions (updates) and DQCL Purpose

Session Convener: Oliver and Daniel  
Session Notes Taker(s):

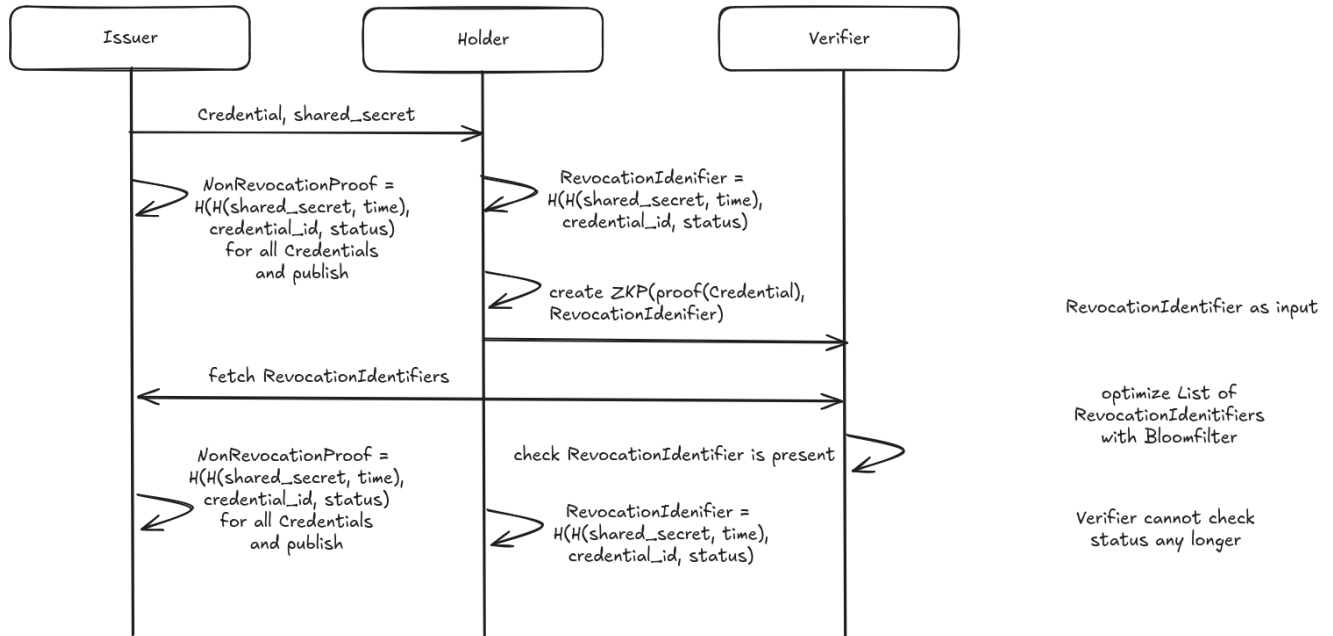
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

NO NOTES SUBMITTED

## Revocation/Status mechanisms for ZKP

Session Convener: Paul Bastian & Christian Bormann  
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:

- We discussed the requirements for good revocation methods and shared a proposal
- unfortunately the proposal does not have Issuer-RP-unlinkability



## Trust DID Web (did:tdw) – Status and Demo

**Session Convener:** Stephen Curran, Patrick St. Louis

**Session Notes Taker(s):** Stephen Curran

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

This session was an overview on Trusted DID Web (did:tdw) DID Method— an introduction, an update on its status and a demo of the implementation work that has been done so far. The `did:tdw` DID Method, being incubated at the [Decentralized Identity Foundation](https://decentralizedidentity.org/) is nearing 1.0 status and we look forward to having that version of the specification done before the end of 2024. A recent update (version 0.4) has addressed what we think are the breaking issues in the spec, and as a result, we expect the rest of the year to be spent doing clarification updates to the spec.

- For information on did:tdw, start with the information site: <https://didtdw.org>
- There are 3 open source deployments of did:tdw (linked on the information site above) in [Python](#), [TypeScript](#) and Go, and two Rust implementations that will hopefully be open sourced Real Soon Now.
- The spec itself is available in the information site and here: <https://identity.foundation/trustdidweb/>
- The slides from the session are available here: <https://bit.ly/tdw-iiw39>
- The demo was of the DID TDW Server, a web server for publishing did:web and did:tdw DIDs. The code for the demo is here: <https://identity.foundation/trustdidweb-server-py>
- A PR to add did:tdw to the DID Method Registry is here: <https://github.com/w3c/did-extensions/pull/581>
- There is a [Universal Resolver](#) plugin for did:tdw, and you can resolve some example DIDs there.

As per the presentation, the roadmap for did:tdw is:

- Finalize the specification this year — 2024!
  - Clarifications (ideally, without breaking changes).
  - Drive to standard-ize the DID Method specification.
- Implementations (in addition to what we already have...)
- Standalone resolver library
- Proxy cache for long-lived resolution — independent of the DID Controller’s life span
- ACA-Py DID Controller, Credo-TS for at least resolution, likely DID Controller as well
- Reference witness
- Continues work on the did:tdw Server
  - Separation from the DID Controller — create, rotate, use — and publication of the DID

Question that was left a bit hanging — here is a more complete answer.

- What happens if an intruder on the web server updates the log to remove some of the log entries?
  - It causes an annoyance — the keys from the removed versions of the DID are removed.
  - Can be detected and the DID updated. Not a typical use case for a Web Server, but if a deployment wants to specifically stop that, it is straightforward. When an unexpected update to the DID occurs, the DID can be updated.
  - Assuming there is a separation of the management of the private keys for controlling the DID and the web server, it is unlikely that the attacker accessing the web server has control of the private keys for the DID, and so taking over of the DID is extremely unlikely. However, if that is a concern, then the use of witnesses can alleviate that. Witnesses extend out the number of service compromises required to “take over” the DID.
  - The specification gives tools and capabilities for those deploying did:tdw to take advantage of those features (pre-rotation, witnesses, separation of key management and DID publication, etc.). The spec. is deliberately not prescriptive on how a deployment uses those capabilities.

### ***COLAPSE (& ID?) a conversation***

**Session Convener:** Kaliya Young

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

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

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

We talked about what collapse means.  
There was not necessarily any agreement.

Kaliya shared that she had been in a seminar recently with Jem Bendell.  
He is the author of [Deep Adaptation](#) and [Breaking Together](#).

## ***Social Web \_ Indie auth + FedCM PART 2***

**Session Convener:** Sam and Aaron

**Session Notes Taker(s):**

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

NO NOTES SUBMITTED

## ***Use Cases & Business Models***

**Session Convener:** Timothy Ruff

**Session Notes Taker(s):** [Ankur Banerjee](#)

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

- [The Cold Start Problem](#) by Brian Chen
- [Running Lean: Iterate from Plan A to a Plan that Works](#) by Ash Maurya
- [The Mom Test](#) by Rob Fitzpatrick

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

- Despite STIR/SHAKEN, spam calls continue. Needs business model.
- Healthcare company in the portfolio
  - If things were nicer once everybody has access
  - Adrian said in practice, a lot of projects have failed.
  - Avoided the 1:many problem of patients and doctors: instead attacked the IT department of the hospital
  - Wall of shame in healthcare where any breaches with more than 500 records breached has to be reported.
- Don't go after banking, healthcare, telecoms. These are regulated. Pick something small and non-regulated. Pick something small that's easy as a bowling "head pin" and knock it down, than do something else.
- Multi-party trial
  - If you can, get at least 1 of each party, that's great
  - Business models have to be created before any multi-party trial
- Value proposition is external facing
  - IT dept to IT dept, cybersecurity spend it high
  - Reduce the attack surface
  - HealthKERI's pitch is that signing each record reduces that attack surface

- Business case is internal facing
- Network effect that blocks you in the beginning keeps you in at the end
- “Queen Bee” principle: nobody cares about lost drones
  - Moving data using VCs from one part of the company to another as issuer and verifier
  - Still multi-party
  - Would it be the best solution?
- Mobile device management (MDM) device postures as VCs
  - Within a company, easy
- “You don’t make the product to make money”
  - Solve the business problem
  - You can always be comfortable with tinkering away with product
- KERI wanted to dive into key management since it was the hardest problem
- The tech needs to support the business model, you can’t do the tech and then figure out a business model
  - Sell the idea, then build it. This is the lean way to run it.
  - Figma and other things to prototype

### ***Looking for the Use Cases for Issuer-Hiding VC***

**Session Convener:** Shigeo Mizuno & Ken W.

**Session Notes Taker(s):**

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

Type Here

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

NO NOTES SUBMITTED

## ***Security and Privacy Standards for Biometrics. Trends, challenges and opportunities for digital ID & SSI***

**Session Convener:** Julien Bringer

**Session Notes Taker(s):**

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

Link to the slides [Security and Privacy Biometrics Standards 20241031 JulienBringer - IIW.pdf](#)

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

See the slides for detailed updates and information.

Progress made since last decade

- improved security evaluation standards for biometrics, with refined profiles and evaluation guidelines available. More traction. Helps increasing security of systems but still to be improved, latest revisions will support going further. Trust comes from security evaluation.
- security and privacy mechanisms have matured to significantly increase trustworthiness of general public systems. Pending that providers and integrators follow the recent standards. Drivers are regulation and business value (incentives for low level of assurance applications are low...). Still the requirements and recommended new approaches (in particular, avoiding a static and rigid system in order to better cope with evolving threats landscape, and to enforce strong isolation) will guide developers to improve the robustness and reliability.

Some applications are still not well covered (cf. slides) - next steps would be to develop standards to cover those applications.

## ***Breaking free from Issuers. You can be the “Issuer” of your data-path to TRUE SSI. ZKTLS***

**Session Convener:** Subhash

**Session Notes Taker(s):**

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

NO NOTES SUBMITTED

## ***Travel + SSI Mesh Not Supply CHN***

**Session Convener:** Neil Thomson  
**Session Notes Taker(s):**

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

NO NOTES SUBMITTED

## ***Credential Schemas for Age Verification and Estimation - Working Session***

**Session Convener:** Otto Mora  
**Session Notes Taker(s):** Otto Mora

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

[2024-10 Proof of Age - IIW](#)

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

We discussed the recent effort at the Decentralized Identity Foundation (DIF) to standardize credential schemas for certain key use cases including KYC, AML, proof of personhood, and proof of age.

The discussion centered around the development of a general purpose age schema which would allow for both “age estimation” (several assurance methods to be used) as well as “age verification”. Otto presented an early draft of the data fields being considered for the schema spec. The group provided feedback regarding the fields and also suggested additional ones to be considered.

Existing solutions for age verification in the industry were discussed, including <https://www.mytruage.org> as well as the support of age verification included in the credit card payment networks (EMV).

Please contact Otto Mora (omora@privado.id) if you would like to participate in the schema definition effort, we will schedule a specific meeting to receive input from SMEs regarding the proposed schema (deadline 3-Dec-2024).

## Concept Mapping Techniques

**Session Convener:** Andrew Hughes  
**Session Notes Taker(s):** Andrew Hughes

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

Concept mapping, identification and authentication process

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

Described the technique of concept mapping and its use to make tacit group knowledge explicit. Talked about how others use concept maps in their work. And the usefulness of of visual representation of textual documents. The group was interested in the value of concept mapping and how it was used in a real situation with a standards committee to arrive at group consensus.

**Material from a report by Andrew Hughes:**

### 1 Concept mapping technique

#### 1.1 What are concept maps, how do they work and how are they helpful?

The concept map technique<sup>[1]</sup> is useful when a group tries to work towards a shared understanding of concepts and terminology of complex topics. Concept maps are also useful when introducing a domain of knowledge to a group.

Concept maps emerged in 1972 as part of research into how an individual's knowledge of a subject area changes over time.

From a paper describing the underlying theory of concept maps<sup>[2]</sup>:

Concept maps are graphical tools for organizing and representing knowledge. They include concepts, usually enclosed in circles or boxes of some type, and relationships between concepts indicated by a connecting line linking two concepts. Words on the line, referred to as linking words or linking phrases, specify the relationship between the two concepts. We define *concept* as *a perceived regularity in events or objects, or records of events or objects, designated by a label*. The label for most concepts is a word, although sometimes we use symbols such as + or %, and sometimes more than one word is used. *Propositions* are *statements about some object or event in the universe, either naturally occurring or constructed. Propositions contain two or more concepts connected using linking words or phrases to form a meaningful statement*. Sometimes these are called semantic units, or units of meaning.

There are no restrictions about level of granularity or depth - the concept map grows in reaction to the group discussion. When creating concept maps, place holders are left for future elaboration.

Also, the group goes back to earlier concepts frequently to adjust and re-confirm that they clearly express the intended meaning.

While a concept map has similar notation as information graphs, taxonomies and ontologies, the concept map is intended to be less formal and less structured to empower the group to explore the concepts without having to worry about perfect expression up front. Note that the notation also resembles entity relationship diagrams, mind maps, and process diagrams - but those diagrams are entirely different from concept maps.

Concept maps are a good tool for discussion and exploration of the language used in a domain. However, they lack the formality of other approaches such as knowledge graphs, taxonomies or formal ontologies which would be better suited as tools for longer term knowledge management.

---

<sup>[1]</sup> <https://cmap.ihmc.us/docs/learn.php> contains resources for learning about concept maps and papers explaining theories and practices.

<sup>[2]</sup> “Novak, J. D. & A. J. Cañas, The Theory Underlying Concept Maps and How to Construct and Use Them, Technical Report IHMC CmapTools 2006-01 Rev 01-2008, Florida Institute for Human and Machine Cognition, 2008, available at:  
<http://cmap.ihmc.us/docs/pdf/TheoryUnderlyingConceptMaps.pdf>



# #IIWRunners Club Run



**Lance Byrd** (He/Him) • 2nd

Identity Developer and Co-Founder - Secure Organizational Identity, vLEI, KER...  
2w • Edited • 🌐



**Internet Identity Workshop** run Wed morning @ 6:30am @ Stevens Creek trail central avenue entrance <https://lnkd.in/e53scxh7>

Spread the word **Rodolfo Miranda James Monaghan Stephen Curran Zaïda Rivai Alexandru Andrei Ariel Gentile Fabrice Rochette Kent Bull Nicholas Racz**



You and 16 others

6 comments

## Reactions



**Lance Byrd** **Author**

2w ...

Identity Developer and Co-Founder - Secure Organizational Identity, vLEI, KE...

**Rodolfo Miranda Brendan Miller Stephen Curran Fabrice Rochette Nicholas Racz Matt MacAdam**



Like · 🌐❤️ 9 | Reply · 1 Reply

# Thanks to our Demo Hour Sponsor OpenID



The **IIW Speed Demo format** involves each person Demoing giving a **5-minute demonstration** of their service, product, physical device, **10 times** to 10 different small groups, rotating through to view them over the course of the hour. **Demo Hour takes place on Wednesday after lunch from 1:30 - 2:30.**

There will be 20 Demo Tables in the Grand Hall each with a # Sign on it that corresponds to the Demo taking place at that table. People rotate through the tables/Demo's in a self-organized way ~ that's a little loud, seemingly chaotic and free flowing, but works!

See the list of Demos via the Demo List below and decide ahead of time the Demo's you'd like to see. You'll be able to see 10 of the 20 Demo's over the hour.

TABLE	Demo Description	More Info
#1	<b>Center Identity Ai enhanced and Visual memory security questions:</b> Matthew Vogel URL: <a href="https://centeridentity.com">https://centeridentity.com</a> Center Identity's demo features AI-enhanced and visual memory security questions, creating a strong, passwordless authentication method that's secure and device-free.	<a href="#">More Info Here</a>
#2	<b>Cerbos:</b> Alex Olivier URL: <a href="https://cerbos.dev">https://cerbos.dev</a> Cerbos is an open source externalized authorization project enabling the complicated logic of roles and permissions to be defined as testable, versionable and auditable policy.	<a href="#">More Info Here</a>
#3	<b>Funke EUDI Wallet Prototypes (SPRIN-D):</b> Yasuda Kristina, Mirko Mollik and Funke Teams URL: <a href="https://www.sprind.org/en/magazine/eudi-wallet-prototypes/">https://www.sprind.org/en/magazine/eudi-wallet-prototypes/</a> 11 teams have been selected to participate in SPRIN-D's Funke (Innovation Competition) to innovate towards most secure, privacy preserving, user-friendly and interoperable EUDI Wallet. We will demo the wallets and talk about our learnings!	<a href="#">More Info Here</a>
#4	<b>OpenID Foundation conformance tests for OpenID for verifiable credentials:</b> Joseph Heenan URL: <a href="https://openid.net/how-to-certify-your-implementation/">https://openid.net/how-to-certify-your-implementation/</a> OIDF has tests that wallets (soon issuers/verifiers) 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 the tests yourself.	<a href="#">More Info Here</a>

#5	<p><b>the Digital Identity Toolkit:</b> Marianne Díaz Hernández  URL: <a href="https://www.accessnow.org/guide/digital-id-toolkit/">https://www.accessnow.org/guide/digital-id-toolkit/</a>  This toolkit aims to help digital rights activists working on digital identification systems to navigate the complexities of the topic in an easier way, as well as to provide them with language that might help get them started in campaigning, advocating, educating, and mobilizing around digital ID systems.</p>	<a href="#">More Info Here</a>
#6	<p><b>Simeon:</b> Audrey Jacquemart and Julien Bringer  URL: <a href="https://simeonid.com">https://simeonid.com</a> Simeon is redefining credential management by offering a seamless, inclusive solution that combines passwords and verifiable credentials in one powerful app. Designed for everyone, regardless of technical expertise, Simeon ensures that convenience and security finally meet.</p>	<a href="#">More Info Here</a>
#7	<p><b>tinySSB (Secure Scuttlebutt) and CRDTs / University of Basel, Switzerland:</b> Christian Tschudin  URL: <a href="https://github.com/ssbc/tinySSB">https://github.com/ssbc/tinySSB</a>  tinySSB is a post-Internet protocol stack for decentral applications that makes systematic use of convergent data structures (CRDTs) and self-sovereign identities. We will demo a fully serverless Kanban board application that runs on Android phones over Bluetooth Low Energy</p>	<a href="#">More Info Here</a>
#8	<p><b>Aserto - Topaz:</b> Omri Gazitt  URL: <a href="https://www.topaz.sh">https://www.topaz.sh</a> , <a href="https://github.com/aserto-dev/topaz">https://github.com/aserto-dev/topaz</a>  Topaz is an OSS authorizer that combines the best of policy-as-code / OPA with the relationship-based access control model described in Google's Zanzibar paper. It ideal for building fine-grained, policy-based, real-time access control for SaaS or internal applications</p>	<a href="#">More Info Here</a>
#9	<p><b>Kwaai demoing Personal AI:</b> Reza Rassool  URL: <a href="https://www.kwaai.ai/">https://www.kwaai.ai/</a>  If AI is to be truly uplifting for humanity, then let's start with AI for humans first. Kwaai has developed the first open-source Personal AI platform. Now you can own and operate your own AI that won't spy and eavesdrop on you. Join the movement democratizing AI.</p>	<a href="#">More Info Here</a>
#10	<p><b>Numeracle/ Need for Secure Verified Identity Presentation (sVIP) in Communications:</b> Sam Etler, Rebekah Johnson, Pierce Gorman  URL: <a href="https://www.numeracle.com/download-numeracle-resources/consumer-research-report">https://www.numeracle.com/download-numeracle-resources/consumer-research-report</a>  New research suggests two thirds of consumers want more trustworthy caller ID information. Join us for a live demo of the only industry-led, standards-based Rich Call Data (RCD) ecosystem engineered to be secure-by-design to deliver trusted identity display to mobile devices.</p>	<a href="#">More Info Here</a>
#11	<p><b>Identity in the Fediverse:</b> Johannes Ernst, Dazzle Labs Inc.  URL: <a href="https://dazzlelabs.net/">https://dazzlelabs.net/</a>  Decentralized social media is making a comeback with products such as Mastodon, Ghost or Threads. Identity is at their heart, but it's not wallets. A demo of how it does look and work, and open issues.</p>	<a href="#">More Info Here</a>
#12	<p><b>Procivis AG will be demoing "Procivis ONE":</b> Eugeniu Rusu“ will Demo our solution  URL: <a href="https://docs.procivis.ch/">https://docs.procivis.ch/</a>  @Eugeniu Rusu will share a description in the coming days.</p>	<a href="#">More Info Here</a>
#13	<p><b>FedID Connect by JLINC Labs:</b> Ben Curtis  URL: <a href="https://fedid.me">https://fedid.me</a>  Description: FedID Connect (FIDC) leverages the portability of OIDC and distribution of ActivityPub to make verifiable credentials accessible to everyone, providing usernames and identifiers that individuals own and control, no matter what happens to the site they signed up on.</p>	<a href="#">More Info Here</a>

#14	<p>Case Western Reserve University/Learning &amp; Employment Record System: Yuqiao (Tina) Xu  URLs: <a href="#">Open Skill Genome Substack</a> &amp; <a href="#">Designing Responsible Universal Learning and Employment Record Ecosystem</a>  Learning and Employment Record System, utilizing AI to generate and verify user academic skill credentials.</p>	<a href="#">More Info Here</a>
#15	<p>Godiddy.com: Markus Sabadello  URL: <a href="https://godiddy.com/">https://godiddy.com/</a>  See some of the latest developments in the DID universe... New DID methods did:tdw, did:dht, linking DIDs to other identifiers, DID Linked Resources, stats and analytics, etc.</p>	<a href="#">More Info Here</a>
#16	<p>Privado ID - ZK Powered Identity Tools: Otto Mora and Tom Stern  URL: <a href="https://www.privado.id">https://www.privado.id</a>  Privado ID is a set of tools which enables to securely and privately exchange credential info using zero knowledge proofs. The demo will showcase the web wallet with embedded issuance, synchronization with our mobile app, and support for multiple L2 Ethereum networks.</p>	<a href="#">More Info Here</a>
#17	<p>Tratteria open source project (company: SGNL) : Atul Tulshibagwale  URL: <a href="https://tratteria.io">https://tratteria.io</a>  Tratteria implements a new IETF OAuth WG draft called "<a href="#">Transaction Tokens</a>" (TraTs). TraTs are short-lived signed JWTs that provide immutable identity and context information in microservices call chains. By providing such immutable context, TraTs prevent attacks like software supply chain, privileged user compromise or malicious insiders, because microservices automatically deny calls that do not have such TraTs associated with them, or the parameters of the call do not match an associated, valid TraT.</p>	<a href="#">More Info Here</a>
#18	<p>HIE of One: Adrian Gropper, MD  URL: <a href="https://github.com/abeuscher/vue-ai-example">https://github.com/abeuscher/vue-ai-example</a>  Medical AI assistants for both patients and clinicians are inevitable as part of medical consultations. The user's agent uses the new GNAP delegated authorization standard, RFC 9635, to connect a patient's entire health record and manage a simple voice chat with a large language model.</p>	<a href="#">More Info Here</a>
#19	<p>UR Codes by FaceTec: Andrew Hughes  URL: <a href="https://urcodes.com">https://urcodes.com</a>  An issuer-signed string in QR code format that contains name-value pairs (like a license number) and a 72 byte facial biometric template. A UR Code makes non-biometric documents into biometric-bound documents. Andrew will make your UR Code!</p>	<a href="#">More Info Here</a>
#20		<a href="#">More Info Here</a>



**Numeracle**  
3,236 followers  
2w • 🌐

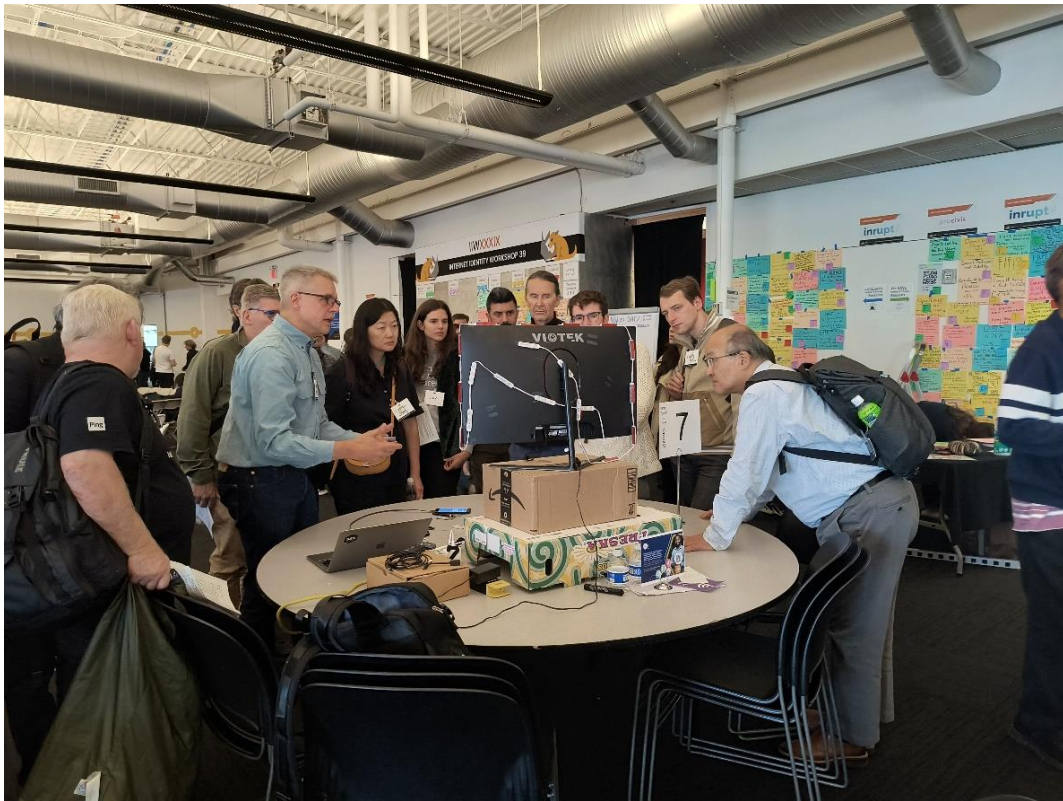


It's day 2 at [Internet Identity Workshop](#), and what's better than a demo of a live call delivered to a consumer handset displaying brand [#identity](#), signed, sealed, and securely delivered with logo display. [#IIW](#)



 You and 19 others

1 comment · 4 reposts



# Diversity and Inclusion Scholarships



## Thank You to Our Diversity & Inclusion Scholarship Sponsors SpruceID and tbd

Through these sponsorships we gave reduced price & complimentary tickets and/or travel and lodging reimbursement to new attendees to IIW who otherwise would not have been able to attend and participate.

*We care about increasing support for women, black, and other starkly underrepresented technologists in our ecosystem. We can't build identity for everyone when demographics are homogeneous.*



## Thank You to our Women's Breakfast Sponsor Curity



MEET OUR SPONSOR



IIWXXXIX

THANK YOU FOR WOMENS BREAKFAST!



## Event Photos taken by Doc Searls

Doc Searls has several hundred candid photos from IIW #39 on his Flickr account



2024\_10\_29-31 IIW XXXIX (39)  
flickr.com

[587 Photos from all 3 Days](#)



2024\_10\_31 Day 3 of IIW XXXIX  
(39)  
flickr.com

[Day 3](#) includes Open Gifting



2024\_10\_30 Day 2 of IIW XXXIX  
(39)  
flickr.com

[Day 2](#) includes Demo Hour



2024\_10\_29 Day One of IIW XXXIX (39)  
flickr.com

[Day 1](#)



**Numeracle**  
3,236 followers  
2w • 🌐



Yesterday was jam-packed at the [Internet Identity Workshop](#), with so many great sessions, including one on business [#identity](#) led by Numeracle's Founder and CEO, [Rebekah Johnson](#). We look forward to the third and final day at [#IIW](#).



## Stay Connected with the Community Over Time - Blog Posts from Community Members

### New Community Resource

Each week Kaliya, Identity Woman and Informiner publish a round of the week's news from the industry. It is called **Identosphere - Sovereign Identity Updates (weekly newsletter)**

You can find it here: <https://newsletter.identosphere.net/>

As a follow up to the session 'Let's Bring Blogging Back' an IIW Blog aggregator has been created here: <https://identosphere.net>

If you want your blog to be included please email Kaliya: [kaliya@identitywoman.net](mailto:kaliya@identitywoman.net)

A BlogPod was created at IIW - Link to IIW Slack -

<https://iiw.slack.com/archives/C013KKU7ZA4>

If you have trouble getting in, email [Kaliya@identitywoman.net](mailto:Kaliya@identitywoman.net) with BlogPod in the Subject.

Planet Identity Revived ~ @identitywoman & @InfoMiner cleared out & updated Planet Identity (see links below) you can support the work here:

<https://www.patreon.com/user?u=35769676>

IIW Community Personal Blog's shared via: <https://identosphere.net/blogcatcher/>

IIW Community dot.org's in the IIW Space: <https://identosphere.net/blogcatcher/orgsfeed/>

## Upcoming IIW Inspired™ Regionally Focused OpenSpace unConference Events

[Did:unConf Africa](#) | With Our Partner [DIDx](#)  
*Bridging the Digital Identity Gap in the SADC Region*

February 18 - 20, 2025 Cape Town, South Africa | [REGISTER HERE](#)

We'll start with an African-Focused Digital Identity Program on the afternoon of 18 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.

[Digital Identity unConference Europe](#) | With Our Partners [TrustSquare](#) & [DIDAS](#)  
*Fostering Collaboration on the digital identity between governments, citizens, and companies across Europe*

March 4 & 5, 2025 / **DICE Ecosystems** / Zurich | [REGISTER HERE](#)

Building Capacity & Capability for Ecosystem Adoption of Verifiable Credentials and Authentic Data

A two-day event with a focus on decentralized identity and verifiable data adoption and mutual learning to get to successful ecosystems faster. DICE Ecosystems is specifically for sector-specific, cross-sector and cross-border business ecosystems building out production use cases to support production applications.

Sept. 2 - 4, 2025 / **DICE2025** / Zurich | [EarlyBird Registration HERE](#)

Annual gathering for the companies and individuals working on developing and deploying digital identity systems in Europe.

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 community of Digital Identity Leaders across Europe.

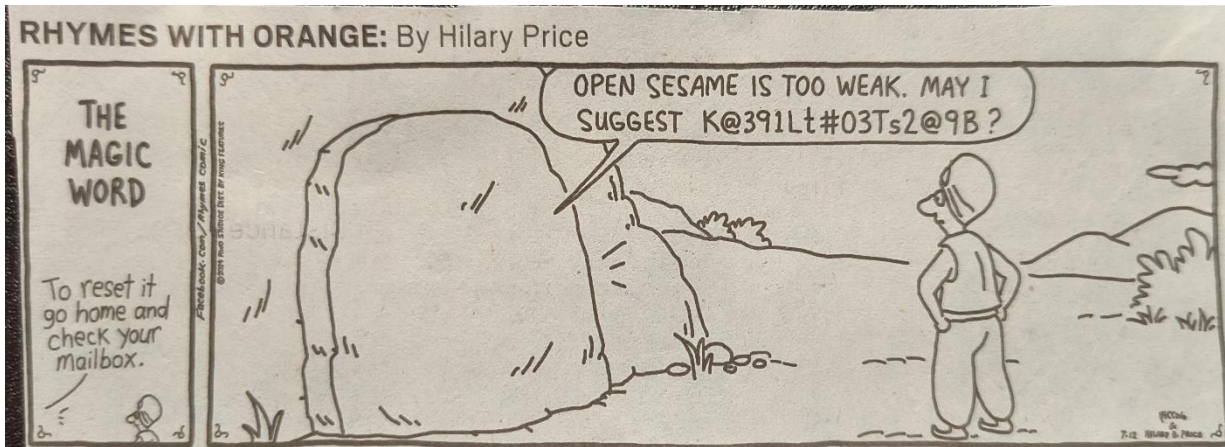
### [APAC Digital Identity unConference](#)

*Fostering innovation and collaboration between emerging digital identity companies and projects across the APAC region / Next Event Date/Location TBD*



## Identity 'Funnies' (comic strips) Shared by Alan Carp!

### Password Magic



### Phishing Badge



Hope to See you April 8,9 & 10, 2025 for IIWXL

## The 40<sup>th</sup> Internet Identity Workshop

REGISTRATION OPEN in December

[www.InternetIdentityWorkshop.com](http://www.InternetIdentityWorkshop.com)

