

IIWXXXVII



INTERNET IDENTITY WORKSHOP 37

October 10-12, 2023

Book of Proceedings

Computer History Museum / Mountain View CA
Opening Circle



Collected Processed & 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

IIWXXXVII In Person in Mountain View, CA
October 10, 11 and 12, 2023

www.internetidentityworkshop.com

Thank You! Documentation Center & Book of Proceedings

Sponsors: AyanWorks & Curity & DIF



Contents

| | |
|--|----|
| Thank You! Documentation Center & Book of Proceedings Sponsors: AyanWorks & Curity & DIF | 1 |
| About IIW | 7 |
| Thank You to our Sponsors! | 8 |
| IIWXXXVII Daily Schedule | 9 |
| Opening Small Group Discussion / Identity Groups You Are Part Of | 11 |
| IIW36 Agenda Creation = Schedule & Workshop Sessions | 12 |
| Tuesday October 10, 2023 Day 1 / Sessions 1 - 5 | 12 |
| Wednesday October 11, 2023 Day 2 / Sessions 6 - 10 | 14 |
| Thursday October 12, 2023 Day 3 / Sessions 11 - 15 | 16 |
| Notes Day 1 / Tuesday April 18 / Sessions 1 - 5 | 19 |
| SESSION #1 | 19 |
| OpenID for Verifiable Credentials - The next generation of OpenID | 19 |
| IIW 101 Session - OAuth 101 | 23 |
| Cedar Policy Language 101 | 24 |
| If DID is So Good, why don't I have one yet? | 26 |
| What is the Future WE want to create? | 28 |
| Ethical AI - assisted note taking | 28 |
| The Chicago Economics School Catalyzed the Corps that ARE the Identity Crisis | 28 |
| Credentials & Risk? Why Shared Data? (Linked Claims) | 29 |
| ARC Regenerative Communities | 34 |
| vLEI Developments and Updates | 36 |
| Overview of ISO 18013-5 Mobile Driving License standard | 37 |
| SESSION #2 | 39 |
| Identity Credential | 39 |
| Introduction to OpenID Connect | 40 |
| Artificial Intelligence and Copyright | 40 |
| Identity Proofing in Federated Systems | 42 |
| “Selling to Enterprises” [sales] | 43 |
| Credentials Community Group “CCG” Hybrid Weekly Meeting | 44 |
| Intro to KERI | 45 |
| A Personal Digital Agent Standard | 46 |
| Best Practices for Recovering from Private Key Compromise? | 47 |
| DIDComm 101 | 48 |

| | |
|---|------------|
| Answers to “The Four Horsemen of SSI (Jeremy Grant Presso) | 49 |
| A Business Person’s Guide to Understanding IIW or The Burning Man of Digital Identity | 50 |
| SESSION #3 | 51 |
| Open Wallet Update + Call for Projects..... | 51 |
| IIW 101 - User-Managed Access (UMA) - Get to know this unique “application of OAuth” ... | 51 |
| The Android & Web Identity API - Proposals | 52 |
| OAuth for First-Party Apps | 53 |
| didwebs for muggles | 54 |
| Verifiable Presentation with Message | 55 |
| Grounding Identity in Truth..... | 57 |
| DIF Credential Trust Establishment - Practical Governance / Sam Curren | 57 |
| BCGov Offers \$CDN100k: Adding Support for W3C Format VCs to AnonCreds v1.0 | 58 |
| SESSION #4 | 60 |
| Introduction to Trust Over IP Foundation (ToIP)..... | 60 |
| IIW 101 - Web AuthN | 61 |
| Credential vs Wallet Selection | 62 |
| UX Challenge for SSI | 63 |
| source: https://ericscouten.dev/2023/iiw/#session-4e-how-are-you-solving-for-the-ux-challenges-of-ssi | 64 |
| SOLID | 65 |
| Privacy as Alignment of Expectations | 66 |
| Can We Solve a Problem in an Hour? Speed Proof of Concept | 69 |
| Confidential Computing Changes Everything - Enabling a Universal Name System (UNS) and Universal Certificate Authority..... | 71 |
| did:PLC: 1,000,000 uses app..... | 73 |
| KERI for Dummies | 73 |
| Externalized Authorization..... | 75 |
| Brainstorm: How SSI can solve the Data Exchange Problems for Healthcare ? (KERI / vLEI / SCDC)..... | 76 |
| Memory-Based Private Keys! Enforcing Entropy Using AI!!! OMG!..... | 79 |
| SESSION #5 | 80 |
| ToIP Trust Spanning Protocol for Muggles | 80 |
| IIW 101 Session - Self Sovereign Identity (SSI) | 84 |
| Federated Auth Network | 86 |
| FEED ME! Unified FEED - What do we need in a Unified Feed of all Asynch communication. | 88 |
| AuthZ Conference | 90 |
| Improving the W3C CCG DID Method Registry | 90 |
| JSON-LD BBS+ Verifiable Credentials with Private Holder Binding, Pseudonym, and more .. | 92 |
| WIMSE - Workload Identity in Multi-System Environments | 94 |
| Building Test Suites | 94 |
| HACKATHONS! did:hack / DIF Learn more, get involved, get hacking! | 95 |
| Secure Issuance for Government Credentials | 96 |
| Identity + Peer Production | 99 |
| Notes Day 2 / Wednesday April 19 / Sessions 6 - 10 | 100 |
| SESSION #6 | 100 |
| BIP32 and You (Fido Row Signatures)..... | 100 |
| GNAP 101 | 102 |
| People don’t want a digital identity | 103 |
| Philosophy: The code behind the code..... | 104 |
| GLEIF’s experience with the vLEI Ecosystem Governance Framework: Lessons Learned ... | 104 |

| | |
|--|------------|
| Human OS - Functional / Modality Challenges - Real World / Digital World..... | 109 |
| Philosophical Foundations of Identity: Pure and Applied Philosophy | 113 |
| Dead man's switch for identity accounts | 115 |
| MFA & Passkeys for people who have trouble maintaining possession of physical factors . | 117 |
| Account Recovery (v | 117 |
| SESSION #7 | 121 |
| Wallet Security and IETF Attestation-based Client Authentication | 121 |
| State of Idm Policy Interop | 122 |
| Trust Spanning Protocol (TSP) Deeper Dive | 126 |
| W3C VC-Edu Plugfests! Credential rendering! Trust Registries! Schemas! W3C VC-EDU Task Force | 128 |
| Standards-Based Digital Credentials Flavors Explained | 129 |
| VCs over Ceramic..... | 130 |
| Create Your Own did:webs..... | 131 |
| PDP & PEP vs. AS/RS Smackdown | 131 |
| The Synchronic Web | 136 |
| The Solution: Citizen-Controlled Digital Identity: An Alterantive to the Mobile Drivers License..... | 138 |
| Online Travel ssi + data privacy - DIF SIG + ToIP TF Sig Work | 139 |
| SESSION #8 | 141 |
| US Healthcare on Trial: Decentralized Identity Use Case Assessment Framework | 141 |
| IETF Status List and other Revocation methods | 143 |
| Blockchain-Free Proof of Personhood | 144 |
| Serverless, Data baseless, Programmable, Smart Wallets (PICOS) | 146 |
| Are there too many identity.orgs? Could we consider how to accomplish our goals w/less of them | 146 |
| Ozero - AuthN in Seconds - Removing Manual OIDC Config | 149 |
| Experiments with JSON-LD payloads secured by JWS vs Data Integrity | 150 |
| World Coin: It's Privacy Impacts..... | 150 |
| What Should DIF (Decentralized Identity Foundation) do for interop? | 151 |
| Augmenting OID4VC with DIDComm | 152 |
| UX for Privacy: Questions not Answers..... | 152 |
| Aries Bifold & APP Attestation | 155 |
| SESSION #9 | 156 |
| Making the Internet AGE Aware | 156 |
| OpenID4VC as Framework vs. Profiles..... | 159 |
| Abbreviated Language for Authorization..... | 160 |
| KERISSE.org, the KERI Suite Search Engine | 166 |
| Targeted Log OUT | 166 |
| Browser API Wallet Query Lang | 169 |
| Should governments be involved in VC ecosystems? | 170 |
| Secure Organizational Identity | 171 |
| Confidential DiD's - Solve Decentralized Key Management and Universal Zero-Trust..... | 171 |
| Experiments with DIDs and DHTs..... | 172 |
| OIX Roaming Between Trust Frameworks | 172 |
| Using DIDComm to protect files in cloud storage..... | 173 |
| IEEE 7012 - Personal Terms and Conditions | 173 |
| Digital Credentials Cons. - VC-API SPEC Implemented as Microservers in Docker Compose | 174 |
| SESSION #10 | 177 |
| International Interoperability Summit - Paris Next Month | 177 |

| | |
|--|-----|
| Sustainable Privacy Re-Identification Attacks..... | 178 |
| Fitting credentials that are verifiable into NIST 800-63-4..... | 178 |
| Identity is a Graph Problem..... | 179 |
| IDP Discovery via Wallets..... | 180 |
| Accelerating Broad Adoption of Digital Trust Technology: British Columbia's approach ... | 181 |
| AnonCreds V2: BBS+, more ZKPs, (perhaps) PQ and CODE!! | 181 |
| Universal Wallet Backup Containers | 183 |
| The P3Pub Protocol (Web-native, lightweight Push-Pull-Publish-Subscribe) | 185 |
| Veramo – DIF Building the community-led supermodular framework for decentralized agents..... | 186 |
| Identity Governance Who? What? How? | 186 |
| Minimum Interoperability Profile for ACR (authentication context)..... | 189 |
| The many different flavors of Selective disclosure + the Future of Consent | 189 |
| DEEFAKES +AI Threats to ID Proofing + verification systems “AI is Rocket Fuel for Fraud” | 191 |
| Notes Day 3 / Thursday April 20 / Sessions 11 - 15 | 192 |
| SESSION #11 | 192 |
| Stitching Together a Web Wallet - What’s there & What’s missing..... | 192 |
| Selective Disclosure is useless | 193 |
| Compassion.IO (How to give/receive help in the virtual world, safely, securely, reliably) | 195 |
| OID4VC Interop Profiles Convergence | 197 |
| BUBBLES? Federation in disadvantaged and disconnected environments | 199 |
| VC ‘render Method’ displaying & rendering verifiable credentials / DCC..... | 200 |
| Bhutan: National ID and SSI | 200 |
| SESSION #12 | 201 |
| BRAINSTORM: Digital identity as a tool in the fight against online Child Sexual Abuse Material (CSAM)? [Privacy vs. CSAM]..... | 201 |
| The SR-71 Could Not Fly without me | 204 |
| Topaz - Demo Open source, fine-grained, policy-based, real-time authorization service.. | 205 |
| Cookie Binding as a Browser Standard | 208 |
| Philosophy of the Crowds - Moral construction in the age of Internet Identity | 209 |
| eIDAS 2 AMA..... | 210 |
| Transaction Tokens Authorization for Multi-workload environments | 212 |
| DIF = Decentralized Identity Foundation Update - What’s the DIF? How to be involved + Hackathons | 215 |
| University “Intro to Digital Identity” | 216 |
| Composable P2P Identity Components on Holochain (not a blockchain) | 216 |
| DIDATA - Decentralized Intelligent Decision and Trust Agent | 217 |
| DID Method Enumeration micro-spec | 218 |
| SESSION #13 | 219 |
| Conceptual History of Society + Identity..... | 219 |
| ACDC (Authentic Chained Data Containers) for Muggles..... | 219 |
| What does Presentation Exchange do? ...and which parts of it do we actually need? | 220 |
| 21st Century Voters Here to Save the Day..... | 220 |
| Key-Based Auth Convoy + Convergence | 221 |
| Low Code a Path to Adoption..... | 221 |
| Did.web Improvements Challenges | 222 |
| APAC Digital Identity OpenSpace unConference - Late 2024 - come discuss how to contribute to making it a success! | 224 |
| Identity Stories | 225 |
| Organizational Ecosystem with BCGov - Lessons learned on adoption and governance.... | 227 |

| | |
|--|-----|
| Session #14 | 228 |
| CLAIM-BOUND VCs - no keyinding? Matching by biometric / names..... | 228 |
| Authentic Data is the Real Sh*t, NOT digital identity | 228 |
| PLAN: Pico Labs Affiliate Network | 233 |
| Intersubjectivity: An Open Discussion | 235 |
| Authorization Exchange (AuthZEN) working group session | 237 |
| Demoscene Dark Matter: Identity of a Digital Arts Subculture | 238 |
| Human Rights impact of Digital Identity Protocols | 240 |
| Consumer Apps in Decentralized Identity..... | 242 |
| Identity through IOT deploying aca-py on balena cloud | 243 |
| did:peer;4 - A document in the DID + Demo | 243 |
| SESSION #15 | 244 |
| ToIP (and everyone's) GLOSSARY - How can we all speak the same language (learn acronyms) | 244 |
| TOKEN BUckets | 246 |
| POST-CAPITALIST Funding & Governance | 246 |
| Demo Decentralized Identity Use Case Assessment Framework US Healthcare | 247 |
| Biometric Holder Binding - The Good Bad Ugly | 249 |
| Real - IT Party Frontal Guerrilla Rebellion..... | 250 |
| KIRA - Key Infrastructure with Remote Attestation (Confidential Computing) | 251 |
| Demo Hour / Wednesday April 19..... | 252 |
| Diversity and Inclusion Scholarships | 256 |
| Event Photos taken by Doc Searls..... | 257 |
| Read Phil Windley's Internet Identity Workshop 37 Report Here | 257 |
| Remembering Vittorio Luigi Bertocci..... | 258 |
| Stay Connected with the Community Over Time - Blog Posts from Community Members | 262 |
| Hope to See you April 16 - 18, 2024 | 263 |



Heidi Nobantu Saul 🐝蝶 @nobantu · Apr 17

...

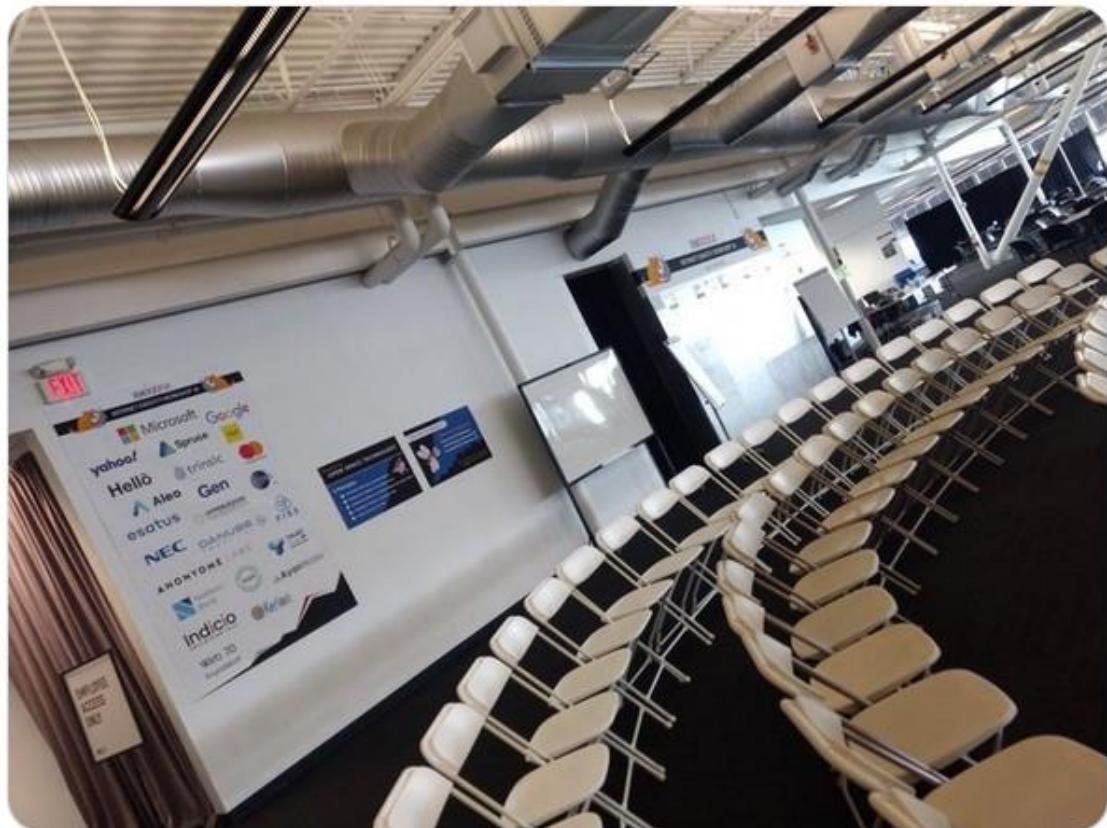
All set and ready to welcome everyone to the 36th #IIW!!

18 years and still going strong ~ can you believe it?

Must be the [#openspace](#) format, live agenda creation keeps things fresh.

Looking forward to seeing old friends and making new ones.

@idworkshop #IIW36



t 4

17

902



About IIW

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

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

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

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

The event is now in its 17th year and is Co-produced by Phil Windley, Heidi Nobantu Saul and Kaliya Young. IIWXXXVIII (#38) will be April 16 - 18, 2024.

Phil Windley ✅ @windley · Oct 23

The latest IIW was great with many high intensity discussions of identity by people from across the globe. » Internet Identity Workshop 37 Report #iiw #identity

windley.com

1 3 2 424

#IIW is powered by [#openspacetech](#) and the magic of [#selforganizing](#) and has been since 2007!

Thank You to our Sponsors!



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

Upcoming IIW Events
IIWXXXVII #38
April 16, 17 and 18, 2024
In Person in Mountainview, CA
<https://internetidentityworkshop.com/>

IIWXXXVII Daily Schedule

IIWXXXVII 3 Day Schedule

| TUESDAY, October 10 / Doors Open at 8:00 | | | |
|---|---------------|----------------|-------------|
| 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 <u>Off the Rails Brewery</u> 111 S Murphy Avenue Sunnyvale, CA 94086 (408) 773-9500 | | | |

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

THURSDAY, October 12 / Doors Open at 8:00

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 | IIWXXXVIII April 16 - 18, 2024 | |

Drinks/Dinner 5'ish No Host @ Das Bierhauz 135 Castro Mountain View

<https://dasbierhauz.com/>



Mike Ebert @mike_ebert · Apr 18

Time for the opening circle at #IIW XXVI!

...



Small Group Discussion / Identity Groups You Are Part Of

During our welcome small group discussions, we invited people to reflect on the different groups that they are a part of and track. Each person wrote those groups up on post-it notes and then we created a large community map.

After the meeting Kaliya took all the post-it notes and entered the data they contained and this is the [resulting spread sheet](#). It gives a sense of the vast range of work and expertise happening now.

There were a lot of participants in a range of standards development and industry associations related to identity.

- W3C Working Groups,
- W3C Community Groups,
- Trust over IP Working Groups and Task Forces,
- Decentralized Identity Foundation Working Groups and
- Special Interest Groups,
- OpenID Foundation,
- IEEE,
- ISO,
- IETF,
- Kantara,
- FIDO.

There are quite a few open source efforts with many sub projects Hyperledger, Open Wallet Foundation and numerous other open source projects.

Key industries with many participants from various organizations include

- Healthcare,
- Finance,
- Education,
- SupplyChain,

There are Government leaders from a range of agencies around the world, Media that people pay attention to, Community Projects and Events. Numerous .orgs, Protocols and Companies, Non Identity Things, and at the end some Unknowns.

Take a look at a summary chart of the results here:

https://docs.google.com/spreadsheets/d/1MGKro8Yg3b1N27mni_WmOOP6m2wj9i9bEre7foKt3Y/edit#gid=2039907020

IIW36 Agenda Creation = Schedule & Workshop Sessions

Bjorn @blhjelm - Oct 10
It's IIW-time. @idworkshop #IIW

IIW XXXVII
INTERNET IDENTITY WORKSHOP 37
October 10-12, 2023

Session 1 1:00 - 12:00
Session 2 12:00 - 1:00
Lunch 1:00 - 2:00
Session 3 2:00 - 3:00
Session 4 3:00 - 4:00

1 2 10 447

163 distinct sessions were called and held over 3 Days.

We received notes, slide decks, links to presentations and photos of whiteboard work for 138 of these sessions.

Tuesday October 10, 2023 Day 1 / Sessions 1 - 5

Session 1

- 1A/ WIGG Identity Credentials Inro + Scope / Tim Cappalli
- 1B/IIW 101 - Intro to OpenID Connect / Michael Jones
- 1C/ AI & Copyright (for everyone)!!!! / Wenjing Chu
- 1D/ Identity - proofing users in federated systems / Jacob Siebach
- 1E/ “Selling to Enterprises” [sales] / Kapildev Arul Mozhi
- 1F/ Credentials Community Group “CCG” Hybrid Weekly Meeting / Kimberly Wilson Linson (Live) & Harrison Tang(via Video)
- 1G Introduction to KERI (Key Event Receipt Infrastructure) / Nuttawut Kongsuwan
- 1H/ A Personal Digital Agent Standard / Adrian Gropper
- 1I/ NO SESSION
- 1J/ NO SESSION
- 1K/ Best Practices for Recovery from Private Key Compromise? / Johannes Ernst
- 1L/ DID Comm 101 and Q&A / Sam Curren
- 1M/ Answers to “The Four Horsemen of SSI” (Jeremy Grant Presso) / Timothy Ruff
- 1N/ A Business Person’s Guide to Understanding IIW or The Burning Man of Digital Identity / Ken Ebert

Session 2

- 2A/ Open Wallet Update + Call for Projects / Tracy Kuhrt & Daniel Bachenheimer / Lucy Yang & Kaliya Young

- 2B/ IIW 101 User Managed Access (UMA) Get to know this unique “application of OAuth” / Eve Maler
- 2C/ The Android & Web Identity API - Proposals / Lee Campbell and Sam Goto
- 2D/ Oauth First Party (native) Apps / Jeff Corrigan
- 2E/ NO SESSION
- 2F/ didwebs for Muggles / Markus Sabadello & Lance Byrd
- 2G/ NEW FUNCTIONALITY brought by ‘Verifiable Presentation with Message / Kazue Sako & Ken Watanabe (sp?)
- 2H/ NO SESSION
- 2I/ NO SESSION
- 2J/ NO SESSION
- 2K/ Grounding Identity in Truth / Shane Oren
- 2L/ DIF Credential Trust Establishment - Practical Governance / Sam Curren
- 2M/ BC Gov \$100K Con - Bring AnonCreds to W3C VC Format / Stephen Curran
- 2N/ NO SESSION
- 2O/ NO SESSION

Session 3

- 3A/ Open Wallet Update + Call for Projects / Tracy Kuhrt & Daniel Bachenheimer / Lucy Yang & Kaliya
- 3B/ IIW 101 - User Managed Access (UMA) Get to know this unique “application of OAuth” / Eve Maler
- 3C/ The Android & Web Identity API - Proposals / Lee Campbell and Sam Goto
- 3D/ Oauth First Party (native) Apps / Jeff Corrigan
- 3E/ NO SESSION
- 3F/ didwebs for Muggles / Markus Sabadello & Lance Byrd
- 3G/ NEW FUNCTIONALITY brought by ‘Verifiable Presentation with Message / Kazue Sako & Ken Watanabe (sp?)
- 3H/ NO SESSION
- 3I/ NO SESSION
- 3J/ NO SESSION
- 3K/ Grounding Identity in Truth / Shane Oren
- 3L/ DIF Credential Trust Establishment - Practical Governance / Sam Curren
- 3M/ BCGov Offers \$CDN100k: Adding Support for W3C Format VCs to AnonCreds v1.0/ Stephen Curran
- 3N/ NO SESSION
- 3O/ NO SESSION

Session 4

- 4A/ Introduction to Trust Over IP Foundation ToIP / Judith Fleenor - ED
- 4B/ IIW 101 - Web AuthN / John Bradley
- 4C/ Credential vs Wallet Selection / Samuel Goto & Tim Capalli (sp?)
- 4D/ NO SESSION
- 4E/ How Are You Solving for the UX Challenges of Self Sovereign Identity? / Gabriel Chartier
- 4F/ SOLID / Doc Searles & Hadrian Zbarcea
- 4G/ Privacy as Alignment of Expectations / Joe Andrieu
- 4H/ Speed Proof of Concept - Can we solve a problem in an hour? / Kyle Peacock

- 4I/ Confidential Computing Changes Everything - Enabling a Universal Name System (UNS) and Universal Certificate Authority / Manu Fontaine
4J/ did:PLC: 1,000,000 uses app / Aaron Goldman
4K/ KERI for dummies / Timothy Ruff
4L/ Externalized Authorization / Omri Gazitt
4M/ Brainstorm: How SSI can solve the Data Exchange Problems or Healthcare ? (KERI / vLEI / SCDC) / Jared Jeffery
4N/ Memory-Based Private Keys! Enforcing Entropy Using AI!!! OMG! / Matthew Vogel

Session 5

- 5A/ ToIP Trust Spanning Protocol for Muggles / Drummond Reed, Wenjing Chu, Sam Smith
5B/ IIW 101 - SSI (Self Sovereign Identity) / Nuttawut Kongsuwan & Catherine Nabbala
5C/ NO SESSION
5D/ Federated Authentication Network / Day Waterberry
5E/ FEED ME! Unified FEED - What do we need in a Unified Feed of all Asynch communication / Steve Vitka
5F/ AuthZ Conference / Sarah C
5G/ Improving the W3C CCG DID Method Registry / Martin
5H/ JSON-LD BBC+VC with Holder Binding & Pseudonyms
5I/ WIMSE - Workload Identity in Multi-System Environments / Justin R
5J/ NO SESSION
5K/ Building Test Suites / Ben Goering
5L HACKATHONS! did:Hack Decentralized ID Foundation - Learn more, get involved Get Hacking / Limari
5M/ Secure Issuance for Government Credentials / Paul Bastian, Torsten Lodderstat
5N/ Identity + Peer Production / Brent Shambaugh

Wednesday October 11, 2023 Day 2 / Sessions 6 - 10

Session 6

- 6A/ BIP32 and You (Fido Row Signatures / John Bradley
6B/ GNAP 101 / Justin Richer
6C/ People don't want a digital identity: / Adrian Gropper
6D/ NO SESSION
6E/ Philosophy: The code behind the code. / Samuel G Hutchens
6F/ GLEIF's experience with the vLEI Ecosystem Governance Framework: Lessons Learned / Karla McKenna
6G/ Human OS - Functional / Modality Challenges - Real World / Digital World / Jeff Orgle
6H/ NO SESSION
6I/ Philosophical Foundations of Identity / Bruce Conrad
6J/ NO SESSION
6K/ Dying w/ Dignity - A consent driven dead man's switch for online services / Dean Saxe
6L/ MFA/Passkeys for unstably housed and other populations who have trouble maintaining possession of physical factors / Matt MacAdam
6M/ NO SESSION
6N/ NO SESSION

Session 7

- 7A/ Wallet Security & IETF Attestation-based Client Authentication / Paul ? and Markus ?
7B/ State of Idm Policy Interop / Gerry Gabel and Phil Windley
7C/ Trust Spanning Protocol (TSP) Deeper Dive / Wenjing Chu, Sam Smith, Drummond Reed

7D/ W3C VC-Edu Plugfests! Credential rendering! Trust Registries! Schemas! / Kerri Lemoie, Dmitiri Zagidulin, Simone Ravaioli

7E/ NO SESSION

7F/ Standards-Based Digital Credentials Flavors Explained / Kaliya Young and Lucy Yang

7G/ VC over Ceramic / Golda Valez and James Pham and Aaron Goldman

7H/ Create Your Own did:webs / Markus Sabadello and Lance Bryd

7I/ PDP & PEP vs. AS/RS Smackdown (How to map them properly?) Eve Maler - Allan Foster - Justin Richer

7J/ NO SESSION

7K/ The Synchronic Web / Thien-Nam Dinh

7L/ Verifiable Government / Timothy Ruff

7M/ Online Travel ssi + data privacy - Dif + TolP TF Sig Work / Neil Thompson

7N/ NO SESSION

Session 8

8A/ US Healthcare on Trial: Decentralized Identity Use Case Assessment Frame / Sophia Goeppinger

8B/ (IETF) Status List & Revocation Mechanisms / Christian Bormann + Paul Bastian

8C/ Blockchain - Free Proof of Humanity / Brad DeGraf Noonao

8D/ Serverless, Data baseless, Programmable, Smart Wallets (PICOS) / Phil Windley

8E/ Are there too many identity.orgs? Could we consider how to accomplish our goals w/less of them / Kaliya Young

8F/ Ozero - AuthN in Seconds - Removing Manual OIDC Config / Dick Hardt

8G/ Experiments with JSON-LD payloads secured by JWS vs Data Integrity / Markus ?

8H/ World Coin - Its Privacy Impacts / Shin'ichiro Matsuo, BGIN

8I/ What Should DIF (Decentralized Identity Foundation) do for interop? / Brent Shambaugh

8J/ NO SESSION

8K/ NO SESSION

8L/ Augmenting OID4VC with DIDComm / Sam Curren

8M/ UX for Privacy - Questions NOT Answers / Alan Karp

8N/ Aries Bifold & APP Attestation / Jason Leach, Clecio Varjao

Session 9

9A/ Making the Internet AGE Aware / Iain Corby

9B/ Converging OID 4 VC Profiles / Torsten Loddersted, Kristina Yasuda & Harmen Van Der Kooij

9C/ Abbreviated Language for Authorization / Mark Berg & David Brossard

9D/ KERISSE.org - Learn Keri! / Henk Van Cann

9E/ Targeted Log OUT / Aaron Parecki

9F/ Browser API Wallet Query Lang / Sam Gogo

9G/ Should Governments be involved in VC ecosystems? / Naoki Yagita and Rintaro Okamoto

9H/ Secure Organizational Identity / Lance Byrd & Rodo & Alex Andrei

9I/ Confidential DiD's - Solve Decentralized Key Management and Universal Zero-Trust / Manu Fontaine

9J/ Experiments with DIDs & DHTs / Gabe Cohen & Daniel Buchner

9K/ OIX Roaming Between Trust Frameworks / Mark Haine

9L/ Using DIDComm to protect files in cloud storage / Steve McCown

9M/ IEEE 7012 - Personal Terms and Conditions / Daniel Hardman

9N/ Digital Credentials Cons. - VC-API SPEC Implemented as Microservers in Docker Compose / James Charraud

Session 10

- 10A/ International Interoperability Summit - Paris Next Month / Gail Hodges + Mark Hodges
- 10B/ Sustainable Privacy Re-Identification Attacks / Sam Smith
- 10C/ Fitting credentials that are verifiable into NISTs digital identity guidelines - SP-800-63-4 / Justin Richer
- 10D/ Identity is a Graph Problem / Alex Babeanu
- 10E/ IDP Discovery thru Wallets / Aaron Parecki
- 10F/ Accelerating Broad Adoption of Digital Trust Technology: British Columbia's approach / Nancy Norris & Aaron Unger
- 10G/ AnonCreds V2: BBS+, more ZKPs, (perhaps) PQ and CODE!!/ Stephen Curran
- 10H/ Universal Wallet Backup Containers / Sam Curren
- 10I/ P3Sub (Push-Pull-Publish-Subscribe) a new protocol / Johannes Ernst
- 10J/ Veramo – DIF Building the community-led supermodular framework for decentralized agents / Nick Reynolds
- 10K/ Identity Governance - Who? What? How? / Wendy Seltzer
- 10L/ Minimum Interoperability Profile for ACR (authentication context) / Pam Dingle
- 10M/ The many different flavors of Selective disclosure + consent/privacy / Francisco Corella, Neil Thomson
- 10N/ DEEPFAKES +AI Threats to ID Proofing + verification systems “AI is Rocket Fuel for Fraud” Andrew Hughes

Thursday October 12, 2023 Day 3 / Sessions 11 - 15

Session 11

- 11A/ Stitching Together a Web Wallet - What's there & What's missing / Neils Flensted
- 11B/ Selective Disclosure is Useless - we have receipts / Timothy Ruff and Sam Smith
- 11C/ NO SESSION
- 11D/ NO SESSION
- 11E/ Compassion. IO (how to give/receive help in the virtual world, safely, securely, reliably) / Samuel Goto
- 11F/ OID4VC Interop Profiles Convergence / Kristina Yasuda, Torsten Lodderstedt, Harmen Van Der Kooij
- 11G/ BUBBLES? Federation in disadvantaged and disconnected environments / Justin Richer
- 11H/ NO SESSION
- 11I/ VC ‘render Method’ displaying & rendering verifiable credentials / Dmitri Zagidulin / DCC
- 11J/ NO SESSION
- 11K/ NO SESSION
- 11L/ Bhutan: National ID and SSI / Ethan Veneklasen + Drummond Reed
- 11M/ NO SESSION
- 11N/ NO SESSION
- 11O/ NO SESSION

Session 12

- 12A/ Brainstorm: Digital Identity as a tool in the fight against child sexual Abuse Material (CSAM) PRIVACY vs CSAM / Michael, Andy, John
- 12B/ The SR-71 Could Not Fly without me / Britt Blazer
- 12C/ TOPAZ - Demo / Omri Gazitt
- 12D/ Cookie Binding as a Browser Standard !! (seeking interest and opinion) Kristina Yasuda & Sameera Gajjarapu
- 12E/ Philosophy of the Crowds - Moral construction in the age of Internet Identity / Thien-Nam
- 12F/ eIDAS 2 Status & AMA / Paul & Torsten
- 12G/ Transaction Tokens Authorization for Multi-workload environments / George Fletcher

- 12H/ DIF = Decentralized Identity Foundation Update - What's the DIF? How to be involved + Hackathons / Limari Navarrete
12I/ University "Intro to Digital Identity" / Jo Windley
12J/ NO SESSION
12K/ Composable P2P Identity Components on Holochain (no a blockchain) / Arthur Brock
12L/ DIDATA - Decentralized Intelligent Decision and Trust Agent / Matthew Hailstone
12M/ DID Method Enumeration micro-spec / Sam Curren
12N/ NO SESSION

Session 13

- 13A/ Conceptual History of Society + Identity / Haro
13B/ ACDC (Authentic Chained Data Containers) for Muggles/ Drummond Reed and Sam Smith
13C/ What does Presentation Exchange do? ...and which parts of it do we actually need? / Mike Jones
13D/ NO SESSION
13E/ NO SESSION
13F/ 21st Century Voters Here to Save the Day / Spener Shirman, Britt Blaser
13G/ Key-Based Auth Convox + Convergence / Day Waterbury, Duke Jones, Fan
13H/ Low Code a Path to Adoption / Jesus Torres
13I/ Did.web Improvements Challenges / Dmitri Zagidulin
13J/ APAC Digital Identity OpenSpace unConference - Late 2024 - come discuss how to contribute to making it a success! / Heidi Nobantu Saul
13K/ NO SESSION
13L/ Identity STORIES / Erica Connell
13M/ Organizational Ecosystem with BCGov - Lessons learned on adoption and governance / Kyle Robinson , Nancy Norris
13N/ NO SESSION

Session 14

- 14A/ CLAIM-BOUND VCs - no keyinding? Matching by biometric / names / Paul and Torsten
14B/ Authentic data is the real sh** NOT digital identity / Sophia Goeppinger, Timothy Ruff
14C/ NO SESSION
14D/ PLAN Pico Labs Affiliate Network picolab.github.io/PLAN / Bruce Conrad
14E/ InterSubjectivity Open Discussion / Will Abramson
14F/ Authorization Exchange AuthZEN / Allan and Gerry
14G/ NO SESSION
14H/ Demoscene Dark Matter - Identity Digital Subculture / Andre Kudra
14I/ Human Rights impact of Digital Identity Protocols / Adrian Gropper
14J/ NO SESSION
14K/ Consumer Apps in Decentralized Identity / Matt Murray
14L/ Identity through IOT deploying aca-py on balena cloud / Patrick St-Louis
14M/ Did:peer:4 A Document in the DID + Demo / Daniel Bloom
14N/ NO SESSION

Session 15

- 15A/ ToIP (and everyone's) GLOSSARY - How can we all speak the same language (learn acronyms) / Drummond Reed
15B/ TOKEN BUckets / Justin Richer
15C/ POST-CAPITALIST Funding & Governance / Kay Waterberry and others
15D/ NO SESSION
15E/ NO SESSION

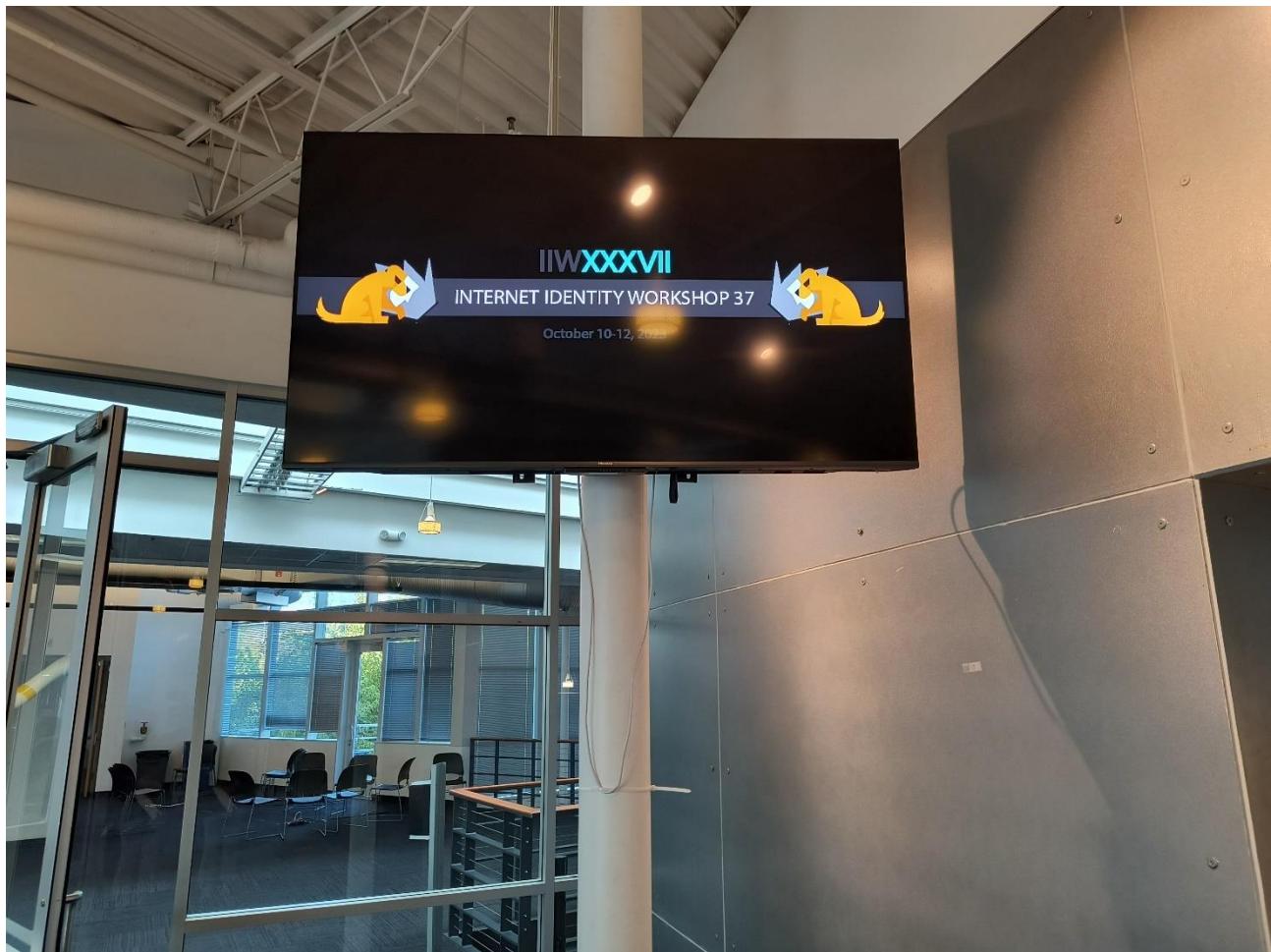
15F/ Demo decentralized identity use case assessment framework US healthcare / Sophia Goeppinger

15G/ Biometric Holder Binding - The Good Bad Ugly / Dan Bachenheimer

15H/ Real - IT Party Frontal Guerrilla Rebellion ? Jeff Orgel

15I/ KiRA - Key Infrastructure with Remote Attestation (confidential computing) Manu Fontaine

15J/ NO SESSION



Notes Day 1 / Tuesday April 18 / Sessions 1 - 5

SESSION #1

OpenID for Verifiable Credentials - The next generation of OpenID

Session Convener: Torsten Lodderstedt, Kristina Yasuda

Session Notes Taker(s): Jin Wen

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

Slides: <https://www.slideshare.net/TorstenLodderstedt/openid-4-verifiable-credentials-haip-update>

Digital Credentials Protocols WG

<https://openid.net/wg/digital-credentials-protocols/>

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

Based on the attached message, the key understandings, outstanding questions, observations, and action items are as follows:

Key Understandings:

- There is a new [OpenID working group](#) for Digital Credentials Protocols, which includes OpenID for Verifiable Credentials (OID4VC)
- Protocol Layer Interoperability is Crucial for communication between different systems and players.
- The European Union has chosen OpenID for Verifiable Credentials for its European Digital Identity Wallet.
- NIST is working on a project to boost the adoption of ISO 18013-5 mobile driving licence (mdoc) and OID4VC

Outstanding Questions:

- How can credentials be moved between wallets and devices?
- How can the right wallet be determined for credential issuance?

Observations:

- There are various open-source libraries available for implementing OID4VC
- A new High Assurance Interoperability Profile is added.
- The protocol is designed to be flexible and work with different credential formats.

Action Items/Next Steps:

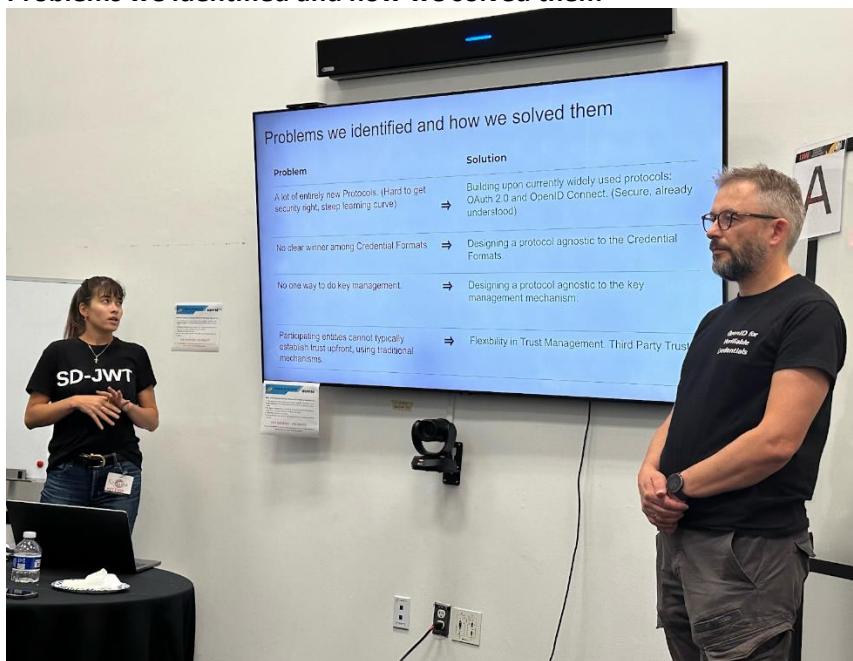
- Attend sessions on different profiles and trust management to learn more about OID4VC implementation.
- Investigate the possibility of syncing credentials across devices and ecosystems.
- Consider joining the OpenID working group to contribute to discussions and stay updated on developments.

Please note that this summary is based on an audio transcript with some parts being unclear or inaudible.

Why Protocol Layer Interoperability is Crucial

One entity needs to talk to the large the number of entities, to increase the value of “Decentralized Identity”

Problems we identified and how we solved them



Developer friendly: built upon widely used OAuth 2.0 and OIDC
Credential format agnostic

Principle Benefits

cryptographically proven
privacy preserving
open standards - vendor neutral

Adoption (selected use-cases)

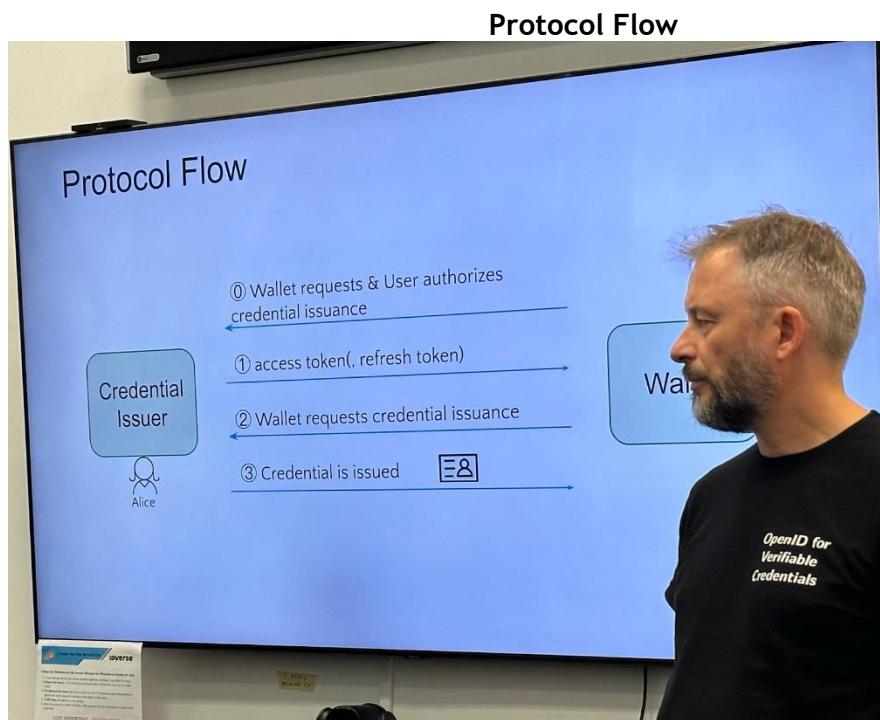
- EUDI wallet
- NIST national cybersecurity CoE
- DIF JWT VC issuance / Presentation profile

OID4VC Formal Security Analysis

one of the contributions from
related spec: DCP-SecTrust - Digital Credential Protocols Security and Trust (see early draft:
<https://vcstuff.github.io/oid4vc-security-and-trust/draft-oid4vc-security-and-trust.html>)

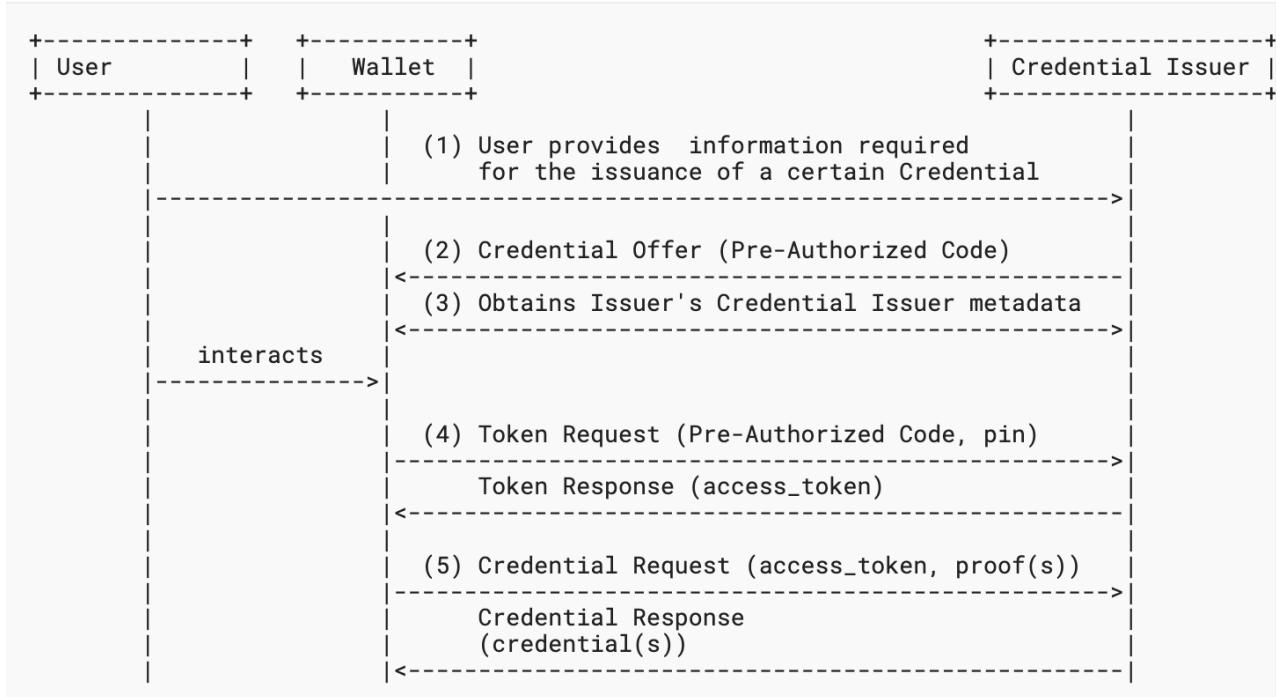
OpenID for Verifiable Credential Issuance (Highlights)

- It's an OAuth-protected API (Credential Endpoint at the Resource Server)
 - o Leverages existing OAuth features and implementations
 - o Easy of use for developers
- Supports various Security levels (including high security with hardware bound keys)
- Various business requirements supported (ex. remote and in-person provisioning)
- Different user-experiences can be achieved (multiple ways to initiate the flow)
- Issuer can check Wallet's capabilities & Wallet can discover Issuer metadata



Authorization Code Flow

https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-11.html#name-authorization-code-flow



Pre-Authorized Code Flow (Overview)

<https://openid.github.io/OpenID4VCI/openid-4-verifiable-credential-issuance-wg-draft.html#name-pre-authorized-code-flow>

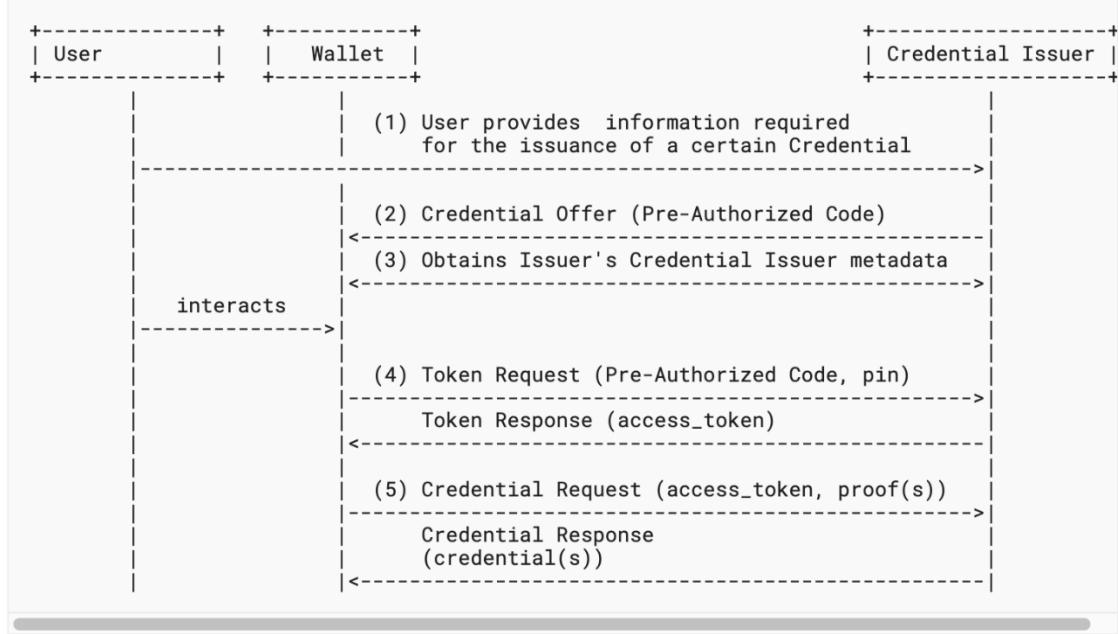


Figure 2: Issuance using Pre-Authorized Code Flow

Actors

User

Wallet

Credential Issuer: Web site, Credential Issuance API

Security and privacy properties of the OID4VC protocols

OpenID for Verifiable Presentations (Highlights)

developer friendly
different user experience
multiple credentials support
different security requirements (supporting High Assurance PI)

same device presentation
cross device presentation

IIW 101 Session - OAuth 101

Session Convener: Aaron Parecki

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

Cedar Policy Language 101

Session Convener: Darin McAdams

Session Notes Taker(s): Sarah Cecchetti

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

Cedarpolicy.com

<https://github.com/cedar-policy>

<https://communityinviter.com/apps/cedar-policy/cedar-policy-language>

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

Cedar policies have a PARC model: principal, action, resource, conditions

Cedar language gives you an allow or deny based on a policy set

AWS has a managed service that offers Cedar called Amazon Verified Permissions

Cedar is open source - both the core language and a rust library with bindings to various other languages.

If you're familiar with Rego, it's very similar.

Cedar is designed to be fast and have bounded runtimes, so it doesn't allow things like loops that might never terminate.

It's designed to be ergonomic, meaning that it's easy to read and write.

Cedar is implemented in a theorem proving language called Dafny that mathematically proves that the language implementation matches the specification.

Cedar can also help you catch logical errors in your policies.

The Cedar team didn't want to write a language - but existing languages were clustered into languages that were expressive but not performant or performant but not expressive, and none of them were amenable to automated analysis. Cedar was designed to be performant, expressive, and analyzable.

How does this interact with CAEP?

CAEP might help get the data into the authorization engine.

What are best practices around writing policies? Should I write them by hand?

It's going to be important as we put UX around it. Every vertical is going to be different.

Cedar sees two audiences: people who want to write raw statements or use a policy authoring tool, and then people who want to use applications to generate policies like photo sharing

If you have a bunch of policies and you're going to ingest another bunch of policies, how does Cedar highlight conflicts or precedence errors?

Cedar has a very straightforward evaluation algorithm - deny by default. Policies are not ordered, they are all evaluated at once. Unless a policy allows it, the action is denied. If policies both allow and forbid, the action is also denied.

Cedar has baked in support for entity hierarchies, enabling RBAC that has a concept of hierarchical groups. It also supports ABAC and you can mix them.

The PARC format of Cedar policies enables clients to “slice” a policy set so that you can tell which policies are relevant to your context, so you don’t have to download the whole policy set, but you have assurance that the answer is the same as it would be if you evaluated the full policy set.

Cedar is implemented in Rust which is secure and fast - most Cedar calls evaluate in less than a millisecond.

Rust is not a theorem proving language, so we have a specification of Cedar in Dafny. There is differential testing to ensure that the two are equivalent.

Are there situations where people want to know more than permit or deny? Yes, they want diagnostics around why access was or wasn’t permitted.

Partial evaluation will enable you to ask questions like “who does have access to this resource?” And “what resources does Alice have access to?”

Can you set up guardrails to tell me when I accidentally open up a hole?

Yes, we intentionally built the language to be amenable to automated reasoning.

If I have five policies that allow, will it return all five?

Yes

Validation in Cedar can detect improper relationships or data typing.

Policy analysis can tell you whether a policy will never authorize anything or whether two sets of policies are equivalent.

If DID is So Good, why don't I have one yet?

Session Convener: James Monaghan

Session Notes Taker(s): Zaïda Rivai

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

The four core properties of a DID:

1. A permanent (persistent) identifier

It never needs to change.

2. A resolvable identifier

You can look it up to discover metadata.

3. A cryptographically verifiable identifier

You can prove control using cryptography.

4. A decentralized identifier

No centralized registration authority is required.

If decentralized ID is so great, why don't I have one yet?

- Where might I get my first (useful) DID
- What obstacles exist
- How should we make people aware? Explain it.

When can I have a decentralized ID?

What makes an Identity Decentralized? How can I take it from one service to another (portability).

1. Decision makers: don't understand

Who thinks you will get your first verifiable credential:

- Government: 13
- Social media: 1
- Finance: 0
- Your employer: 5
- Education: 6
- Social Media: Speed is much faster. VC: bitcoin passport.
- Gov: Slow. Speed a
- A lot of verification age: must not keep

Instances:

- TrueAge: buying physical good.
- BC government
- Military connect: can verify

What obstacles exist: *Even if I had one today? How do I know how the issuer is?*

- The pain has to be really bad.
- No one cares about having an autonomy.
- 21 million fake ID's a day in Europe.
- Ecosystem is huge.
- Those that write the checks, the business decision makers don't understand. They want to make it a property investment for themselves. That falls down in interoperability.
 - If I create something in SOLO, how can that become interoperable?
 - How do you compare to other technologies?
 - All the frameworks that are currently available. You need to decide to go there.
- One trust framework? Is that possible?
- Legally: can't use a digital ID to buy alcohol? You need to change your ID.
- People's perception of a digital service, entire service is in one single app. Digital credentials: you have your mobile wallet, collect from various sources (businesses, gov etc...) and talk to a third player.
- Standard way of doing thing:
- Multi party marketplace: manufacturing the (military connect).
- There is no immediate value for the consumer
- If the issuer isn't using it for themselves, not so interesting. Is it easy to access already
- Eliminate a lot of friction for the consumer, form filling etc... Bureaucracy will be done much easier. People need to experience the benefits.
- Age assurance: should enforce this such that the digital ID version is the ONLY way to use certain websites.
- Not just use digital credentials to do something
- Identity: low frequency use case? How often are you actually using this?
- Identity: establishing digital relationships, rather than just 'Identity'.
- Urgency isn't there yet
- PKI infrastructure.
- Many think that tooling is necessary
- BC: law issues VC to lawyers. Lawyers can get an ID. VC wallet: developing our mobile verifiable capability. Pre program proof request. Whole bunch of permutations. What motivates a lawyer: applications, lawyer is doing that in their job to access documents, so they got that motivation to get their credentials. Has nothing to do with credentials. They can be used outside of BC.
 - Proof of authority.
- 20 millions pounds could be saved in UK healthcare.
- Confusing the benefits of digital identity with decentralized Identity.

How many use cases can be served using MDL

- You cannot present the MDL to Utah, but you can groceries, credit union, airport,

Risk assurance.

1. Lack of interoperability
2. Communication
3. Definitions

What is the Future WE want to create?

Session Convener: Samuel Hutchens
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:

The Future of We that We want to create should be one of Value, Core Stds and Impactful to what The Present requires in avoiding redundancy.

Ethical AI - assisted note taking

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

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

No Notes Submitted

The Chicago Economics School Catalyzed the Corps that ARE the Identity Crisis

Session Convener: Britt Blaser
Session Notes Taker(s): Britt Blaser

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

https://docs.google.com/presentation/d/1x_05KFq9F3E6Mh54sjNq2Ufh4fS2TJ841RX-8v3D-XY/edit#slide=id.p1

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

No Additional Notes Provided

Credentials & Risk? Why Shared Data? (Linked Claims)

Session Convener: Golda Velez, Phillip Long, & Dmitri Zagidulin
Session Notes Taker(s): Phillip Long

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

Verifiable_Credentials LinkedClaims hashlinks multibase

[LinkedTrust.us](#),

[Composing Credentials with LinkedClaims and Cryptographic Bindings](#), RWOT11, The Hague, 2022

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

The presenters introduced LinkedClaims as having two distinguishing features.

- 1) Leveraging the binding of two different self-issued verifiable credentials with a link, and
- 2) Describing a new linking method that involves using multibase encoding of the digest hash of the address and the content pointed to, and applying a proof to those together to establish a tamper evident binding or hashlink between the two credentials

VC: eg. illustrating a generic VC claiming a skill

-
- when issued
 - issuer
 - id: URN: UUID: 123/CID/<https://example.com/vc/123>

 - subject: Dmitri
 - knows how to draw
-

Proof

What are the use cases for which LinkedClaims was developed?

- **Linking two VCs** and more specifically linking not just to a VC as an object but to individual claims *within a VC* that have IDs to anchor to them
- Proofed hashlinks to external resources
 - PDFs
 - images
 - webpages
 - etc. etc.
- evidence - pointing to evidence associated with an evidence claim in a VC
 - any of the digital objects listed above but also GitHub repo contents (or the repos themselves)
 - video files demonstrating a skill or competence
- 3rd Party confirmations

- a recommender making a claim in a self-authored VC to corroborate a skill, competence or other attribute included in the recommendee's self-authored or organizationally issued VC
- adversarial attestations
 - a self-authored credential that points to a claim in another credential challenging that claim (note this raises the question how the contested claim is found by the person challenging it).
- audits
 - this use case applies to a third-party individual investigating the use of say philanthropic funding intended to cover the costs of goods or services delivered to a target community actually arriving and being used as expected. The investigator writes a self-authored credential with 'evidence' (pictures, audio recordings of interviewees, etc.) to corroborate the delivery as per expectations, or not.

A more formal representation of a linkedClaim from the RWOT11 paper is presented below:

Example: A Verifiable LinkedClaim

This example is composed of two components – an initial standalone VC and then an LinkedClaim of that VC, with a one way cryptographic binding to it.

Initial (Self-issued) VC:

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/openbadges/v3"
  ],
  "type": [
    "VerifiableCredential",
    "OpenBadgeCredential"
  ],
  "issuer": {
    "id": "did:key:z6MkrHKzgsahxBLyNAbLQyB1pcWNYC9GmywiWPgkrvntAZcj",
    "name": "Alice Jones"
  },
  "issuanceDate": "2022-05-01T00:00:00Z",
  "credentialSubject": {
    "type": "AchievementSubject",
    // Note that the subject of the VC is the issuer, hence self-issued
    "id": "did:key:z6MkrHKzgsahxBLyNAbLQyB1pcWNYC9GmywiWPgkrvntAZcj",
    "achievement": {
      "id": "urn:uuid:e8096060-ce7c-47b3-a682-57098685d48d",
      "type": "Achievement",
      "name": "UAV Control System for Drone Navigation",
    }
  }
}
```

```

    "description": "<description goes here>",
    "criteria": {
        "type": "Criteria",
        "narrative": "<narrative>"
    }
},
"proof": {
    // Signature goes here
}
}

```

LinkedClaim to the above VC:

```

{
    "@context": [
        "https://www.w3.org/2018/credentials/v1",
        "https://w3id.org/security/suites/ed25519-2020/v1",
        "http://cooperation.org/credentials/v1",
        "@vocab": "http://cooperation.org/credentials/v1#"
    ],
    "type": [ "VerifiableCredential", "VerifiableRecommendation" ],
    "issuer": {
        "id": "did:web:bob.example.com",
        "name": "Bob"
    },
    "issuanceDate": "2010-01-01T00:00:00Z",
    "expirationDate": "2020-01-01T00:00:00Z",
    "credentialSubject": {
        // Note that the credentialSubject.id is the id of an individual Achievement in
        // the target VC
        // It could just as readily be the id of the VC, but the authors wanted to
        // highlight that a section of the VC could be targeted
        "id": "urn:uuid:e8096060-ce7c-47b3-a682-57098685d48d",
        "digestMultibase": "zb1B1M6Bve5JEaNqeJSmuE", // digest of the Achievement being recommended
        "recommendation": {
            "statement": "This is a recommendation regarding Alice's 'UAV Control System
            for Drone Navigation' achievement. Alice has an exceptional skill set as an UAV
            guidance control engineer. See also the attached evidence."
        },
        "recommender": {
            "id": "did:web:bob.example.com", // MUST be same as issuer
            // the recommending entity's bona fides, tailored to the specific claims
            // on a per-use basis
            "relevance": [
                // Generic expertise claims (such as CV / resume / degrees)
                {
                    "id": "https://SmartResume.com",

```

```

    "type": "SmartResumeProfile"
},
{
  "id": "https://linkedin.com/Bob",
  "type": "LinkedInProfile"
},
{
  // link to a credential I received saying I have a degree to this subject
  "id": "https://example.edu/degrees/class-of-2021/bob", "name": "University Degree Credential"
},
{
  "id": "https://sigspatial.acm.org/members/12345",
  "description":
    "https://www.acm.org/special-interest-groups/sigs/sigspatial",
  "name": "SigSpatial Membership Credential"
},
// Specific expertise item tailored to the recommendation
{
  "id": "https://example-journal.com/my-article.pdf",
// optional hashlink (note that 'multibase' is a part of the in-progress
// IETF spec https://datatracker.ietf.org/doc/html/draftmultiformats-
multibase
  "digestMultibase": "zQmdfTbBqBPQ7VNxZEYEj14VmRuZBkqFbiwReogJgS1zR1n",
  "name": "Control Systems in Unmanned Flight",
  "citation": "...",
  "description": "I have published an article in a peer-reviewed journal."
}
],
}
},
},
"evidence": [
  {
    "id": "https://github.com/example-org/control-testsuite/
tree/5ce453592c5fbaeb065453804e588868f5621ee", // verifiable point in the
commit history as the repo itself may change
    "type": ["recommendationEvidence"],
    "name": "Control System Test Suite",
    "description": "The code used to control a UAV delivering packages to an
address.",
    "digestMultibase": "..."
},
{
    "id": "https://control-systems-journal.example.com/12345.pdf",
    "digestMultibase": "zQmdfRKkx7Uf8Rpr079Uh",
    "name": "Geopositioning in Control Systems",
    "citation": "...",
    "description": "A particularly insightful implementation of geopositioning
with precision; I was very impressed with Alice's approach."

```

```

    }
],
"proof": {
  // Signature goes here
}
}
}

```

A simpler, more graphic way to demonstrate this idea :

LinkedClaims: LERs Bound Together

- 1 Multibase hashlinks
- 2 Linked Claims

Self-issued credential by job seeker

```

"@context": [
  "type": [
    "issuer": {
      "credentialSubject": {
        "type": "AchievementSubject",
        ...
        "achievement": {
          "id": "urn:uuid:e8096060...", ←
        }
      }
    }
  ]
]

```

PL

Self-issued LER LinkedClaim: supporting job seeker's assertion

```

"@context": [
  "type": [
    "issuer": {
      "credentialSubject": {
        "type": "SmartResumeProfile"
        ...
        "digestMultibase": "zb1B1M6Bve5JEaNqeJSmuE",
        "recommendation": {
          "statement": "recommendation statement.."
          "recommender": {
            "id": "did:web:bob.example.com", same as issuer
            "relevance": [
              {
                "id": "https://SmartResume.com",
                "type": "SmartResumeProfile"
                "id": "https://a-journal.com/article.pdf"
                "digestMultibase": "zQmdfTbBqBPQ7VN..."
                "name": "Control Systems in UAV Flight",
                "citation": "...",
                "evidence": [I can put in hashlinked evidence etc.
                "proof": {

```

Summary:

- LinkedClaims provide an on-ramp for incorporating unsigned data into complex proofed claims
- Hash-based linking (url + multibase hash) allows cryptographically binding to any permanent digital object
- Use of LinkedClaims implements the pattern human social recommendations as networked VCs
- LinkedClaims allows you to build a social graph of people in relation to their claims about each other when their claims are in publicly accessible locations

Questions that surfaced:

Q: How does hashlink binding two VCs where a specific claim in one is linked to a comment, corroboration or observation in another, differ from self-disclosure?

A: Self-disclosure is about selecting elements within a VC to include in a presentation of that VC to a third-party. If the holder chooses not to reveal an attribute within a credential they can create an

can select those assertions they wish to remain private and present only those that they would like to share.

LinkedClaims is more about building persistent connections between digital objects and credentials to add structure and facilitate a recipient (relying party) make connections that the holder would like to highlight between claims found in different verifiable credentials.

ARC Regenerative Communities

Session Convener: Day Waterbury

Session Notes Taker(s): Trent Larson

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

<https://www.hylo.com/groups/arc>

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

Basic premise: The most significant barrier to building a digital public goods stack is the misalignment of economic incentives under “accumulationist” capitalism. Funding tech-for-good requires new models, some of which are available now, and others which yet-to-be.

ARC Regenerative Communities proposes that we fund collaborative tech through the placement of real estate in perpetual trust in support of the creation of a network of land-based community incubator/innovation hub/institutes.

Case in point: Brewster Kahle of Internet Archive: 75% of money raised goes to people, but half of that goes to rent, so 38 cents of every dollar is lost to the landlords and banks. So he bought an apartment building and provided workforce housing to Internet Archive employees, calling it Foundation House. He would like to see 5% of all housing in the U.S. as “foundation housing” for non-profits.

The ARC vision takes this further, and would like to transition 100% of all land/resources out of the ownership model that serves extractive capital accumulationism and into a stewardship model aligned to the purpose of planetary thriving.

In permaculture practice, berms (little hills) and swales (little valleys) are built to direct and slow the flow of water to encourage it to soak into the landscape. We’re asking the question: What are the socioeconomic equivalents of berms and swales that encourage the flow of resources to soak into the landscape of our endeavors? How can we prevent resources from running off and pooling in the accounts of “old paradigm” rent-seeking value-ransomers.

People to read/listen to:

- Paul Krafel - wrote the book Shifting, which discusses flow.
- John Fullerton - Capital Institute (regenerative economics)

Perpetual Purpose Trust (PPT): A trust with a purpose as the beneficiary.

- Case study: Firebrand Bakery in Oakland, CA, a purpose-aligned for-profit LLC
 - 30% Founder, 30% PPT, 40% Investors and Worker-Owners
 - Has taken outside investments as dividend flips; higher dividend percentage until a minimum 2x return is reached, then riveting to a pro rata share.
 - PPT ensures continued alignment with the mission to reduce barriers to employment and provide living wage jobs
- Homeboy Bakeries hires only formerly incarcerated individuals (not sure if they have a PPT; curious about ownership/profit model)

Personhood of Living Places: rights of nature cum sovereignty of nature as a new legal basis for right relationship

- Examples in Aotearoa/New Zealand and Canada
 - In Aotearoa the Board of Stewards includes 6 indigenous community members and 3 representatives of the crown
 - Similar in effect to purpose trusts if you consider the continued wellbeing of the living place (e.g. mountain, river, etc) to be the purpose.

Cooperatives and Communes at various scales:

- Terran Collective
 - A small community of 5 or 6 that have made commitments to one another including cohousing, and income sharing and are collaborating on a development of a prosocial collaboration platform.
 - “Big Squad Energy”
- Mondragon
 - Diverse industries
 - Actual territory
 - Lots of vertical integration and member services
 - Essentially a small regional government in northern Spain
- Zebras Unite
 - A mutual support network of coops
- Obra
 - Multiple industries (tech, health, etc)

New ways of investing:

- Dividend Flip: taking higher dividend payments at first until they've reached their agreed return)
- Capped Returns: a limit to the amount of returns
- Incubating Public Goods with the intent to “Exit to Community”
- Ecosystem Raise: de-risking by spreading investments over an ecosystem of initiatives.

Recommended reading:

- Lewis Thomas - Lives of A Cell
- Frijof Capra - Tao of Physics
- David Graeber - Dawn of Everything

The goal of ARC is to assemble small groups to form alignments and have an emergent process where we incubate a different approach.

Side note: Ontological Commoning (credit to Steve Melville)

vLEI Developments and Updates

Session Convener: Karla McKenna

Session Notes Taker(s):

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

https://github.com/WebOfTrust/IIW37/blob/main/2023-10-10_vLEI-Update-IIW37-October_v1.0_final.pdf

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

Not the official note-taker, but I've posted some notes here:

<https://ericscouten.dev/2023/iiw/#session-1l-vlei-developments-and-updates>

Overview of ISO 18013-5 Mobile Driving License standard

Session Convener: Francisco Corella, Andrew Hughes

Session Notes Taker(s): Dan B

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

Andrew kicked-off the discussion with a brief overview of ISO, the International Organization for Standardization.

He explained that the subcommittee responsible for the mDL standard started working in about 2016 on the project called ISO/IEC 18013-5

This standard was published in September of 2021 and multiple entities including those in the USA, EUR, and AUS have started testing and rolling out infrastructure - including the TSA and AAMVA.

ISO/IEC 18013-5 is the standard for Local Presentation and includes

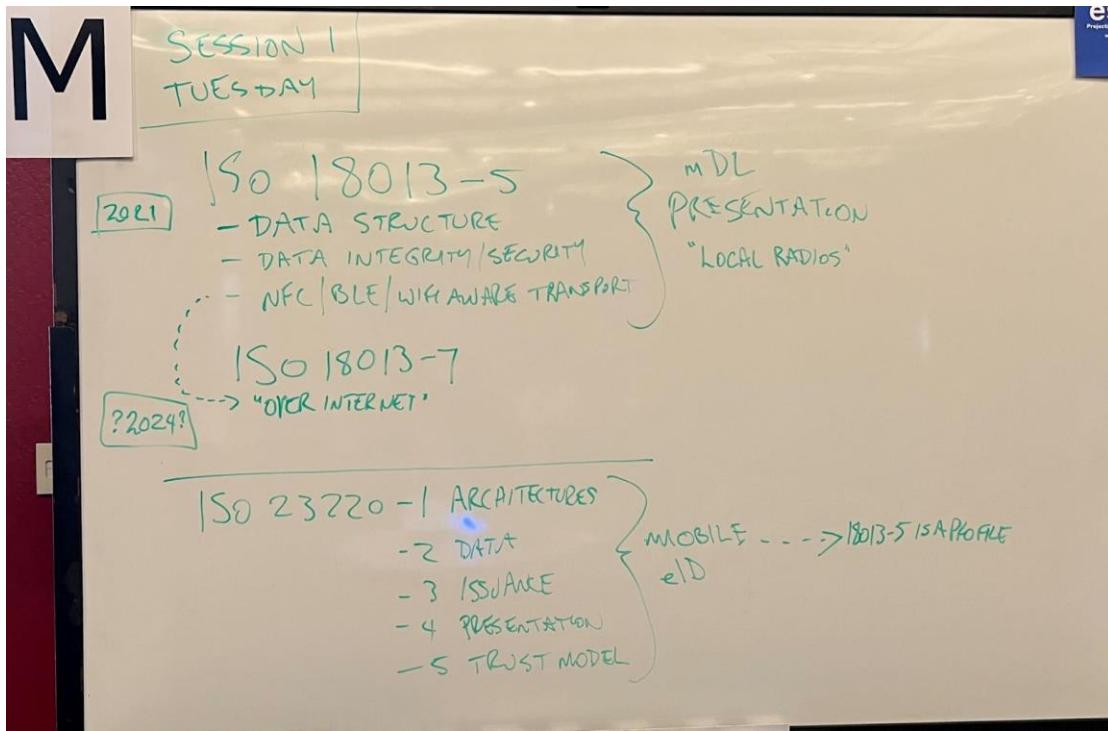
- Data Structure
- Data Integrity and Security
- Transport: QR Code, NFC, BLE, Wifi Aware

ISO/IEC 18013-7 will be the standard for Remote Presentation

- expecting publishing in 2024
- RESTful api to request identity info
- OpenID4VP to present identity info

Underlying the mDL “profile” (and others) is a series of standards which define the *Building blocks for identity management via mobile devices* :

- ISO/IEC 23220-1 Architecture
- ISO/IEC 23220-2 Data
- ISO/IEC 23220-3 Issuance
- ISO/IEC 23220-4 Presentation
- ISO/IEC 23220-5 Trust Model



Francisco picked it up from here. His presentation spoke to the *Innovations and Vulnerabilities of the ISO mDL*.

The powerpoint slides can be found at: <https://pomcor.com/documents/overview-of-the-mdl-standard.pptx>

Great work. Keep it current to the challenges that will come your way. Vulnerability is The Variable. The Std is The Constant.

SESSION #2

Identity Credential

Session Convener: Tim Cappalli

Session Notes Taker(s): Jin Wen

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

<https://github.com/WICG/identity-credential> to be more specific:

<https://github.com/WICG/identity-credential/blob/main/identity-credential-proposal.md>

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

Based on the attached PDF[1] and the additional text[2], the key understandings, outstanding questions, observations, and action items are as follows:

Key Understandings:

- The discussion revolves around wallet discovery, invocation, user experience, and privacy concerns.
- There is a debate on whether the browser should be involved in the invocation process or if it should only handle discovery.
- The group acknowledges the need for wallet selection during the credential provisioning process.

Outstanding Questions:

- What information should be provided to the OS or browser for discovery?
- How can the user experience be improved without crossing the privacy line?
- Is it possible to create a system that satisfies both privacy and user experience concerns?

Observations:

- Multiple communities are coming together, each with different trust levels and perspectives.
- The group recognizes the importance of agreeing on the problem and finding a solution that works for all parties involved.
- There is a concern about the adoption of the proposed API and its potential limitations.

Action Items/Next Steps:

- Explore different approaches, including origin trials, to find a solution that satisfies both privacy and user experience concerns.
- Consider the developer experience when designing the API and its implementation.
- Discuss the possibility of providing enough information to the OS or browser for discovery without compromising privacy.
- Continue the conversation and collaboration among the group members to reach a consensus on the best approach for wallet discovery and invocation.

Citations:

[1] <https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/1666532/c7467032-ab70-4f62-b82f-8d81037061cc/wicc-identity-protocol-31-minutes.pdf>

[2] <https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/1666532/6f3f1fa4-e037-4865-8d12-60f2e67011d3/paste.txt>

Introduction to OpenID Connect

Session Convener: Michael B. Jones

Session Notes Taker(s): Michael B. Jones

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

The presentation is posted at https://self-issued.info/presentations/OpenID_Connect_Introduction_10-Oct-23.pptx and https://self-issued.info/presentations/OpenID_Connect_Introduction_10-Oct-23.pdf.

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

Approximately 30 people attended the session and there were some great questions!
This was an invited “101” session.

Artificial Intelligence and Copyright

Session Convener: Wenjing Chu

Session Notes Taker(s):

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

Response to the Copyright Office’s Notice of Inquiry and Request for Comment 2023-6

What is AI? Create models to predict things

What is Copyright? Trade off/balance that gives a creator rights for a given amount of time; protect against copying

We specifically discussed these 3 questions:

- Is a work created by someone using Generative AI tools copyrightable?
- When someone uses copyright protected material in Generative AI training, should they get the author’s permission and licence? Is it “fair use”? Is it just “reading” (not ‘copying’)?

- Can identity tools we discuss in IIW be used for transparency and provenance in an effort to help solve the dilemma?

The group had a wonderful and lively conversation - thanks for all attendants who contributed to this session including at least two attorneys! Thank you.

The group had a final note: when the Internet came along many years ago, we all casually gave up a lot of our private data for nothing. We must not let that happen again in the age of AI.

The following are notes taken by Tracy Tuhrt. Thanks Tracy.

Notes:

Question from audience member: does this differentiate between AI and Gen AI?

Discussion around Writer's Guild and the output of AI generated content

Copyright office said that the graphic created by Midjourney was not covered by copyright. Only text written in the graphic novel.

No copyright for items created by a machine.

The Constitution says "authors" in relation to copyright. The discussion currently is around what is an author

Discussion around existing technology (drones to drop paint, camera to take pictures) and how you can copyright the output by using these machines.

Software, digital media, games, digital music and generating these items.

Can you replicate the output?

Cannot copyright prompts because they are considered functions.

AI is a tool. People are required to add prompts.

If you have no copyright to the NFT, you have no rights to the copy either.

Discussion around "work for hire" and how a Hollywood studio requires "work for hire" to ensure the entire work can be copyrighted.

Training AI models with copyrighted work. Question 8

The answer may be different depending on the type of media (text, image, music). Is it fair use?

Fair use (1st amendment vs copyright clause - fair use is if it supported by the 1st amendment)

Does it reduce the value by feeding it into the model? Ingest vs. copy. Human brain vs. silicon brain.

Is the output an exact copy?

Provenance / content based watermark
Feeding into AI vs Using AI output
Contributory vs heresy
Copyright is strict liability. Intent does not matter.
Citations of the source for AI generated works
The ground is what is already on the internet

What did this specific weights does this data hit? What weights were used for the generated material? Registry with public information about where the data came.

Identity Proofing in Federated Systems

Session Convener: Jacob Siebach
Session Notes Taker(s): Jacob Siebach

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

Identity-proofing, federation, authentication, identity providers

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

Let us assume a three-tiered identity provider (IdP) system :the top being T1, the middle being T2, and the bottom being T3. When a user attempts to access a relying party (i.e. an application) at T3, the user is federated from T3 to T2, and then from T2 to T1, and the user signs in with their account at T1. If there are multiple independent IdPs on the third tier, all federating to one IdP at tier two (T2), what happens when a user at one of the T3 IdPs needs to change the account used at T1, without losing access to their systems fronted by T3?

The real issue is connecting the T2 account to the new T1 account; everything downstream of T2 will remain the same. In this scenario, T2 cannot pass any information to the T1 system; think of systems that use Google or Facebook as their IdP—they can authenticate users, but Google will not let you send info about your user in your app to be stored on their systems!

There are a couple of possibilities:

1. If there is an Identity Assurance Level (IAL, from NIST 800-63) sufficient at the provisioning of the account, then those processes could be used to identity proof the user and then change accounts. (For our specific circumstance this is not a valid option.)
2. When the account at T3 is provisioned, the user could be given a secret piece of information (some passkey) that could be used to prove that they own the T3 account. If

the user needs to create a new T1 account, they divulge the secret information to the admins who then know that the user does indeed own the T3 account.

3. As the T2 account contains information from T1 (sent as an assertion during previous authentications), the admins could use that information to verify that the user knows the info from the T1 account, and thus allow the connecting of the T2 account to a new T1 account.

It was generally agreed that, given the various constraints of the system, this is a Hard Problem.

“Selling to Enterprises” [sales]

Session Convener: Kapildev Arul Mozhi

Session Notes Taker(s):

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

Today's Session about Enterprise Selling(breaking the odds) Internet Identity Workshop 37 -

Computer History Museum  [ID](#)

- Strategize your go-to-market plan and ensure your product fits the market.
- Don't be afraid to make direct phone calls and put yourself out there.
- Embrace rejection and maintain a strong passion for your work.
- On Fridays, analyze and categorize your list of 30 contacts for the following week, focusing on customer profiles.
- Start the week off with a high volume of calls.
- Continuously monitor customer behavior and actions on LinkedIn.
- Show persistence in following up with potential customers.
- Focus on selling a 30-minute meeting rather than solely selling the product or solution.
- Target both implementation teams and CXOs for sales.
- Aim to make 120 calls per day to secure 2 to 4 meetings.
- Prioritize hiring individuals who are passionate in sales
- Explore reasons why a customer may not be interested when they express this sentiment.
- Make an effort to meet customers in person whenever possible.
- Create curiosity and intrigue to improve your sales efforts.
- Follow these seven essential guidelines for success.

Credentials Community Group “CCG” Hybrid Weekly Meeting

Session Convener: Kimberly Wilson Linson (Live) and Harrison Tang (via video)
Session Notes Taker(s):

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

Credentials Community group provides both education and broad community feedback to W3C working groups.

We want to help more folks feel comfortable contributing to the work and participating in work items. Proposing them and leading.

Because of the size and diversity of interests, CCG should serve as the intersection for other organizations to get feedback on their standard initiatives.

We need to curate more introductory education. And offer opportunities for “community” - leave opportunities for mentorship/buddies...maybe a session every month or two devoted to smaller group discussion.

Link to sign up for CCG membership: [Mission | W3C Credentials Community Group \(w3c-ccg.github.io\)](https://w3c-ccg.github.io)

Intro to KERI

Session Convener: Nuttawut Kongsuwan

Session Notes Taker(s): Catherine Nabbala

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

Link to the slides <http://bit.ly/keri-intro-iiw37>

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

KERI Why

- Most identity-related operations are idempotent. Hence, a double spending proof is not necessary for (most) identity systems. This is different from crypto currency systems where double spending proof is its primary requirement.
- KERI is a more scalable alternative to blockchain for building decentralised identity systems
- KERI is portable with or without blockchains
- KERI is recoverable from Quantum Attack

KERI What

- KERI is a variant of blockchain (i.e. having a has-chained data structure) that does not have a shared distributed consensus mechanism, i.e., no shared governance.
- KERI has local ordering of transactions, called key events, in contrast to global ordering of transactions in traditional blockchains
- Autonomic identifier (AID) is a persistent, self-certifying (self-authenticating) identifier
- The key state of an AID is determined by its Key Event Log (KEL)
- In KERI direct mode, KEL may be exchanged in a peer-to-peer manner
- In KERI indirect mode, KEL may be exchanged using key event witnesses. This is because a controller of an AID may not always be online, so the controller may designate witnesses that store and forward key events to any requestor.
- Witnesses can be hosted on different platforms e.g Digital Ocean, AWS.
- KERI
 - Key - asymmetric key cryptography
 - Event - a series of key events related to the management of Autonomic Identifiers (AIDs) using pre-rotation
 - Receipt - receipt of key event from validators and/or witnesses
 - Infrastructure - protocol for building decentralized identity systems

KERI How

- Demonstration of KERI command line interface (KLI) to perform key inception and key rotation of a KERI AID.
- Showed a KEL and revealed its hash-chained data structure

A Personal Digital Agent Standard

Session Convener: Adrian Gropper

Session Notes Taker(s): Adrian Gropper & Scott Mace

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

We want there not to be any lock-in, and allow self-hosting

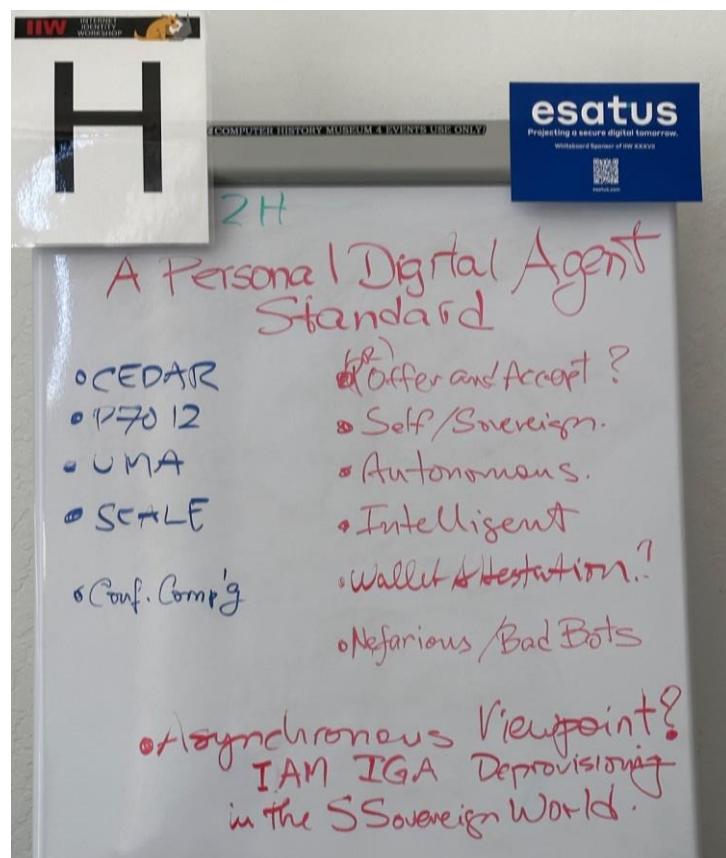
User concentric request model

Cloud-based agent and personal device agent may be very different; both are needed

Eve: aisle vs window – great example of personal sovereignty

IIW Presentation Slides

https://docs.google.com/presentation/d/1Myzb4SXBC43CtLSZ6wtX5Sn27FqhLS8FFqPm_s4Vnr8/edit



Best Practices for Recovering from Private Key Compromise?

Session Convener: Johannes Ernst

Session Notes Taker(s): in lieu of the note taker: Johannes Ernst

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

Somebody volunteered to take note for this session, but they weren't added here. From memory

Best practices:

- Have a higher-level authority re-certify a new key pair and have the old key pair revoked.
 - Lots of practical difficulties
 - Undesirable to have a hierarchy of authorities

KERI has pre-generated key pair, can it be used here? But: lots of complexity. Suitability for the open web unclear?

Johannes outlined a potential scheme called the Key Ratchet which he came up with ca 2006, where:

- instead of publishing a single public key key, N (like 10) public keys are published for N key pairs, which are ordered
- the active keypair is the first keypair; the operational system has access to the private key of the first key pair, no others, so those can't be compromised
- all other private keys are in cold storage ($N+1$ one total)
- kth public key is signed with $k+1$ st private key before publication, to create a chain. Last public key not published.
- when operational key pair is compromised, the recovered (or alternate) operational system starts using the second key pair
- when key pair $l > k$ is started to be used, it is a signal that all keypairs before l are now invalid.
- when ratcheting forward, new key pairs are generated and stored in cold storage as needed to keep N the same; new public keys are signed and published
- as attacker does not have access to private keys other than compromised first key, clients can unambiguously distinguish between the valid and the compromised system
- Will document publicly at <https://tech.dazzle.town/> one of these days

DIDComm 101

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

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

Alice and Bob send messages using DIDComm. Recipient might not have have a publicly viewable endpoint. Mediator helps with that. Mediator has to pass messages thru.



Demo DID (demo.didcomm.org):

```
did:peer:2.Vz6Mkh87R3WjTNiKVsDtzyQdatc7Kfp4J9ffQc9SreQuhEyNf.Ez6LShTdwrX8DqW8HyMya
KpBLPYvbRLjZx3NetF3p9YVkJpD.SeyJ0ljoiZG0iLCJzIjp7InVyaSI6ImRpZDpwZWVvOjluRXo2TFNqdF
BDbzFXTDhKSHppYm02aUxhSFU0NkVhaG9hajZCVkRlenVWclpYNIFaMS5WejZNa3RBU0VRSDZMNk
Y2OEt3UjQ1TWINSIFNQzF2djISb3RNcDhp3pGQ2ZLa3NaLINXM3NpZENJNkltUnRJaXdpY3IJNkItaDB
kSEJ6T2k4dlpHVjJMbu5zYjNWa2JXVmthV0YwYjNJdWFXNWthV05wYjNSbFkyZ3VhVzh2YldWemMy
Rm5aU0lzSW5JaU9sdGRMQ0poSWpwYkltUnBaR052YlcwdmRqSWIMQ0prYVdSamlyMXRMMkZwY
ORJN1pXNTJQWEptWXpFNUIsMTIMSHNpZENJNkltUnRJaXdpY3IJNkluZHpjem92TDNkekxtUmxkaTV
qYkc5MVpHMWxaR2xoZEc5eUxtbHVaR2xqYVc5MFpXTm9MbWx2TDNkekld2ljaUk2VzEwc0ltRWI
PbHNpWksa1kyOXRIUzkyTWIjc0ltUnBaR052YlcwdlIXbHdNanRsYm5ZOWNtWmpNVGtpWFgxZCIsI
mFjY2VwdCI6WyJkaWRjb21tL3Yll19fQ
```

Using this DID, Phil was able to create a connection from his browser (<https://demo.didcomm.org/#!/Phil>) to Sam. They both updated their names for the other and exchange messages.

Mediator is set up when Sam opens demo and the demo and mediator use a protocol to ensure Sam's DIDDoc has the correct info set up for the mediator.

Every DID contains enough information to establish a contact. This replaces the introduction protocol that was required in DIDComm V1.

DID rotation is built in to allow people to create a new DID for the relationship for every contact. DID is not registered anywhere. Both parties keep track of the changes on DIDDoc changes.

DIDComm gives you confidence that you're talking to the party who controls the DID. It doesn't give you any information about the other party that you can trust (like their name). Use VC's registries, or .well_known for that.

They picked this protocol to share names (user profile info): <https://didcomm.org/user-profile/1.0/>

Here's a good (canonical?) DIDComm reference: <https://book.didcomm.org/>
Bruce created an invitation for a pico (which supports DIDComm v2):

Sam, here is a one-time-use to try if you wish:

did:peer:2.Ez6LSdrcsVaiN7wMwk7BYTsL7MbMFCDGSBWGKzYadv6gL36JN3.Vz6MkhJKRt9fnt1eDDq9DpAqv9vn6KEC5A4qSoQswfUoaVyce.SeyJ0ljoizG0iLCJzljoiaHR0cHM6Ly9QTEFOLnBpY29sYWJzLmlvL3NreS9ldmVudC9jbG5rcGpwazIwaHVyemhwcmQ2dzg5c3IxL25vbmUvZGlkby9kaWRjb21tdjJfbWVzc2FnZSIslmEiOlsiZGlkY29tbS92MilslmRpZGNvbW0vYWlwMjtlbnY9cmZjNTg3II19

This extemporaneous demo failed but will be fixed.

Answers to “The Four Horsemen of SSI (Jeremy Grant Presso)

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

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

Not the official note-taker, but I posted a summary here:

<https://ericscouten.dev/2023/iiw/#session-2m-answers-to-the-four-horsemen-of-ssi>

A Business Person's Guide to Understanding IIW or The Burning Man of Digital Identity

Session Convener: Ken Ebert

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 #3

Open Wallet Update + Call for Projects

Session Convener: Tracy Kuhrt & Daniel Goldscheider / Lucy Yang & Kaliya
Session Notes Taker(s):

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

[Slide deck](#)

Group continued post-it exercise from day -1, Resources people could contribute; What is missing?

I could only attend part of the session. Notes from the part that I attended here:

<https://ericscouten.dev/2023/iiw/#session-3a-openwallet-foundation>

IIW 101 - User-Managed Access (UMA) - Get to know this unique “application of OAuth”

Session Convener: Eve Maler

Session Notes Taker(s): Eve Maler, Scott Mace

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

[Presentation PDF](#)

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

3B UMA 101

UMA adds control across party sharing.

An OAuth token enforces UMA

Consent legally requires manifestation, knowledge, and voluntariness. People are mostly the last one asked.

Digital consent has serious practical challenges achieving revocability, contract meeting of the minds, choice in relationship building, and consent seeker good faith.

UMA enables asynchronous permissioning that can include high-quality consent. It is a technology that can enable right-to-use technology...

UMA permissioning: user experience opportunities

One type of policy-setting experience

Benefits:

1. Choice in sharing with other parties
2. Convenient sharing/approval with no outside influence
3. Centralised monitoring and management
4. Control of who/what/how at a fine grain

Some known implementations

Benefits for service providers

1. True secure delegation; no password (or passkey) sharing
2. Scale permissioning through self-service
3. Resources accessed from distributed locations
4. Foster compliance through standards

Relationship-based health data sharing scenario

The Android & Web Identity API - Proposals

Session Convener: Lee Campbell and Sam Goto

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

OAuth for First-Party Apps

Session Convener: Jeff Corrigan

Session Notes Taker(s): Aaron Parecki

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

OAuth, Step-Up Authentication, First-Party, Mobile Apps

<https://datatracker.ietf.org/doc/html/draft-parecki-oauth-first-party-native-apps>

<https://github.com/aaronpk/oauth-first-party-apps>

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

Flow summary:

- Application collects information from the user, posts to the new “Authorization Challenge Endpoint”
- Happy path: that was enough, server returns an authorization code, can exchange for an access token

The new endpoint introduces a challenge-response mechanism

- If the credentials weren’t enough, the endpoint can return an error response indicating the client needs to collect more

Gluu - Janssen project

Has implemented the -00 draft in the server as well as a demo native app

Other mobile app considerations

- Which first-party app is this
- Metadata about the app? App, version
- Send app attestation information in the Dynamic Client Registration request

New document: “Best Practices for First-Party Native Apps”?

- Collect features and extensions of OAuth that give you the best properties of a first-party app with a real user login
- Use platform app attestation with Dynamic Client Registration to establish a public/private key
- Use private key JWT client authentication at all endpoints
- Use DPoP bound access tokens
- Use FIDO/WebAuthn for user authentication

In the spec, should the “device session” last beyond the acquisition of the authorization code?

Need some way to tie an authorization request to a previous session when using for example step-up.

Could use the “device session” as a long-lived credential, but then you would probably want it to be DPoP bound.

Currently in OAuth, we don’t have a way to say “I want to step up this existing session”. In the web environment the AS can use an existing web session, do we need an equivalent for mobile? Could reuse the device session for that, or could reuse the OpenID Native SSO secret, or could use an ID token. Still needs more investigation into this area.

Proof of presence vs step-up authentication. Some challenges from the RS may want to ask for a fresh FIDO proof. Naive implementation is to always prompt the user before every high risk API call. More complex implementation treats the FIDO proof with a variable time decay. The step-up authentication spec can still solve this, even though it’s not necessarily literally stepping up.

If you are concerned about app impersonation in your deployment, there are things you should do to protect against that, such as using app attestation at the dynamic client registration endpoint. Some deployments don’t care about app impersonation, but might still want to use the direct authentication mechanism defined in the draft.

did:webs for muggles

Session Convener: Markus Sabadello & Lance Byrd

Session Notes Taker(s):

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

See here:

<https://docs.google.com/presentation/d/1BC9y4YvLPwOJwnwpwl8puJYwJHUONL0vLITxOCOK8FY/>

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

Verifiable Presentation with Message

Session Convener: Kazue Sako and Ken Watanabe
Session Notes Taker(s): Jin Wen

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

Slides of the presentation

<https://sako-lab.jp/slides/iiw37-VerifiablePresentationWithMessage.pdf>

Slide deck From Waseda Univ. Sako Laboratory

POSTER: Using Verifiable Credentials for Authentication of UAVs in Logistics

https://link.springer.com/chapter/10.1007/978-3-031-41181-6_45

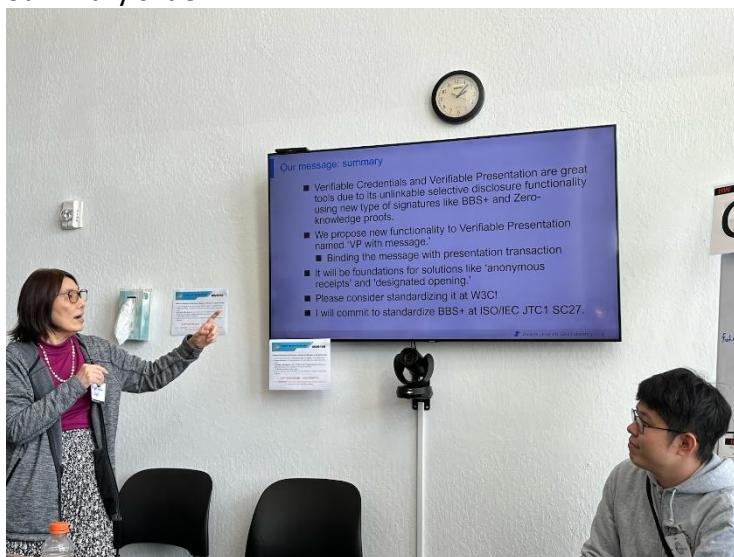
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Terms used: Zero Knowledge Proof, BBS+ signature

background info: <https://github.com/mattrglobal/bbs-signatures>

The key idea of this session to choose BBS+ vs. SD-JWT is SD-JWT can not create unlinkable proof

Summary slide:



discusses a new functionality called "verifiable presentation with message" in the context of unlinkable selective disclosure using new types of signatures like VBSS and zero-logics. Key understandings, outstanding questions, observations, and action items include:

Key Understandings:

- The new functionality allows for verifying a presentation transaction while also receiving a message from the authenticated party.
- This can be used for anonymous receipt and designated opening, allowing for more complex use cases.
- The proposed functionality aims to standardize the order of receipt and enrich the use case of verifiable presentations.

Outstanding Questions:

- How does the proposed functionality compare to existing standards like JWT and derived verifiable presentations?
- Are there any limitations or restrictions with the use of BBS+ signatures in this context?

Observations:

- The use case presented involves drones in a logistics scenario, where verifiable credentials are used to authenticate the drones and ensure they are working under the same contract.
- The implementation uses Hyperledger Ursula and Mattr Global J-Sign and Signatures libraries.

Action Items & Next Steps:

- Consider standardizing the proposed functionality and integrating it with existing standards.
- Explore the use of more generic JWT format for this purpose.
- Investigate the potential for randomizable encrypted claims to prevent linkability.
- Attach the slide deck to the post for further reference.

The discussion highlights the potential benefits of unlinkable selective disclosure and the need for further exploration and standardization of the proposed functionality.

Grounding Identity in Truth

Session Convener: Shane Oren
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

DIF Credential Trust Establishment - Practical Governance / Sam Curren

Session Convener: Sam Curren
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

BCGov Offers \$CDN100k: Adding Support for W3C Format VCs to AnonCreds v1.0

Session Convener: Stephen Curran
Session Notes Taker(s): Kevin Griffin

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

Presentation: <https://bit.ly/AnonCredsCWU> — contains all the links to the Code WIth Us opportunities listed below.

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

AnonCreds are a format of VC. AnonCreds encompasses the issue/present/verify triad, w3c is just_ the data model.

You can use predicates to determine the information shared during presentation

AnonCreds predates the W3C VCDM and currently does not match the spec.
The goal is to match the VCDM 1.1 (2.0 isn't final)

Turns out its easy to get AnonCreds to conform by moving the data around from AnonCreds, into W3C VCDM 1.1

BC Gov is interested in AnonCreds for its privacy preserving characteristics.

Stephen shows large chunk of JSON

AnonCred field -> w3c field
cred_def_id -> issuer
schema_id -> credentialSchema.type/schema/definition
values.name.raw -> credentialSubject.name
signature -> proof

Utilises an additional context and @vocab (notably controversial)

Using vocab to avoid having to define what's in credentialSubject.
In the future use the context to define what is in credentialSubject.

Given w3c vcdm supports multiple proofs, you could use an AnonCreds one in conjunction with a NIST approved one... that might be valuable

Limitation you can put AnonCreds schema into/json-ld format but not the other way around (flat claims list in anon creds)

Claims are encoded as integers in anon creds as they have always done

Not supporting credentialStatus2020

IssuanceDate is required in w3c vcdm and not in Anon Creds!

FlexCreds via multiple signature schemes

“[Code with Us](#)” is a procurement program to allow folks to contribute to open source projects (with money)

Three programs each 35,000 \$CDN

AnonCreds Rust update implementation to transform anon creds into w3c, including wrappers
python/js

- \$5k design
- \$25k impl
- \$5k demo

[Apply here](#) - open until October 20, 2023

AnonCreds in W3C format in Aries Cloud Agent Python

- \$5k Design
- \$30k impl

[Apply here](#) - open until October 20, 2023

Enabling support for multiple proofs on a single credential will be the interesting part...

AnonCreds in W3C format Aries Framework JS and Aries Bifold

- \$5k Design
- \$30k impl

[Apply here](#) - open until October 20, 2023

[BC Gov Digital Marketplace](#)... click the link to apply

SESSION #4

Introduction to Trust Over IP Foundation (ToIP)

Session Convener: Judith Fleenor, Executive Director, Trust Over IP Foundation

Session Notes Taker(s): Judith

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

<https://trustoverip.org/permalink/Intro-to-ToIP-Deck-IIW-Fall-2023.pdf>

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

The [Trust Over IP Foundation](#), a Joint Development Foundation project within the Linux Foundation. We are an international collaborative community with over 500 individual and corporate members.

Our mission “to provide a robust, set of common standard and complete architecture for internet-scale digital trust.” It is a simple mission, but not at all easy and that’s why it takes a collaborative community to get it right.

Together our members are creating specifications, recommendations, whitepapers and guides to assist governments and organizations embarking on the creation of interoperable trust frameworks at scale.

The hallmark of our organization is the ToIP is the ToIP Dual Stack, with the Technical Stack paired with the equally, if not more important stack, the Governance Stack. Please look at the [slide deck](#) for images of the stack, and description of our work items.

Introductory and Foundational Documents

- [Trust Over IP Foundation White Paper V2.0 \(PDF\)](#)
The history of trust, the new era that’s upon us, and an overview of the Trust Over IP stack that supports its implementation.
- [Design Principles for the ToIP Stack V1.0 \(PDF\)](#)
This paper recommends the 17 core design principles for the design and development of the ToIP stack, including computer network design principles, “human network” trust principles, and general design principles.

The ToIP Foundation produces a wide range of tools and specifications, organized into five categories:

- Specifications to be implemented in code
- Glossaries to be incorporated in other documents

- Recommendations to be followed in practice
- Guides to be executed in operation
- White Papers to assist in decision making

Great Session

TOIP standards and frameworks should be implemented to The Current market in bringing about the transformation and interoperability at scale and well in time.

IIW 101 - Web AuthN

Session Convener: John Bradley

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

Credential vs Wallet Selection

Session Convener: Tim Cappalli / Sam Goto

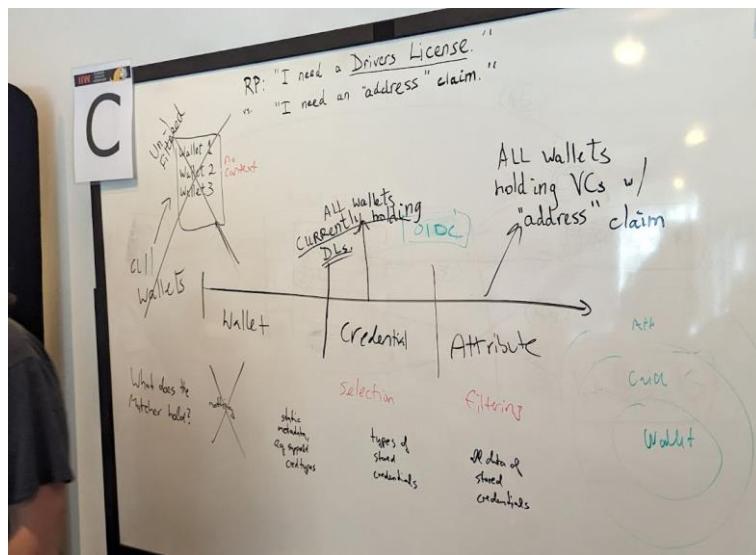
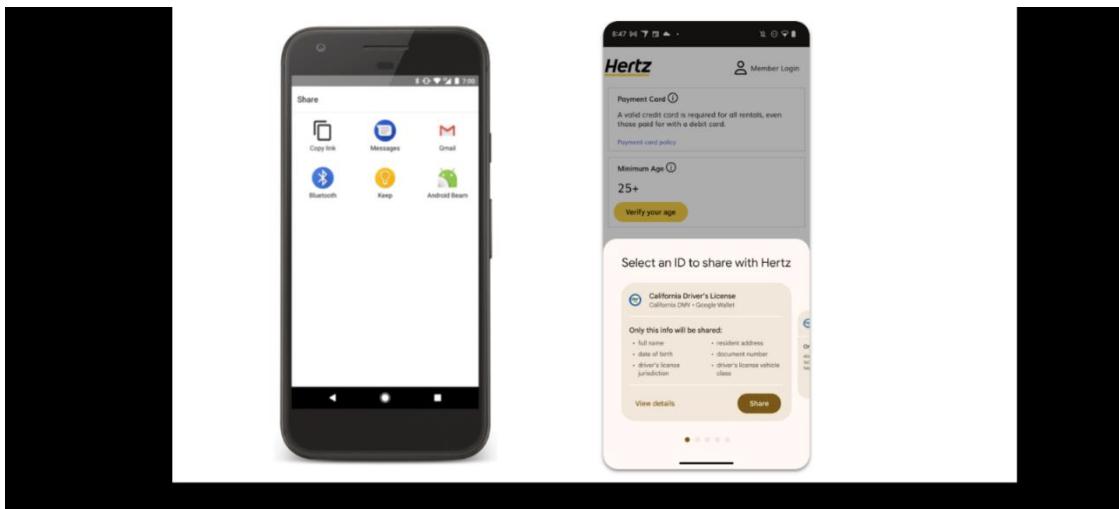
Session Notes Taker(s): Tim Cappalli

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

<https://github.com/wicg/identity-credential>

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

The goal of this session was to continue a discussion from an earlier intro session and also previous IIWs. - Google showed some of their incubation work in Chrome and Android, and explained how their selection UI was rendered, which party is responsible for each component, and how existing protocols could run over the



UX Challenge for SSI

Session Convener: Gabriel Chartier
Session Notes Taker(s): Jin Wen

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

round table introduction of UX related issue:
bridge the gap of familiarity and the technical details behind the scene
list of problem areas:

- key management
- password manager

Foundation of cryptography authentication

shared by Sukhi Chuhan (Senior UX Designer at Ontario government)
user research on digital wallets
what if government giving you a digital wallet
mental model: for most of the people, physical world use case is the starting point

Familiarity is the key
content message is important: instead of biometric authentication, use Face ID.

End to end experience coming from end user

Online experience

Accessibility concern: do not tie a particular device to a particular



Issues raised:

- Onboarding and education
- Balance between security and ease of use

Moderator Q: Who has solved a serious UX challenge already?

One answer: "If you get the UX right for a new technology, it will not be adopted." Hmm.

Sukhi Chuhan (Senior UX Designer at Ontario government): Expectation is that VCs for end users needs to be about ease of use. Make it more and more like what you can do with physical IDs.

If you're creating a new digital wallet product, you are competing with free and built-in from Apple and Google.

Terminology has a big impact. Example: "biometric authentication" scares users, but "Touch ID" and "Face ID" don't.

Remember accessibility. For example, people with impaired vision can't really use QR codes. Also, some people with disabilities and also children may have caregivers or guardians who need to be able to act on their behalf.

Most users will pick utility over sovereignty any day.

Some resistance to using platform-provided wallets due to perception of security concerns and hackability.

Audience Q: How do you present VCs in a way that's digestible?

BC wallet specifically avoids showing information on screen. They want to force the info to be transmitted digitally and displayed on the *verifier's* device, not the holder's device. On-screen display is easily faked by the credential holder.

source: <https://ericscouten.dev/2023/iiw/#session-4e-how-are-you-solving-for-the-ux-challenges-of-ssi>

SOLID

Session Convener: Doc Searls & Hadrian Zbarcea
Session Notes Taker(s):

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

#IntentionEconomy, #SolidProject, #ProjectVRM, #LinkedData, #DecentralizedWeb

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

Doc introduced the motivation behind the Intention Economy and shared that Sir Tim Berners-Lee's [Solid Project](#) was in part inspired by his book. Doc mentioned how consumers can create marketplaces and actually inform merchants unequivocally about their needs and wants via intentcasting, the alternative to advertising that goes in the other direction.

Hadrian made the case that the technology to implement the Intention Economy already exists. The Solid Project and W3C standard created by @TimBL provides ideal technological infrastructure for storing data, giving agency to consumers as owners of their data and providing a universal API to access data, a consent based sharing mechanism and the basis for a layered services infrastructure for the Intention Economy.

The conversation touched on Identity, data portability, and the need for Solid Pod hosting providers. At scale, interoperability, and hence governance, is required, so the alternatives were explored. At scale, however, it is clear that only a federated model would work and why polycentric governance is needed.

One important aspect of Solid is that it decouples identities from storage from applications. Hadrian emphasised that this creates a fundamental opportunity for application developers. First, because data is already present/stored in Solid Pods, therefore in many cases a backend is not needed (the Pod is the backend). This makes application development faster and cheaper, reducing risks and development cycles. In addition to that, it favours a style where applications are smaller and feature oriented due to the use of Linked Data, further reducing costs and risks.

The presentation concluded with a call to action to use Solid Pods as data stores, a technology that provides agency to users as data owners. One idea was to integrate [Picos](#) with Pods, and we hope to demonstrate that at the next IIW.

Privacy as Alignment of Expectations

Session Convener: Joe Andrieu

Session Notes Taker(s):

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

Note prepared by: Michael Becker (notes in Markdown, use a markdown reader to render)

****Privacy is an Alignment of Expectations****

_ [Joe Andrieu](<https://www.linkedin.com/in/joe-andrieu-a0528/>)_

Developed with [Scott David](<https://www.linkedin.com/in/scott-david/>), linked to functional identity.

..

Hold loose violated my privacy...

Violating my privacy by creating a situation of potential future harm.

The Framework

**** The Framework**:** Privacy is an alignment§, in a context, of expectations (of constraints) about how you are recognized, remembered, and responded (and redistributed).

_ Old element of framework [for information about me and shared with me]_

_ This is first framework that links privacy to and identity: The "verbs" in the framework can be operationalized as a framework that can lead to the development and policy, including safe harbor._

-

^ Contextual boundary

- could include third-party
- has a time element
- spatial dimension
- temporal intentional
- Generational shift

§ Alignment links to:

- * Governance (how we agree to align on a particular context)
- * policy
- * Regulations

About exceptions

There is no one expectation

The expectations can be,

- * formal and informal
- * Static or dynamic
- * Decreed or negotiated or mandated

Discussion

Privacy is about setting up a boundary as an indicator of privacy...But this does not work, is it fake "control"...people may choose to not respond to boundaries.

"Barriers are indicators" as a substitute for control.

"Locks don't keep thieves out; they keep honest or incapacitated people honest."

"Unless there is someone that is willing to be at risk, then you have no security. People need to put themselves in harm."

"You can never guarantee that is secure. You can put in measures to make breaking those measures more expensive than what's its worth."

"Privacy are element of being safe."

How does this address the ransomware problem?

- * This gives options to help the organization, but it does not address the power balance.

"Privacy is an end, not a means." The Francis is not privacy; it is a signal that I'm trying to achieve privacy.

"Privacy is the feeling that you have about safety or security."

"Privacy and security leads to a sense of safety."

Need debate: which is more important freedom or safety

"Privacy is something you can ask for and given or refuse to you."

Reversing the assumption that privacy is about control...it is not, it is about a "request."

How you respond to me could violate my rights because of my identity (e.g., if you share my race).

What you do with the data matter just as much as the data.

NOTE: Data is NOT in the operation. It is not about the data itself.

"You don't need technology to get alignment."

"If you have rules then you have understanding," similar to

Data can be used in harmfully, even though I feel safe.

"There is a difference between feeling safe and actually being safe."

LinkedIn example: an economic barrier to your privacy. People have looked at my profile.

The powerful don't need privacy because they have power. Privacy is about protection the disenfranchised.

Roosevelt on Four Freedoms

- * of speech
- * of religion
- * from want
- * from fear

"Debates over privacy are really debates about how power will be allocated in an information society and how much power the humans in that society will get as consumers or citizens" --Neil Richards, author of Why Privacy Matters

"Privacy is a social good." If you don't share at all, you're a hermit.

"When you disclose information to a person or group, you choose what to disclose, with the rule. If you release the information, this creates boundary turbulence. It influences privacy."

"In the digital world, there is not implied or tacit, it is all explicit. In digital we don't have tacit queues."

"What if the problem is not about solving privacy, it is about empowering people?"

"Ability to be yourself in your own mind is fundamental to you being human."

Key consideration is "retroactive retrospective."

Privacy in Medieval England.

Is having privacy the lack of privacy violations?

Mis-alignment of expectations

People really don't understand what it means to share.

Terms

* Privacy

* Boundaries

* Boundary Turbulence

References

- * [**Book**: Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse By Elizabeth M. Renieris(<https://mitpress.mit.edu/9780262047821/beyond-data/>)
- * [**Task Force** IEEE 7012 Standard for Machine Readable Personal Privacy Terms](<https://standards.ieee.org/ieee/7012/7192/>)
- * [Chatham house Rule](https://en.wikipedia.org/wiki/Chatham_House_Rule).
- * [Why Privacy Matters](<https://www.amazon.com/Why-Privacy-Matters-Neil-Richards>)
- * [FDR and the Four Freedoms Speech](<https://www.fdrlibrary.org/four-freedoms>)
- * [Is Modern Privacy Better than Medieval Privacy?](<https://richardrabil.com/2018/09/08/is-modern-privacy-better-than-medieval-privacy/>)
- * [Book: It's Complicated: The Social Lives of Networked Teens](<https://www.amazon.com/Its-Complicated-Social-Lives-Networked/dp/0300166311>)
- * [Privacy in Colonial New England 1630-1776](<https://www.amazon.com/Privacy-Colonial-New-England-1630-1776/dp/0813903394>)
- * [Conceptualizing Privacy](https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2086&context=faculty_publications)

Can We Solve a Problem in an Hour? Speed Proof of Concept

Session Convener: Rex Peacock

Session Notes Taker(s): Jesus Torres

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

1st concept: giving a VC can we do a quick way of how it should be displayed.

We looked at a few standards for json forms

json forms Retool json ui schemas

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

We began walking through a simple implementation.

Given an example (#1) credential from <https://www.w3.org/TR/vc-data-model/>, we tried to represent it using the JSON Forms ui schema by converting it manually, after some quick research to find a more appropriate format. The partial resulting schema we ended up with was this:

```
{
  "schema": {
    "type": "object",
    "properties": {
      "id": {
        "type": "string"
      }
    }
  }
}
```

```

"properties": {
    "id": {
        "type": "string",
        "title": "id"
    },
    "type": {
        "type": "string",
        "enum": ["VerifiableCredential", "AlumniCredential"]
    },
    "issuer": {
        "type": "string",
        "title": "issuer"
    },
    "issuanceDate": {
        "type": "string",
        "format": "date",
        "title": "issuanceDate"
    },
    "credentialSubject": {
        "type": "object",
        "properties": {
            "id": {
                "type": "string",
                "title": "id"
            }
        },
        "alumniOf": {
            "type": "object",
            "properties": {
                "id": {
                    "type": "string",
                    "title": "id"
                }
            }
        }
    }
},
"data": {
    "id": "http://example.edu/credentials/3732",
    "type": "AlumniCredential",
    "issuer": "https://example.edu/issuers/14",
    "issuanceDate": "2010-01-01T19:23:24Z"
}
}

```

The output form could display the data, and when combined with a UI schema, it could create a more complex UI. However...

Conclusion

Unsurprisingly, the JSON form schema is best suited to generating forms, and is not as useful at representing already generated data. While other strategies like HTML and Markdown could be applicable, they have their own security challenges and also aren't able to solve for the general challenge of grouping inputs representing verifiable credentials in a visually pleasing way.

Confidential Computing Changes Everything - Enabling a Universal Name System (UNS) and Universal Certificate Authority

Session Convener: Manu Fontaine

Session Notes Taker(s): Charles Lanahan

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

Universal Name System, TEE, Secure Enclaves, Universal CA, Universal Data Protection Repo, HushMesh Inc. Link to slides:

<https://drive.google.com/file/d/1f3NDrbuukNZHbUwbUUH9ymxeddiYg8Q4/view?usp=sharing>

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

Motivation for the Project - “Digital Piece of Mind”

The root vectors of security issues on the Internet were identified by the speaker as:

1. Insiders (employees at the CAs, DNS maintainers, Federation maintainers, etc...)
2. Weak relational links among entities on the Internet

Thus the solution (*paraphrased by the notetaker*),

1. Take out people from the infrastructure of trust
2. Use secure enclaves and careful governance to create very strong relational links among these entities.

First step: Creating a Universal Naming Scheme

As the URL/URI is **domain/path/resource**

The *Universal Naming System (UNS)* is **stemID#context#key_name** where the “#” sign denotes an HMAC function deriving new key expansions from entropy in the stemID.

The speaker notes that this scheme can be used to:

1. Derive keys as expressed
2. Symmetrically sign using such derivations
3. As well as be extended recursively to create infinite keys in the self contained manner.

stemIDs in this scheme are currently defined to be:

1. True random (as supported by secure enclave entropy construction?)
2. 256-bit
3. identifiers
4. that are also keys

Confidential Computing

The scheme relies on the secure elements and enclaves and putting total trust in these devices. The presenter asserts that doing so will allow us to protect data in use while also enabling verification in an environment that can't be replicated without these devices. He believes that in the future there will be no identity on the Internet without these mandated devices providing the backbone security.

Trust scheme

Trust Scheme relies on trustees.

Trustee <-> Trustee

Alice <-> Her Agent <-^> His Agent <-> Bob

A name is picked by Alice, is hashed into the UNS scheme described before, and then propagated through the Trustee network to Bob. The Trustees prevent mitm attacks by expanding this network of agents and trustees. The trustees can't see anything other than the hashes via this propagation.

UNS + UCA + UDPR chains of custody make it so that security is asserted to be universal over the scheme.

Note: The speaker asserts here that the stemID isn't actually in control of the user's agent but is in control of the trustee with which they interact. This confused me (the notetaker) but I forgot to follow up on it so I never quite figured out if this was an issue or not.

They Hushmesh need help with creation of governance for Trustees if anyone is looking to partner.

No humans involved in UNS scheme. No trustees can actually see any data flowing over the network.

Right now they have a openid connection IP and a set of REST apis for cell storage, personal crypt, mesh fact anth, transactions.

did:PLC: 1,000,000 uses app

Session Convener: Aaron Goldman
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

KERI for Dummies

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

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

Shout out Sam Smith!

The main concepts of what and why, but not the how

What is KERI, why do we need it?

Basic Idea...

With KERI we envisioned a future state where everybody can sign and verify people, orgs and things can digitally sign anything they deem important.

We don't need a blockchain, we need a protocol for verifying a piece of data, we don't have to trust a 3rd party or a blockchain.

If we can have an open protocol for "sign my stuff" "let me verify your stuff"

1st characteristic _completely decentralized_

Am I self sovereign if I can sign and verify anything?

In the world of digital identity its about consistency of control.

We're represented by consistency of control.

KERI is about consistency of control (of an identifier derived from private keys), but the point is consistency of control is how we prove who we are.

Even with a passport, you're proving control of a physical artifact and your biometrics, correlates control.

Question, how do I know "Phil" sent me a request for 1000\$.

What will give me the assurance that Phil sent me that request.

How about a message digitally signed by keys controlled by Phil, we have a pre-existing relationship, I might trust that.

Comparison:

Phone numbers are hidden behind a "contact" why can't the same be applied to an identifier?

Side bar:

Apple M1 chips inherit a set of private keys so that everything signed by the device is never in question.

People and things need to create their own keys, they can't be "given" to you.

You still need to trust the "thing" being used to create your keys, but easier if it's a device you control, vs the cloud (someone else's computer) we're worried about non-repudiation

For early adopters to do things like password managers, we're so close to making private keys, right now we're just doing passwords.

PKI has been around a long time, but how do I know I have the right public key at the moment I need to verify something.

currently solved by CA lists in browsers and we trust the people who put them there

Ref to a hacked CA, (I missed the name sorry...)

The promise of KERI is that it solves the problem of knowing you have the right key state at the moment you want to verify it. KERI protocol _through magic_ allows me to publish my public keys via Key Event Log (Hash chained data structure (yes, you can call it a mini blockchain)).

KERI enables you to publish them via witnesses (publishing them makes things duplicity/tamper evident)

Question;

What if I want more keys for a given identifier?

In KERI you can use a "rotation" event to add more keys/change algorithms (not a dummy question :)

KERI super power: pre rotation

When you incept an identifier you create two sets of keys, your current signing keys and a cryptographic binding (hash) to my future keys. (Forward cryptographic commitment).

Now it's trivial to rotate to new keys.

When you make a commitment to a future key set the blake3 hash is quantum proof.

If a quantum attack comes along and breaks my current signing key, I can rotate to my next key.

How do you do consistency of KELs?

Witnesses provided a mechanism to achieve this since you included them when you incept or rotate to.

Adoption is cat videos.

The End.

Externalized Authorization

Session Convener: Omri Gazitt

Session Notes Taker(s): Omri Gazitt (post facto) - others welcome!

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

Presentation slide [deck](#)

AuthZEN WG [listserv](#), OIDF charter proposal slide [deck](#)

Topaz OSS [project](#)

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

“Externalizing authorization” boils down to a few principles:

- purpose-built authz service
- fine-grained access, principle of least privilege
- policy-based access, separation of concerns
- real-time access checks
- comprehensive monitoring, centralized logs

Discussion and feedback during the session:

- Embedding scopes in access tokens isn't necessarily an “anti pattern” - it can compose with externalized authorization as a pattern. The problem is when you use it for a purpose it wasn't designed for (fine-grained access)

- The “Zanzibar” data model really feels like a re-hash of the ACL model (even before we had RBAC). [OG: it’s a reasonably elegant synthesis of RBAC and ACLs, where permissions are inherited through the graph of subject/object relationships)
- Alan Karp: what you describe suffers from the “Confused deputy problem”
- Mark: you need both policy and data
- Getting data to the authorizer is indeed one of the “hard problems”
- Practical issue with ABAC systems: standardizing what the attributes mean is hard. E.g. in one effort, out of hundreds of attributes, only 13 were standardized
- Capturing and aggregating decision logs is a hugely important (and often overlooked) aspect of authorization - it is invaluable for compliance and forensics
- AuthZEN WG focused on standardizing the message exchange patterns between PEPs and PDPs - how to observe / track the work?
- Policy composition (and standard building blocks?)

Brainstorm: How SSI can solve the Data Exchange Problems for Healthcare ? (KERI / vLEI / SCDC)

Session Convener: Jared Jeffery

Session Notes Taker(s): Sophia Goeppinger

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

HC's cybersecurity problem: Cannot solve the massive amount of breaches no matter where they go

- There is a lot of money to be had in the data they transfer back and forth (3-8x for what a credit card goes on in the market): social security, weight, age, payment methods, health records → Hackers take that (e.g., set up fake clinics to send all that information to CMS to be reimbursed and pretend theses are all their patients)
- They don't tackle the root problem: **Broken identity structure** (we are only as secure as the weakest link in the data supply chain):
 - The data supply chain is long in healthcare: From the origination (clinical set up where you go to put in your information, e.g., payment model, etc.) → Provider (health system) → Payer, drugs, etc.) → all pieces represent an attack surface to get back to the treasure troth, i.e., the EHR system
 - When an attack happens, these stakeholders only have to pay the fine, but the CIO does not get fired because he just did everything up to the industry standards
 - BUT the problem is getting worse so that it can no longer be seen as a cost of business

- They have a donor-acquired infection: Obama doctrine pushed the industry into the digital era → **Problem:** acquired the infection of insecure digital ID: They don't have the ability to identify and authenticate the organizations they are dealing with and the patients in their care (business policy and law) → The data must flow anyway; now it's about how can we make sure that it's secure

What's broken:

- HC lives in a “when, not if,” world of security incidents. Cyber insurers are backing out of the industry
- Most health systems don't understand their 3rd party data exchange landscape
- Current solutions are either insecure or code-heavy, cost-prohibitive, and non-portable

💡 The future we should work toward: Health data that's **easy to share** and **impossible to hack** → HC only focuses on Nr. 1 but not Nr. 2

Why is HC data stolen:

- Comprehensive nature of the record: A lot of financial information is contained in the medical record and other valuable stuff → If you get a medical record, you get the whole person
- Being able to access other revenue sources: Set up fake clinics and go to CMS to want to get paid for the service they allegedly did but really didn't

Health data matters because it is a direct link to life

What makes cybersecurity in HC so special? It is not just the only high-value data industry (banking, shopping history on Amazon, etc.)

→ Why are the cybersecurity solutions specific to HC?

- Whatever solution needs to fit industry expectations (where they are at, what tech stack they have) and regulations (build to standards, e.g., FHIR), i.e., what they will accept
- HC in the US costs twice as much and has more disparity than in any other; everything that happens in HC is driven by the mantra of avoiding transparency → Leads to problem with HC adopting best practices → Waste! (and someone's waste is someone's bottom line) → We live in a data economy (healthcare is part of that)

The solution to this problem: Path of adoption of best practices; need a better way to do the data exchange

- Need to sell it to the under-tier of players in the space
- Allow someone outside of the waste to get their spoon in the firehose because they don't get any of the 4 trillion today (it's not coming from the inside!), e.g., Amazon, Apple, etc. - 4 trillion dollar mafia → Don't take the infrastructure that is there as a given
- Establish solid **organizational identity** between these groups:
 - Get KERI as a standard implemented into TEFCA workforce
 - Business case:

- Reduce their risk
- More security

→ Solution can be applied to many other sectors

Problem with HC: Data needs to move through many parties (not just A to B and that's it)

HC has an extreme delegation problem: Hard to introduce system that have accountability and allow the flexibility of delegation that is required to run a hospital/medical practice → Much of what the SSI world has done in this context is ignored delegation as fundamental component of the solution

Ease of sharing: HC is excited about blockchain but they don't really know what they are talking about

Adoption falters when you need to get everyone on the chain → Non-starter for the industry (how to not need everyone sharing in the governance of the data and the structure): They don't want to share governance → How to leverage the technology we have to get to the data exchange

HIE

- Always institutional focus
- Patient matching problem → Only in the US
- How to move the data around without individual consent: Move data with the transparency and interaction with the individual (then no patient matching issue) like Apple Health, e-commerce, financial system
→ But mafia doesn't want to move to that and there is no regulation to drive them into that direction (that is exceptional about healthcare)
- Introducing in this Byzantine system a blockchain method or standardization risks introducing **transparency**
 - Transparency amongst competitors
 - Transparency to the policymakers (unions)

→ Would need sophisticated ZKPs on top of blockchain → Transparency is a problem → Go peer-to-peer on transaction instead of across the entire chain BUT then you have a **severe delegation problem** as there are so many intermediaries (you don't know how to address the other side, end-to-end?) (how do you make this work?)

Nature of intermediaries

- Data brokers (not involved in clinical care) → Could get rid of them → Show up in all three areas
- Aggregate data because they want to have a snapshot in time instead of getting it on-demand (business reasons or research) → Store it
- Master data indexes: Aggregate identity data for the purpose of patient matching in the probabilistic environment
- And others

→ Sometimes intermediaries need themselves; they just insert themselves in the data exchange

If you move data on demand you need

QHINs role in TEFCA: Sign a reciprocal agreement: in order to belong in TEFCA/other HIE models before it they have to (a) identify the patient (deal with the patient matching problem); (b) given a particular patient whether any of their service providers have data about this particular patient to respond to the broadcast query

HIPAA doesn't allow you to use data for research without patient consent

Memory-Based Private Keys! Enforcing Entropy Using AI!!! OMG!

Session Convener: Matthew Vogel

Session Notes Taker(s):

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

AI, Private key, entropy

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

Topic: The fusion of memory-based private keys and the application of AI to enforce and enhance entropy.

Summary: Today's discussion unveiled an innovative approach to security, centering on memory-based private keys. The core idea rests on the belief that individual memories hold inherent uniqueness, and when used as a basis for private keys, can provide a deeply personal and secure authentication method. To further fortify this method, the proposal of employing AI to enforce and heighten the entropy of these memory hints was introduced. Such AI-driven augmentation ensures that the private keys derived are not only individualistic but also adhere to the highest standards of cryptographic security. The assembly's response to this proposition was overwhelmingly positive. The blending of personal experiences with AI-optimized entropy signifies a groundbreaking stride in creating secure systems that resonate on a personal level with users. Given the potential of this integration to redefine personal security paradigms, there was unanimous agreement on its pursuit and further exploration. This venture into intertwining human memories with advanced technological security mechanisms promises an exciting trajectory toward the future of authentication.

SESSION #5

ToIP Trust Spanning Protocol for Muggles

Session Convener: Drummond Reed, Wenjing Chiu, and Sam Smith

Session Notes Taker(s): Jin Wen

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

<https://trustoverip.org>

<https://trustoverip.org/blog/2023/08/31/mid-year-progress-report-on-the-toip-trust-spanning-protocol/>

PUBLIC LINK to the ToIP Trust Spanning Protocol for Muggles slide deck used for this session:

[https://docs.google.com/presentation/d/1dgaTwxRubnpj7M83840mz53_ijfwEkajndrBBEQthgU/e
dit?usp=sharing](https://docs.google.com/presentation/d/1dgaTwxRubnpj7M83840mz53_ijfwEkajndrBBEQthgU/edit?usp=sharing)

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

This is about the Layer 2 of peer-to-peer communication

Format

First, background from Wenjing and Sam

Then 7 minutes for each of the 7 concepts listed in the link above

1. Verifiable Identifiers
2. End-to-End Authenticity and Confidentiality
3. Direct Connections (Inner and Outer Channels)
4. Routing Via Intermediaries (Routing Channels)
5. Relationship Context Channels
6. Text and Binary Encoding
7. Trust Task Protocol Framework

#1 Verifiable Identifiers

Traditional ip stack shown (hourglass design): highlighting IP address as the thinnest layer “the waist” of the hourglass model.

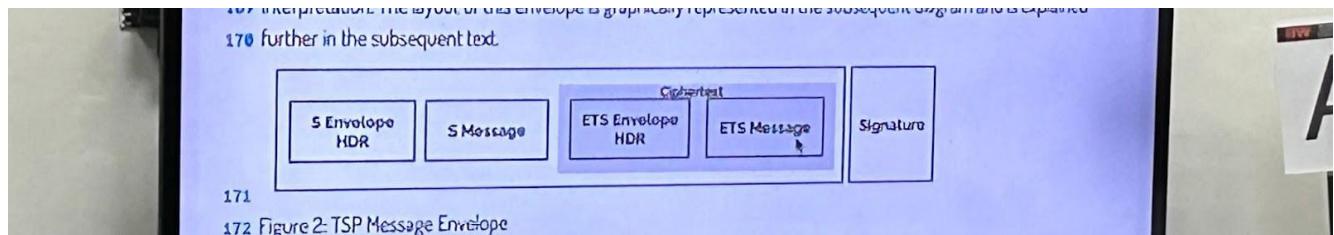
VIDs are the “waist” of the Trust spanning protocol.

Verifiable Identifier (VID) is a DID, became a W3C standard in 2022

VIDs are an even broader category than DIDs, the most specific being Autonomic IDentifiers (KERI AIDs)

Benefits: with VIDs, every single communication is cryptographically verifiable

Trust Spanning Protocol (TSP?) messages are structured following “ESSR” (Encrypt Sender, Sign Receiver) pattern.



The bottom line: by binding the sender's public key inside the encrypted ciphertext and binding the receiver's public key in the enclosing signed plain text, an adversary is prevented from forging messages that compromise either authenticity or confidentiality. So the trust spanning protocol can achieve both strong authenticity and strong confidentiality by applying ESSR to all messages that require both properties. (<https://trustoverip.org/blog/2023/08/31/mid-year-progress-report-on-the-toip-trust-spanning-protocol/>)

correlation privacy concept



Figure 1: A direct connection showing one ToIP channel tunneled inside another for partial correlation privacy.

In Figure 1, the VID labels A_0 and B_0 are publicly-observable VID labels used to form the outer channel (shown in red). They are outside the two endpoint boxes because they are publicly observable on the Internet. The VID labels A_1 and B_1 are private interaction VID labels that form the inner channel (shown in orange). They are inside the two endpoint boxes because they are completely private to A and B. Each ToIP message between A_1 and B_1 is carried in the encrypted payload of ToIP messages between A_0 and B_0 , so A_1 and B_1 are never exposed publicly on the Internet.

#4: ROUTING VIA INTERMEDIARIES (ROUTING CHANNELS)

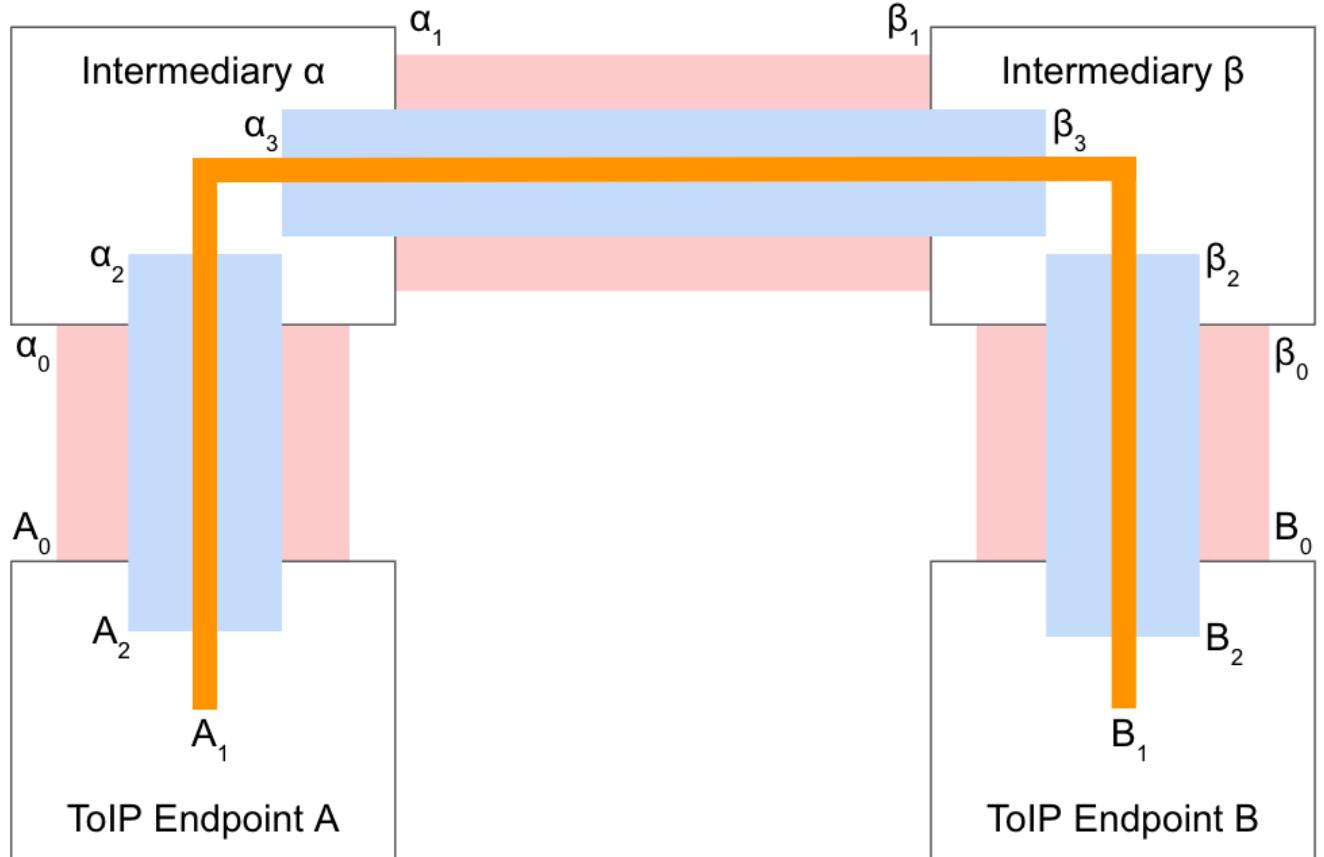


Figure 2: Adding a routing layer tunneled via intermediaries for stronger correlation privacy

In this configuration, both A and B first establish outer channels over direct connections with their respective intermediaries α and β (shown in red between VIDs A_0 and α_0 , and B_0 and β_0 respectively). Then A and B tunnel another ESSR protocol (shown in blue) inside the outer channel to send ToIP routing messages. This routing channel gives the intermediaries α and β just enough information to pass the messages to the next hop on the path. The full path is never revealed to any single intermediary; all α and β know is the next destination.

The inner channel (orange) is layered within the routing channel (blue). As with direct connections, this is the fully private interaction channel between A_1 and B_1 . Neither α or β know about A_1 and B_1 , and cannot see any of the communications on this inner channel. To use a physics analogy, this inner channel has two layers of “insulation” that prevent the *heat* (private information) from leaking out into the *environment* (third parties observing the outer channel).

This routing architecture is not limited to two intermediaries; it can scale to more as needed. However adding more intermediaries is not required to enable better correlation privacy; it simply increases the number of intermediaries that would need to be compromised to learn the full path.

#5 Relationship Context Channels

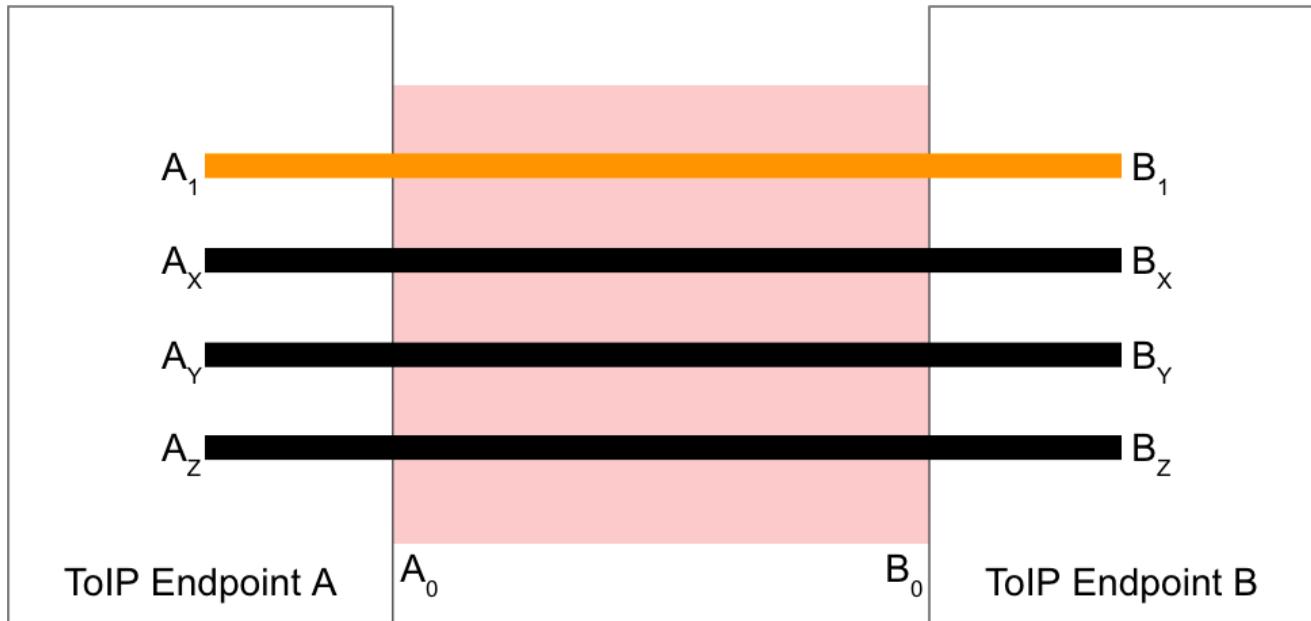


Figure 3: Using the default inner channel as a control channel to establish new independent relationship context channels between A and B

#6 Text and Binary Encoding

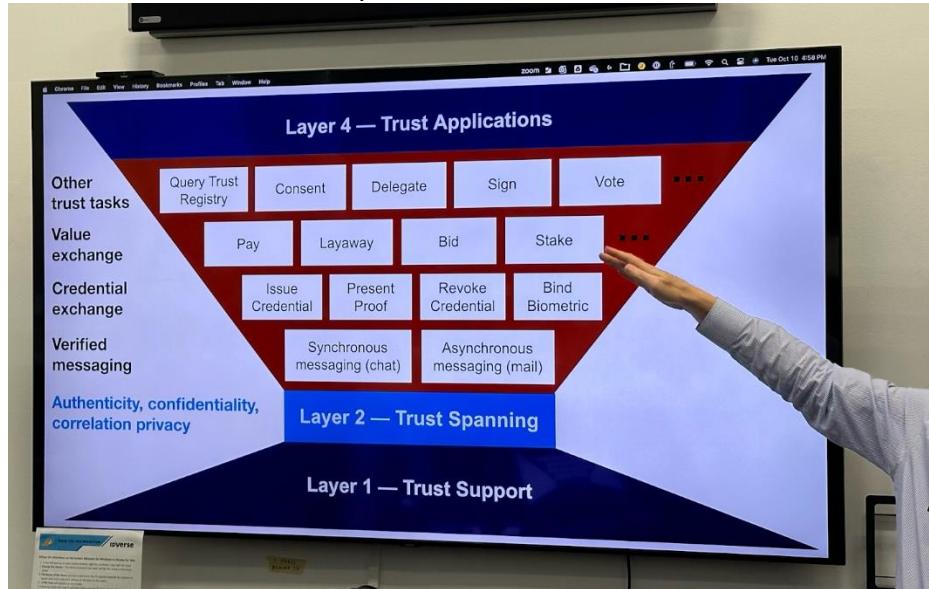
Refer to CESR for Muggles

CESR for First Year Wizards - Google Slides

https://docs.google.com/presentation/d/12nX_IIPp5xw8qAxhZy-ae2aWYytYQmFBbB9K3PcVhqQ/edit#slide=id.g411be7e84_0_0

#7 Trust Task Protocol Framework

Four standard trust and beyond:



IIW 101 Session - Self Sovereign Identity (SSI)

Session Convener: Nuttawut Kongsuwan and Catherine Nabbala
Session Notes Taker(s):

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

Link to the slides

https://docs.google.com/presentation/d/1_eKNevgLW6UWHjTIJllycPY8PJ1GPYIkIq1gn8AhbL0/edit?usp=sharing

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

Notes prepared by Michael Becker (notes in Markdown, use a markdown reader to render)

****SSI 101****

A wonderful review of SSI history (how we got here) and the technical elements: DIDs, PCs.

Why do we need SSI?

Claim- Privacy Concerns

 Evidence- Snowden leak, 2013

Claim- Large data breaches

Claim- The Internet is not secure (was built without an identity layer)...was built on an assumption of trust.

The invention of the Internet, 1969, first message USC to Standard (the opinion)

The evolution of the Internet

* **1970** - Centralized Identity

- Every site has its own security
- Your data is not portable or usable
- Personal data honeypots for data breaches

* **2000** - Federated Identity

 - turns data barons into data emperors (IDP: Identity providers, e.g., Google, Facebook, etc.)

- Open ID invited at IIW

* **2009** - introduce "zero trust architecture" we address for the first time that the

* **2015** - Decentralized

- originated at IIW in 2015, IIW #20

Principles and Characteristics of Self Sovereign Identity, Christopher Allen

* **Existence**. Users must have an independent existence.

- * **Control**. Users must control their identities,
- * **Access**. Users must have access to their own data.
- * **Transparency**. Systems and algorithms must be transparent.
- * **Persistence**. Identities must be long-lived.
- * **Portability**. Information and services about identity must be transportable.
- * **Interoperability**. Identities should be as widely usable as possible.
- * **Consent**. Users must agree to the use of their identity,
- * **Minimalization**. Disclosure of claims must be minimized.
- * **Protection**. The rights of users must be protected.

Definitions

- * **Granular disclosure**
- * **Ownership vs. control vs. management of data**
- * **Valorization of data**
- * **Holder**
- * **Referer**
- * **Issuer**
- * **Wallet**
- * **Agent**
- * **Governance** , can tell you what you can/should do and not do within the system, Layer 1: establish what methods to use,
- * **Idempotent** denoting an element of a set which is unchanged in value when multiplied or otherwise operated on by itself.
- * **Universal Resolver**
- * **Decentralized Identifier (DID)**,
 - has four properties, globally unique, resolvable, highly available, and cryptographically verifiable; has a scheme, method (how you use it or find its policies), and the ID.
 - currently there are [183 methods](<https://w3c-ccg.github.io/did-method-registry/>)
- * **DID Document** DID document includes public key, authentication protocols, and service end-points for cryptographically- verifiable interactions
- * **Verified Credentials**
- * **Identifiers** , is an ID issued by a [trusted] authority used to identify another entity (e.g., individual, bot, machine)

Resources

- * [The 7 Laws of Identity (2005)](<https://www.identityblog.com/?p=1065>)
- * [Principles and Characteristics of Self Sovereign Identity, Christopher Allen] (<https://decentralized-id.com/self-sovereign-identity/characteristics/>)]

Federated Auth Network

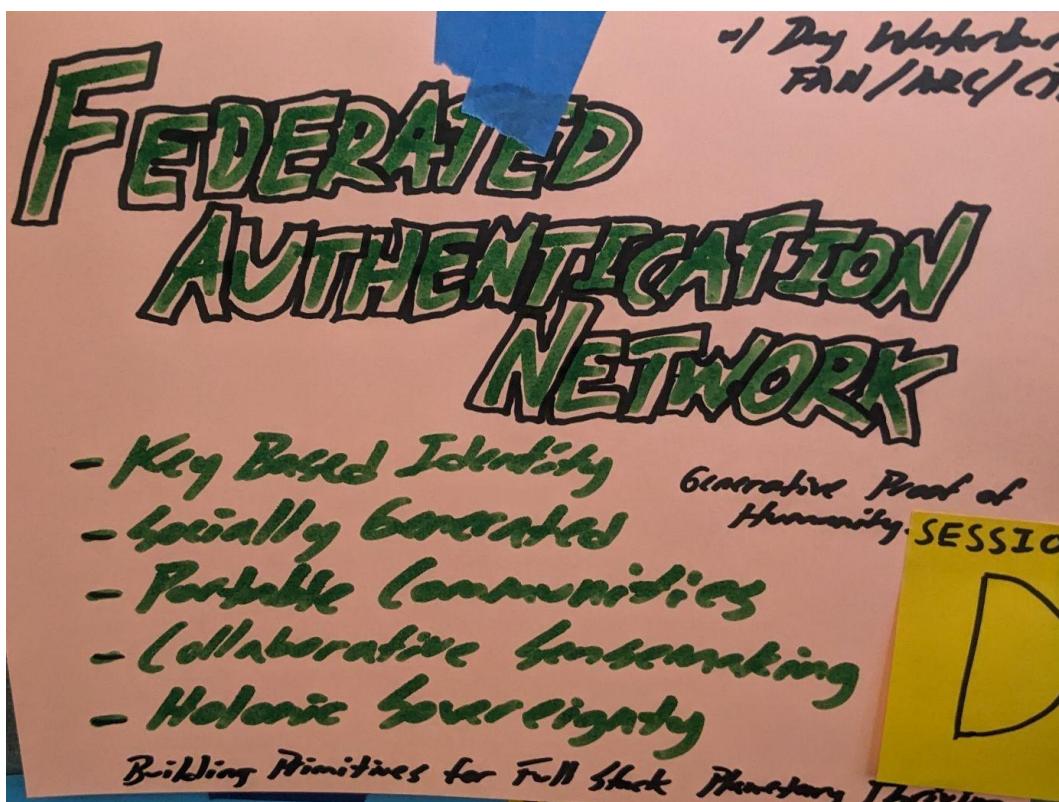
Session Convener: Day Waterbury
Session Notes Taker(s): Day Waterbury

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

<https://git.deepnet.com/fan/fanauthmanager>

#ssi #keybasedauth #generativeidentity #proofofhumanity #openprotocol

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



Understanding the Federated Authentication Network requires flexibility in defining terms so that we might humor the F.A.N. backronym:

- **Federated** might mean that we have a P2P “federation” of people who trust each other, sign one another’s keys, etc., or it might just mean the general alliance of FAN-enabled websites and apps, or perhaps in some cases federation-proper might happen, where the public keys of users on one server are shared with another federated server so that the person can easily login anywhere in the network.
- **Authentication** could also be P2P in that we might just be talking about exchanging keys so we can send encrypted and signed messages (in some sense we’re authenticating one another as peers), or, as more commonly understood we could be authenticating as users on a server to access restricted content or permissions on a website or app. I often just

shorten this to “auth” to intentionally increase ambiguity/flexibility of the term to include “authorization”.

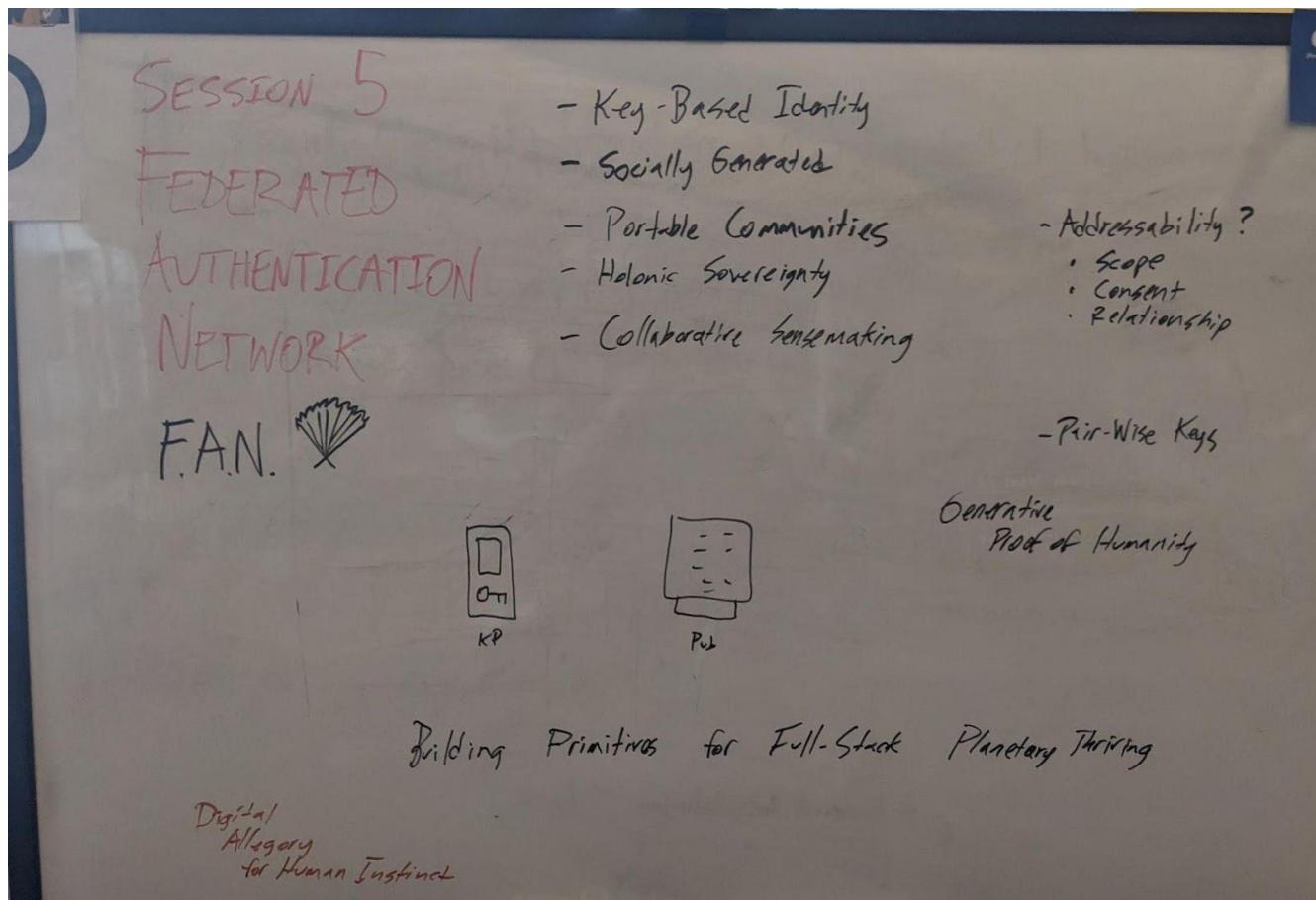
- **Network** is already sufficiently broad since it indicates both human and computer networks.

What is FAN and what problems does it aim to solve?

- Key-Based Identity
- Socially Validated
- Proof of Humanity
- Holonic Sovereignty

In support of...

- Portable Communities
- Collaborative Sensemaking
- Liquid Democracy
- Emergent Chaordination



"Building Primitives for a Full Stack of Digital Public Goods supporting Planetary Thriving"

FAN started out as an SSO project in the CTA (Collaborative Technology Alliance) Collabathon '23. We have buy-in for integration among CTA member platforms/apps. Then we'll aim to integrate

with other open-source software, including Mastodon and other Fediverse apps. And tomorrow, the world.

A criticism was brought that this wasn't really built for and might not appeal to a large enterprise market. And that's okay, we're not building in support for large companies with command-and-control models. Our architecture specifically encourages self-organizing forms of governance based on trust and consent.

Existing partners include: GreenCheck/NAO, CTA (Hylo, Catalyst, Nestr, Factr, Forby, and others).

We are actively seeking development and integration partners! Please contact Day via email at deim@protonmail.com or via Signal at +1 707-205-7686.

Transcript (from audio playback to Google voice typing):

FEED ME! Unified FEED - What do we need in a Unified Feed of all Asynch communication

Session Convener: Stephen Vitka

Session Notes Taker(s): Stephen Vitka

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

Here is the original thinking (a bit out of date)

<https://www.dropbox.com/s/v9u7zod8rg50rr2/Contact%20Credits.pdf?dl=0>

A few months back did a presentation

<https://archive.org/details/shorttalks-metegov-20230614>

deck :

https://docs.google.com/presentation/d/1K1r6GLiHE9rrofAlb_DZFWZkv_kk2RZlfijpVUyRJc/?usp=sharing

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

We discussed the opportunity to create and features of a Unified Feed.

Unified Feed: All asynchronous communication is available offline, in a user prioritized list.

A cure for what Hassan Manaj characterized as "I have 100 apps I use to stay in touch with the same 8 people."

GDPR and California Law require continuous API access to our platform data, so this is now possible to build.

Features requested:

1. Filtration - by source, platform, and Virtual Agent with parameters. Example "Batch incoming messages from X into groups of 10." also Mood and Work/Project Modes with as user definable and community configurable filtration pre-sets.
(Also touched on using weighted #tags, which is method to refine their use make less spammy)
2. Social Discovery through trust and rep networks
3. Click through to sites without sign in. (integrated Oauth?)
4. Most posts/content also viewable natively in user customized viewer.
5. De-dupe incoming messages, and allow you to reply closer to primary post (vs. re-posts)
6. Drag Feed into another Workflow (to do list, etc.) or vice versa.
7. Integrated Micropayment, example, watching something in my feed autopays the right people.
8. Optional Payment for Attention: Each user can set an \$IndiscriminatePrice that anyone can send a message to the top of their feed. User can lower price for anyone /any set in particular, and virtual agents can negotiate prices based on user settings for content that is of interest to the user.

Such users can send their purchase or other data to vendors to induce them to pay close to their \$IndiscriminatePrice to contact them! Vendors can send boring ad which will get read or they could send a link to a world of content customized according to what the user chooses to share. This could lead to the disintermediation of platforms from advertising. and fantastic customer experiences we will look forward to opening. See attached paper, deck and video prez for Steve's early, yet extensive work on this...

AuthZ Conference

Session Convener: Sarah Cecchetti
Session Notes Taker(s):

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

Moving forward there will be a recurring meeting. sarahcec@amazon.com will be the host of the meeting (AWS Chime).

Members can join this Google Group: <https://groups.google.com/u/2/g/authorize/members>

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

Folks from leading Authorization companies such as Axiomatics, Aserto, 3Edges, Strata, and AWS got together to discuss the creation of an authorization-dedicated conference in the vein of Authenticate. We discussed options such as:

- running it as a workshop of an existing event (e.g. EIC, Identiverse)
- running it prior to or after an existing event (e.g. EIC, Identiverse)

Improving the W3C CCG DID Method Registry

Session Convener: Martin Riedel
Session Notes Taker(s): Robert Leonard

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

- DID Method Registry

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

- Deprecation of DID Methods:
 - The upcoming W3C working group will discuss the potential support for deprecating DID methods.
- Discussed different ideas about the liveliness checks of DID Methods:
 - Discussed tradeoffs about performing liveliness checks every 6-12 months.
 - Two approaches were discussed:
 - Manually emailing the registered DID method owner.

- Submission of a test suite via GitHub, which would demonstrate functionalities like DID resolution and updates.
- The group's consensus leaned towards the overall goal of incentivizing the registration of quality DID methods but not being a gatekeeper.
- The recommended way for an actor to acquire the registration of an existing DID method is to directly communicate with the current owner.
- Multiple Registrations for the Same DID method:
 - The group's consensus leaned towards multiple DID methods should be allowed to register under the same namespace.
 - Currently, editors would however deny conflicting name registrations.
 - There's uncertainty regarding the support for this in the current DID method registry implementation.
 - This brought up another topic of defining what the “quality” of a registered DID method is and how to compare DID methods (also if they can be compared)
- Standardisation for DID Method Resolution:
 - Another topic for the upcoming W3C DID working group will be the potential standardisation of DID method resolution.
 - This can be applied towards the W3C DID Registry which could require all DID Methods to provide resolution (testable) endpoints. Some DID methods might need valid exceptions for this.
- Resource Recommendation:
 - A podcast was recommended for more information on DID methods and DIDs in general: <https://rubric.cc/>

JSON-LD BBS+ Verifiable Credentials with Private Holder Binding, Pseudonym, and more

Session Convener: Dan Yamamoto

Session Notes Taker(s):

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

Presentation Slides: <https://speakerdeck.com/yamdan/json-ld-bbs-plus-verifiable-credentials-with-private-holder-binding-pseudonym-dot-dot-dot>

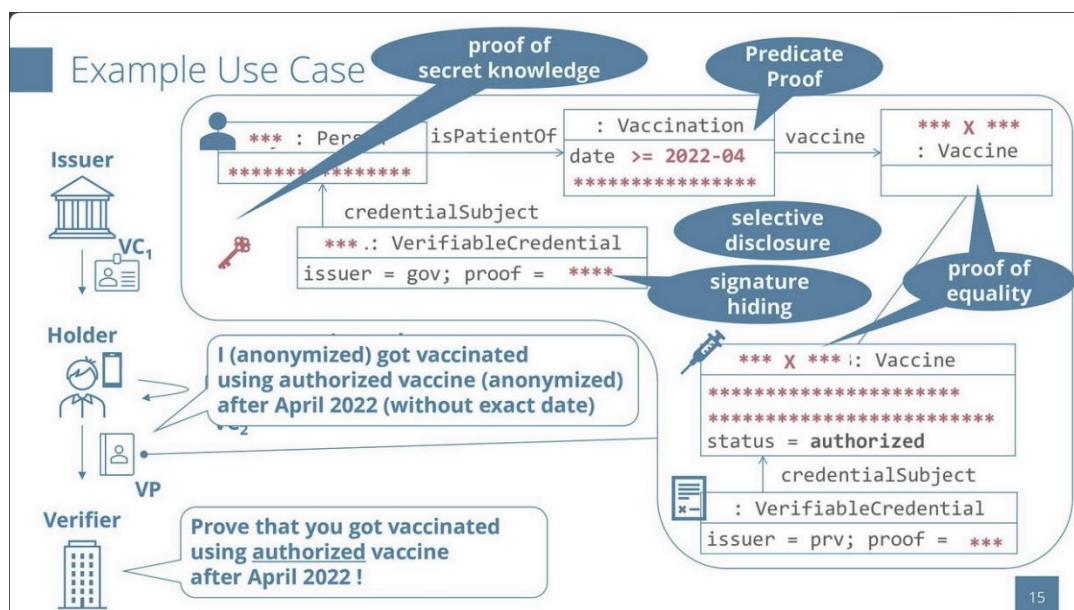
Live Demo: <https://playground.zkp-ld.org/>

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

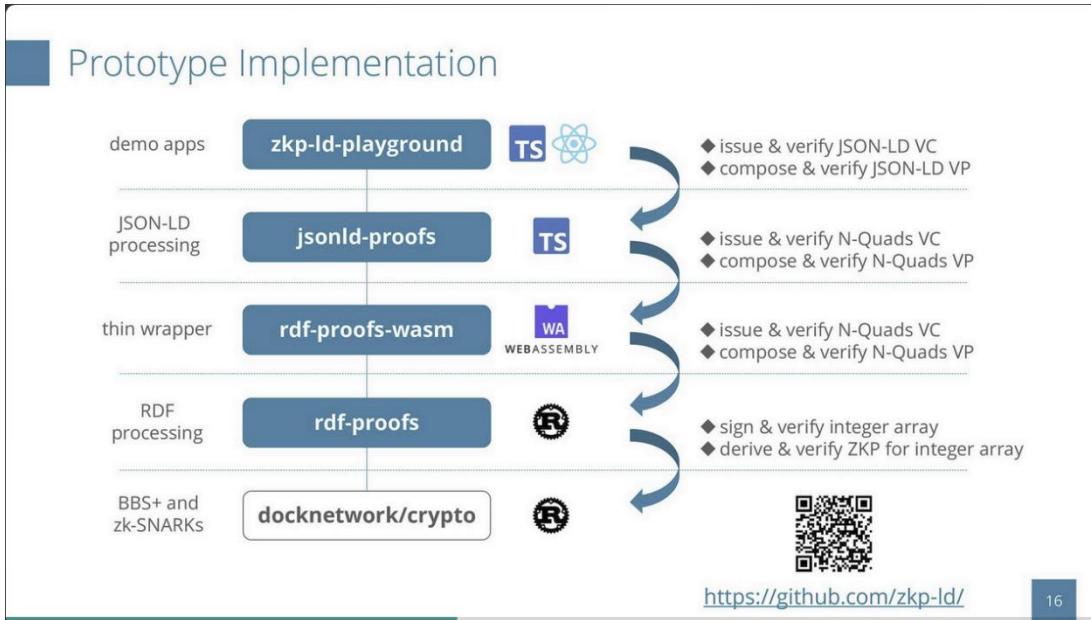
Convener explained JSON-LD Verifiable Credentials based on BBS+ signatures with the following features:

- selective disclosure
- hiding signature value (for unlinkability)
- proof of equality for hidden attributes, enabling anonymous linked data
- blind signatures for private holder binding
- pairwise pseudonymous identifiers (PPIDs)

An example usecase was illustrated using slides, where a Holder combines two VCs (key-bound Vaccine certificate & unbound Vaccine specification) and uses zero-knowledge proof techniques to selectively hide unnecessary parts of attributes.



Their prototype implementations, using docknetwork/crypto library as their building block, have been published on GitHub. More documentations are expected to be added.



The session included a live demo of their implementation.

Playground

<https://playground.zkp-ld.org/>

17

Discussed:

- Comparisons with other BBS+ implementations including Hyperledger AnonCreds v2
- How to implement PPID using Pedersen commitments and BBS+
- A brief introduction of “termwise” encoding that enables proof of equalities
- Why do we need Canonicalization? -> to resolve ambiguities before signing and verification

WIMSE - Workload Identity in Multi-System Environments

Session Convener: Justin Richer
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

Building Test Suites

Session Convener: Ben Goering
Session Notes Taker(s): Charles Lanahan

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

Test suites, ActivityPub, Aries, Openid Connect

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

Motivation for this talk was to create a better test strategy for ActivityPub and to see what others are doing. Speaker moved to explore the participants.

First speaker (notetaker) called out that the Aries Interop Profile was a pretty good example of interop testing over a quite complex communications protocol that was somewhat usable for testing one's own implementation. Noted that testing was quite hard, might be better to do in a set of data artifacts that should occur at intermediate steps of a communications workflow.

Second speaker was from DCC - Digital Credentials Coalition. They've gone to make that kind of thing happen in their test suites. Its all about adoption and making tests. Hard to force a community. Thought openid connect was a good example of a community with tests for providers and clients.

Third speaker called out VC-API. Activity Pub was doing "good enough" testing. Ie) Test implementations against each other one by one. Brute force testing.

openid cert program

ceramic, 3blocks -> pass test suite for rebuilding W3C VC

Accessibility W3C Conformance Profiles were pointed out as good examples of using 1) rules 2) props under a hierarchy of human motivated tests to provide testing for accessibility.

Aerospace does a good job connecting human languages -> rules to test in their checklists and profiles.

Openid has a test suite in browser form. Its pretty sweet.

State management is a major issue in some protocols.

Why not mastodon instead of X.

Web intent intended but not achieved.

Major diff between the spec as written and what implementations actually do. ie) TLS, HTTP, email et al...

HACKATHONS! did:hack / DIF Learn more, get involved, get hacking!

Session Convener: Limari Navarrete

Session Notes Taker(s): Limari Navarrete

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

Slide Deck <https://docs.google.com/presentation/d/1it1xYotfV8-fXuuXvmQObNDTDAiVm7KyMbXI4dhyQAI/edit?usp=sharing>

did:hack winner demo <https://youtu.be/sikLAwKHTYw?feature=shared>

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

This was an overview of the did:hack hackathon which took place in early June 2023. We discussed why we held this event, how we put it together and who was involved. There was a great discussion on the positive effects of hackathons on adoption and interoperability. The co-organizers and hackathon winners were present and we enjoyed an extensive demo of their decentralized personal finance app. We also had an overview of the upcoming DIF hackathon with a \$19,500 prize pool. <https://difhackathon.devpost.com/>

Secure Issuance for Government Credentials

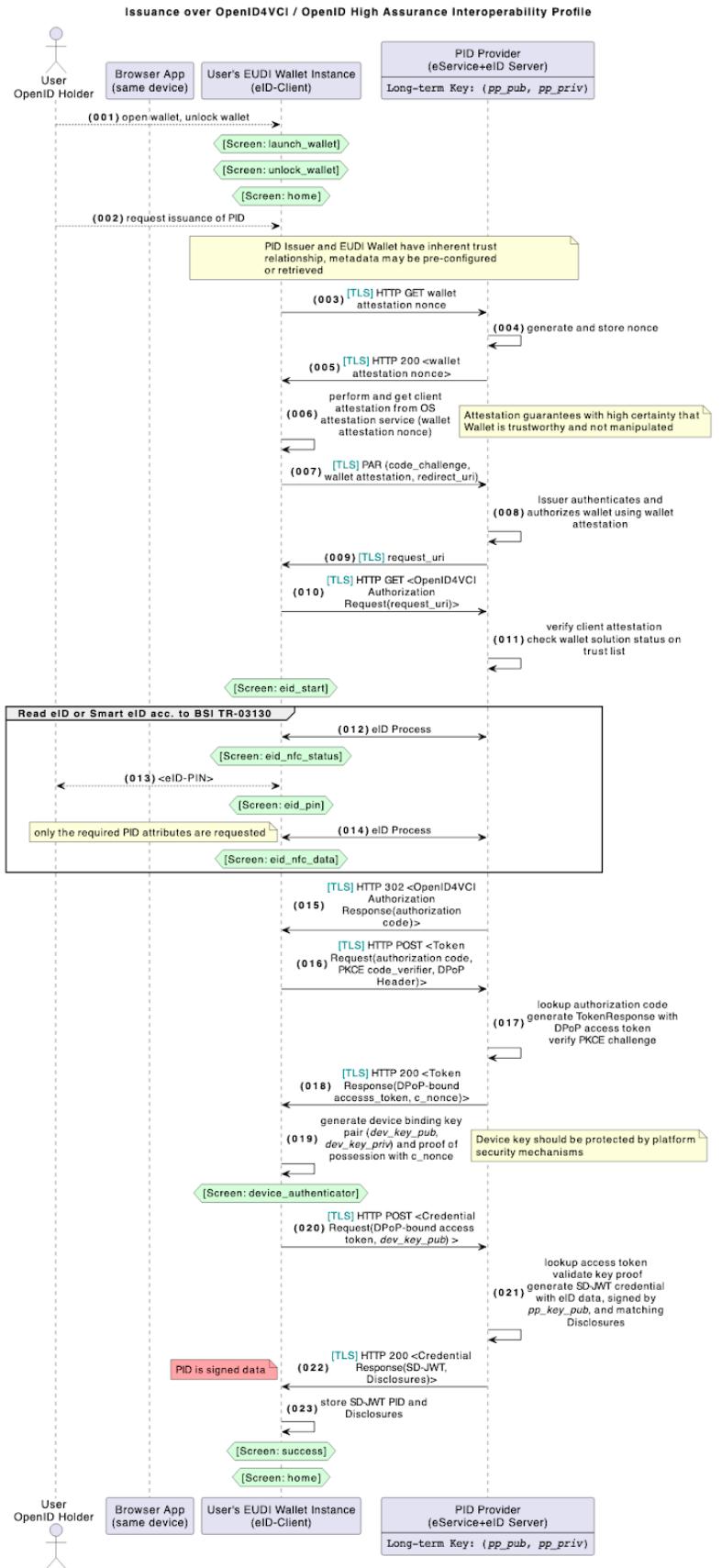
Session Convener: [Paul Bastian](#), Torsten Lodderstedt
Session Notes Taker(s): Andrew Hughes

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

- Talk is about Government issuance of PID to devices at eIDAS High
 - based on project building an German eIDAS government wallet
 - using OpenID for Verifiable Credential Issuance
 - Architectural assumption is that the secure element is on the device
 - some differences in different architectures
 - where the keys are (in the mobile, cloud HSM)
 - where authentication happens
 - mobile devices offer many different ways to store keys - complex situation
 - National ID Card issuance - flow starts from the wallet
- << showed a sequence diagram for Issuance via OID4VCI / OpenID High Assurance interoperability Profile >>



CONTINUED BELOW



- Wallet authenticates towards the backend using attestations (from OS vendor/app store); attestation is bound to a key that the wallet controls; used for proof of possession
- <<< The point is to transform the platform specific attestations into 'interoperable' attestation structure (as a JWT) - and that is passed to the issuer as an authentication >>>
- this will require the backend wallet services to produce a standardised JWT
- if need to provide non-correlation between issuers, should use fresh attestations
- << concept of OID4VCI issuance is an issuance API that is OAuth protected >>
- << discussion about certification levels for key protection >>
- German national ID cards have a chip - and today, presentation is to hold the card against your smartphone then enter PIN. This work is to improve the UX to avoid the physical presentation experience. All at eIDAS High level.
- in Germany, PID must be at level High - but most interactions happen at level Substantial- in the future these might be reconciled - discussion must happen
- This presentation is to show that it is possible to issue credentials at eIDAS LOA High with OpenID 4 Verifiable Credential Issuance

Identity + Peer Production

Session Convener: Brent Shambaugh

Session Notes Taker(s): Brent Shambaugh

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

<https://www.sensorica.co/>

<https://www.internetofproduction.org/>

http://ovn.world/index.php?title=Main_Page

<https://www.valueflo.ws/>

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

How does this relate to identity? Identity is something that I am capable of & reputation. May need to tie this to a DL so you don't defraud. Down the road have all this access.

To [combat fraud in contributions] we have red flag mode for logging hours of contributions. If the numbers look weird they are not added until they are resolved.

[other things in the system have identity] Do inanimate objects have identity? Does this chair have an identity? Decentralized identifiers are like the name of the chair.

Does this have something to do with identity? Talking about our experience in Montreal [it has to deal with] OVNs. Open Value Networks people are deriving the value, and OVNs do not exist in a vacuum. Identity is in an OVN because there are people involved.

Physical workspace...small use case. Want people to come to use same person as ID. Now completely digital banking SoFi How verify come in. How done test to go gamble. Usually pass through.

We are all part of production and creating surplus. Kept beyond big institute[s] [with] peer production...outpace with technology. People are very tribal and exclusive. Americans are very terrified by socialism ..do things for yourself and by yourself.

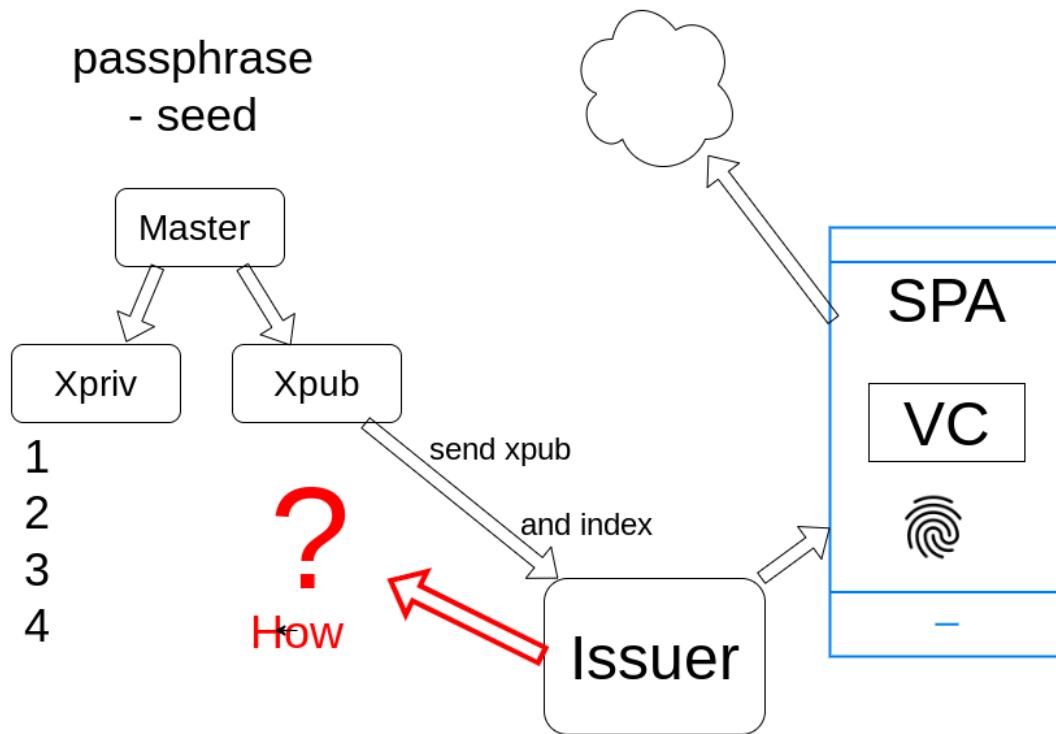
Idea of AI coming in. Ai has been and explosive thing now for mass consumption. How do we protect . end going back to peer to peer. hyper individualistic society is the problem. can we go back to peer-to-peer. command. people that will always be exploitative . create technology that will uplift humanity. we should have an ai president and congress...universal human rights....everyone should be ever to vote on policy..

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

SESSION #6

BIP32 and You (Fido Row Signatures)

Session Convener: John Bradley
Session Notes Taker(s): Mike Schwartz



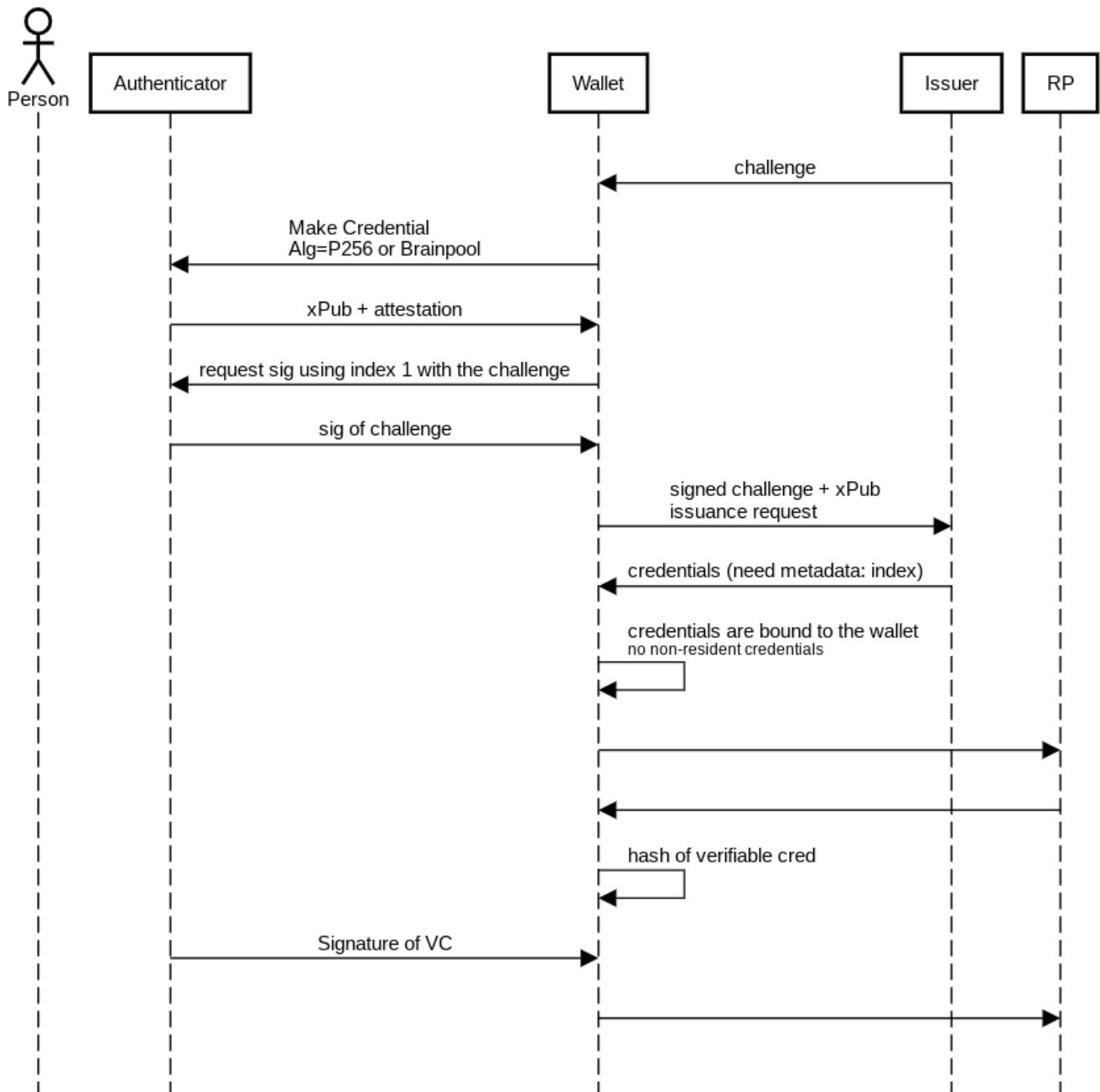
Makes the wallet portable in the same way we've made the passkeys portable, allow you to hardware protect your proof keys -- so when you get a new device, you'll get your keys. Competing with secure enclave and strongbox--gives more vendor independence.

Need an extention to CTAP in order to make this happen (to sidestep charter of Webauth).

PRF extension does symmetric encryption / decryption with a key that can't be phished without the user authenticating.

If user accidentally deletes the signing key, it has a big blast radius. If you delete the credentials for signing into your wallet, you are screwed. You have to provide a warning to people about how important the credential to get into the wallet app.

Key Derivation to optimize the UX of multiple Authenticator keypairs



[Source](#)

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

What is the use case?

- FIDO wasn't designed for two parties (issuer, rp), but new SSI infrastructure has three parties (wallet, issuer, verifier). But to get the benefits of the portability of FIDO keys, can

we use cryptographic strategies like BIP32 to derive additional keys to share verifiable claims tied to our FIDO key without creating correlatability.

- Passkeys are distributed to all the users devices... can we use passkeys to derive keys that enable us to prove control of credentials? So when we install a wallet on a new device, it can request credentials from the respective issuers (without prompting the user 10 times to prove presence?)
- This use case is outside the scope of the _____ charter? Would the charter need to be updated?

GNAP 101

Session Convener: Justin Richer

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

People don't want a digital identity

Session Convener: Adrian Gropper

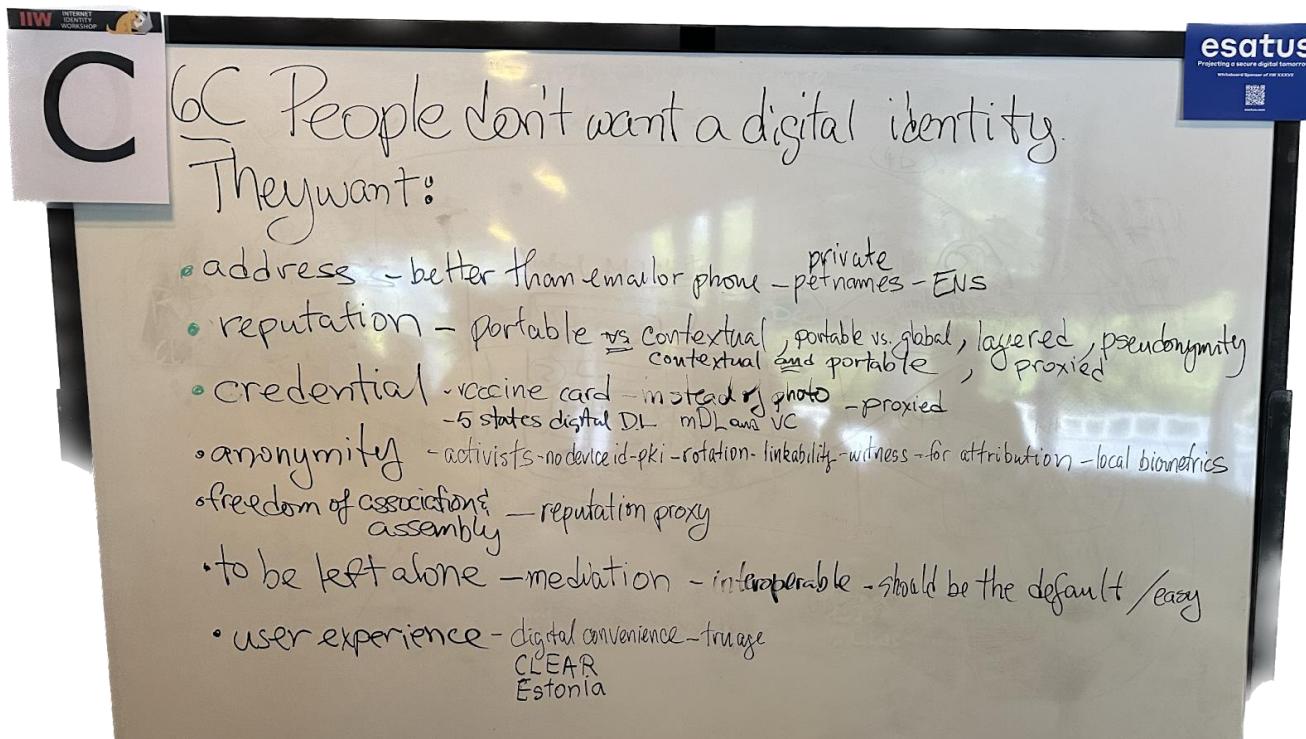
Session Notes Taker(s):

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

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

Not the official note-taker, but I posted a short recap here:

[Session 6C: People Don't Want a Digital Identity; They Want ...](#)



Philosophy: The code behind the code.

Session Convener: Samuel Hutchens
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

GLEIF's experience with the vLEI Ecosystem Governance Framework: Lessons Learned

Session Convener: Karla McKenna
Session Notes Taker(s): Zaïda

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

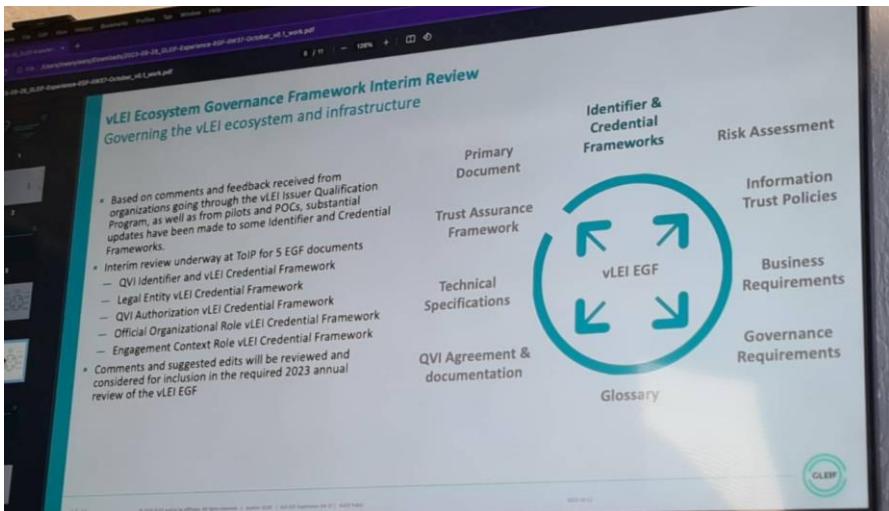
https://github.com/WebOfTrust/IIW37/blob/main/2023-10-11_GLEIF-Experience-EGF-IIW37-October_v1.0_final.pdf

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

GLEIF's Ecosystem Governance Framework (EGF) experience
vLEI: trusted frameworks
Digital version of the LEI system

Feedback on governance and organisations from:

- Qualified vLEI issuer program
- Setting up own operations
- Authenticate the holders
- Ecosystem governance framework
- Are you giving the right credential
- Are they getting the credential in the wallet



They issue to legal entity

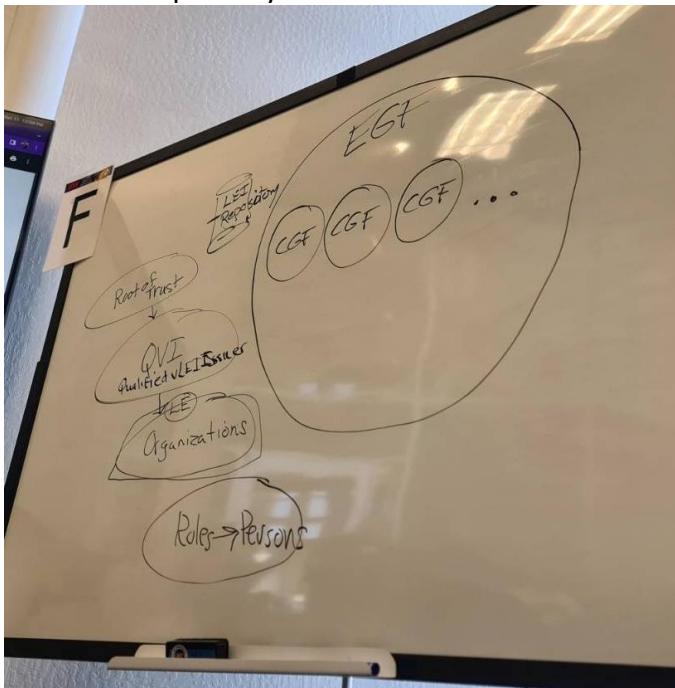
- Either QVI
- Or vLEI

Inside the credentials

- Modular architecture for all the pieces you need to get an overall digital trust ecosystem

You have to be qualified

- Domain: qualified by IQI
- DNS: registers
- LEI repository



Hierarchical system

1. Root of trust
2. QVI (Qualified vLEI Issuer, GLEIF can do that)
3. Organizations
4. Roles —> Persons

GLEIF:

- LEI identity by its LEI using VC (ACDC: authentic chain data container)
- What they wanted: LEI would be part of the credentials
- LE not only binds to the QVI but ALSO to the organisation it's issued to. How are we able to revoke? If we revoke the LE credential, everything broken down.
- Cryptographically bind organisation to LEI repository
- ROCK or LEI ROCK (70 global regulators)
- When a registrar comes for an LEI: legal entity form
- 600 registration authorities that are able to proof that that organisation exists
- Not just talking about all entities that are portable

OOR

- OOR: has an LEI
- Most of the time it's a name
- QVI: easy to verify person and role
- Structure of OOR role within credential
- Require change in schema
- More information? Put in OOR in credential
- Have to ask company to revoke it

Mix of organisations that use LEIs

LARS:

What are the stakeholders?

- GLEIF
- Holder in LEI
- Q vLEI issuers
- People that get role credentials
- Users (membership, consortium, verifiable authority between party A and party B)
- Trace all the way back to GLEIF that LEI was indeed an LEI
- Cryptographic verifiable authority

What happens when the Lei consists of a single person?

- Separate sections for one employer (sole proprietorship)
- Binds company
- But it should actually have 2-3 employees

Bhutan

- Digital identity scheme for citizens
- Digital identity scheme for organisations

What is the process for a new

- The LEI is affected by change of control
- You have to update LEI
- Status of LEI (QVI do that) in global LEI
- Credentials need to be revoked if LEI is not up to date
- So the LE that is issued by the QVI gets revoked!!!
-

How are LEI's used?

- Give CEO
- CEO: be able to use LEI within policy of organisation
- Give them different kind of tools
- To make it more secure and better
- That will be in the company's framework
- Signing and binding can be done within the LEI's

Notes

- You have to have an LEI to get a vLEI
- Council of QVI that will have self governance what they are doing: GLEIF has governance of LEI's

What have we learnt from the original documents?

The screenshot shows a presentation slide with the following content:

Lesson #1 Governance as a differentiator for the vLEI

- The detailed work done on the EGF is one of the most significant and important differentiators for the vLEI.
- Based on GLEIF's history and experience as an organization under regulatory oversight, strong governance was a given.
 - Governance is so important to the LEI as a founding principle and it was normal for GLEIF to expect to extend the importance of governance standards to which GLEIF is used to having to comply to the vLEI.
 - So GLEIF places significant importance on governance for the vLEI. And . . . the formation of TolP and the guidance provided by TolP in developing and encouraging the use of the TolP metamodel for the vLEI EGF reinforced the importance of this governance.
- Let's discuss

On the right side of the slide, there is a circular logo for GLEIF, featuring a stylized 'E' composed of vertical bars in black and teal, set against a light blue background.

Lesson #2 Learn from doing

Important updates to the vLEI EGF have been due to learning from practical experience with QVI qualification, POCs, pilots and implementation

Example:

- While GLEIF leveraged the important feature of multi-sig signing of vLEI credentials as much as possible, finding a secure, workable approach for issuance of vLEIs to organizations with a single employee that had signing authority was needed.
 - This demographic, whether in the form of organizations that are sole proprietorships or organizations with more than one employee but with only one authorized signatory, would be needed to support almost all use cases for the vLEI.
- While an initial approach focused on issuing credentials to sole proprietors was included in the drafting and in the v1.0 of the VLEI EGF, it clearly became evident that:
 - First, more clarity was needed overall regarding the responsibilities for the process of Identity Verification (Identity Assurance and Identity Authentication) of both QVIs and representatives of organizations;
 - Second, that more thought was needed to ensure that the same level of care, certainty and security could be achieved especially in cases in which a single person acted as the Designated Authorized Representative to contractually bind either a QVI to GLEIF or a client organization to a QVI, a Legal Entity Authorized Representative who could authorize the issuance and revocation of vLEIs for its organization and the Holder of either an official or functional role vLEI credential for its organization.



Lesson #3 Is there an optimal process for drafting and maintaining the EGF?

Deadlines vs. Necessary engagement vs. Spreading the knowledge

- How do you prepare and draft a comprehensive EGF, keeping the momentum going, maintaining consistency throughout?
 - Relying on one person; engaging those with necessary expertise; laying the foundation for spreading the knowledge

Example experience:

- For the initial drafting of the EGF, the ToIP metamodel for EGFs still was young.
 - Drafting required much guidance from ToIP to understand the types of documents, their purposes and focuses for content, their formats and styles for preparation.
- Result, the comprehensive, overall, interactive view of the vLEI EGF still largely is held by just one person
 - There were challenges to provide the knowledge to those colleagues who would:
 - operate the services for the vLEI (examples: Qualification Program, vLEI technical operations, the service desk, risk management and compliance)
 - promote the vLEI to potential QVIs, potential users/adopters of vLEIs interested in POCs, pilots and implementation

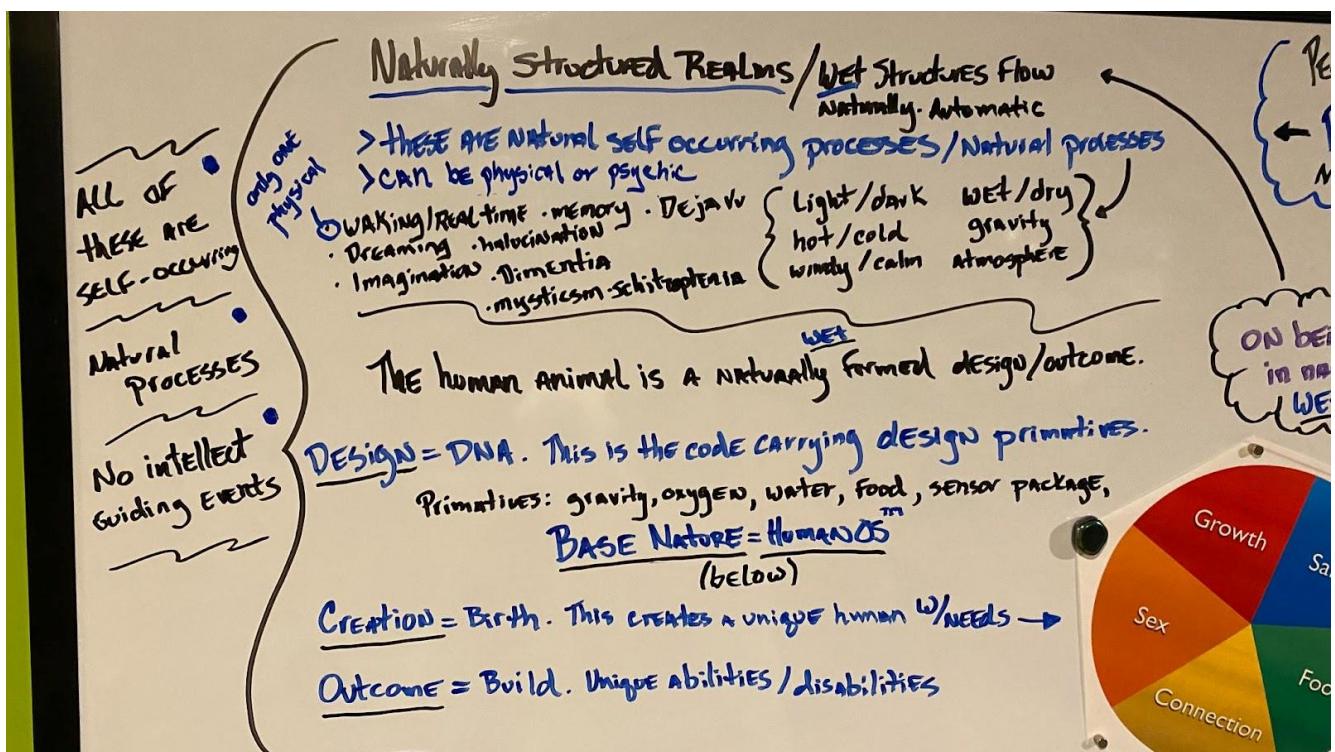
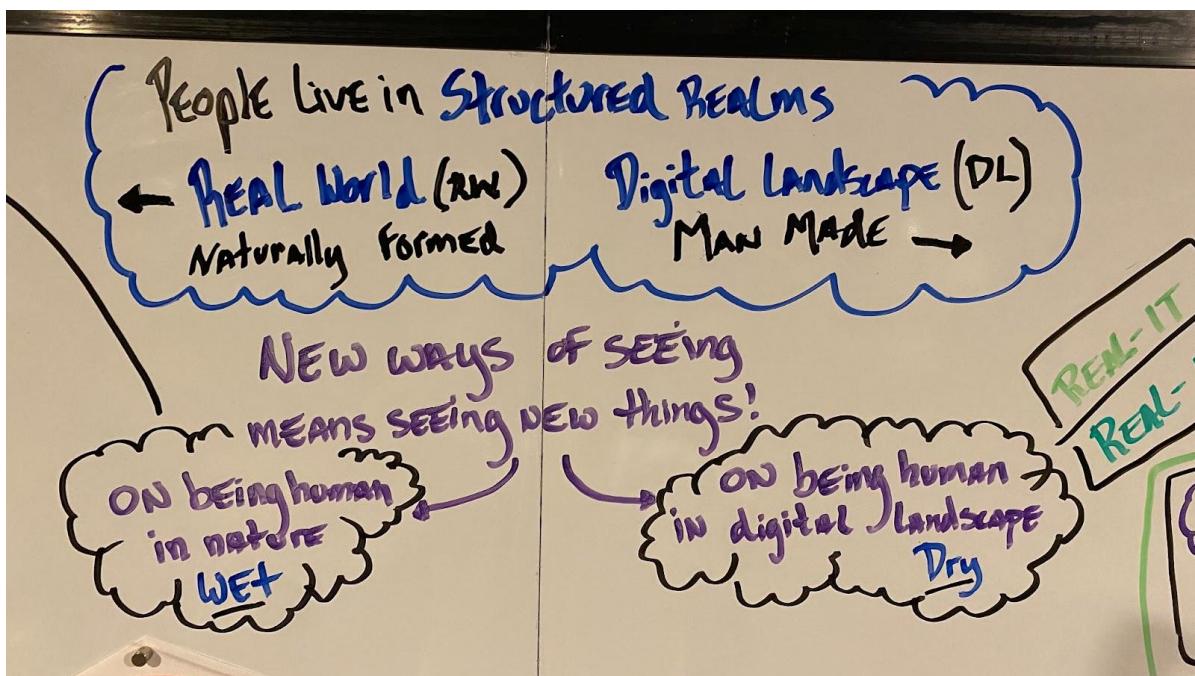
▪ Let's discuss

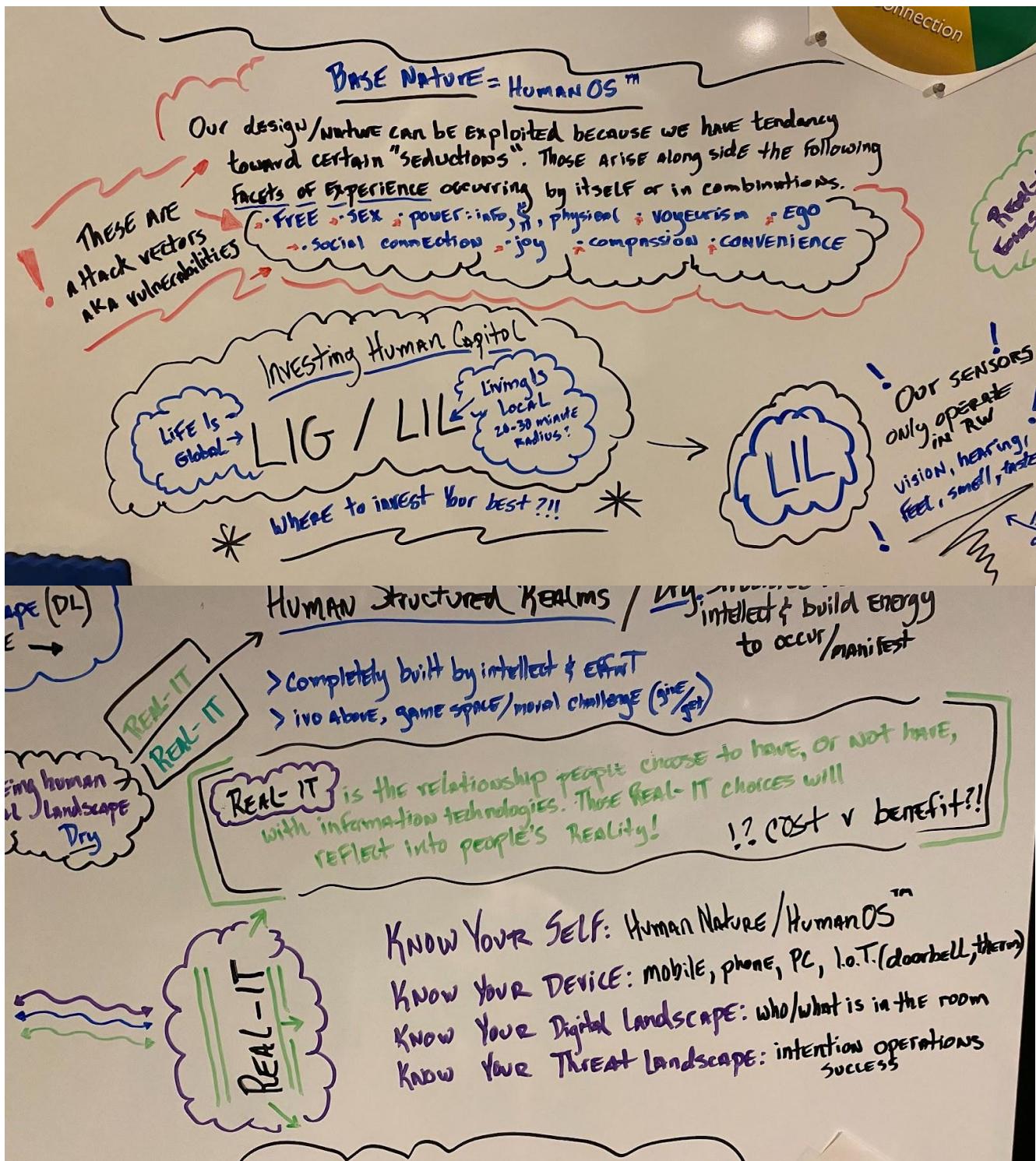


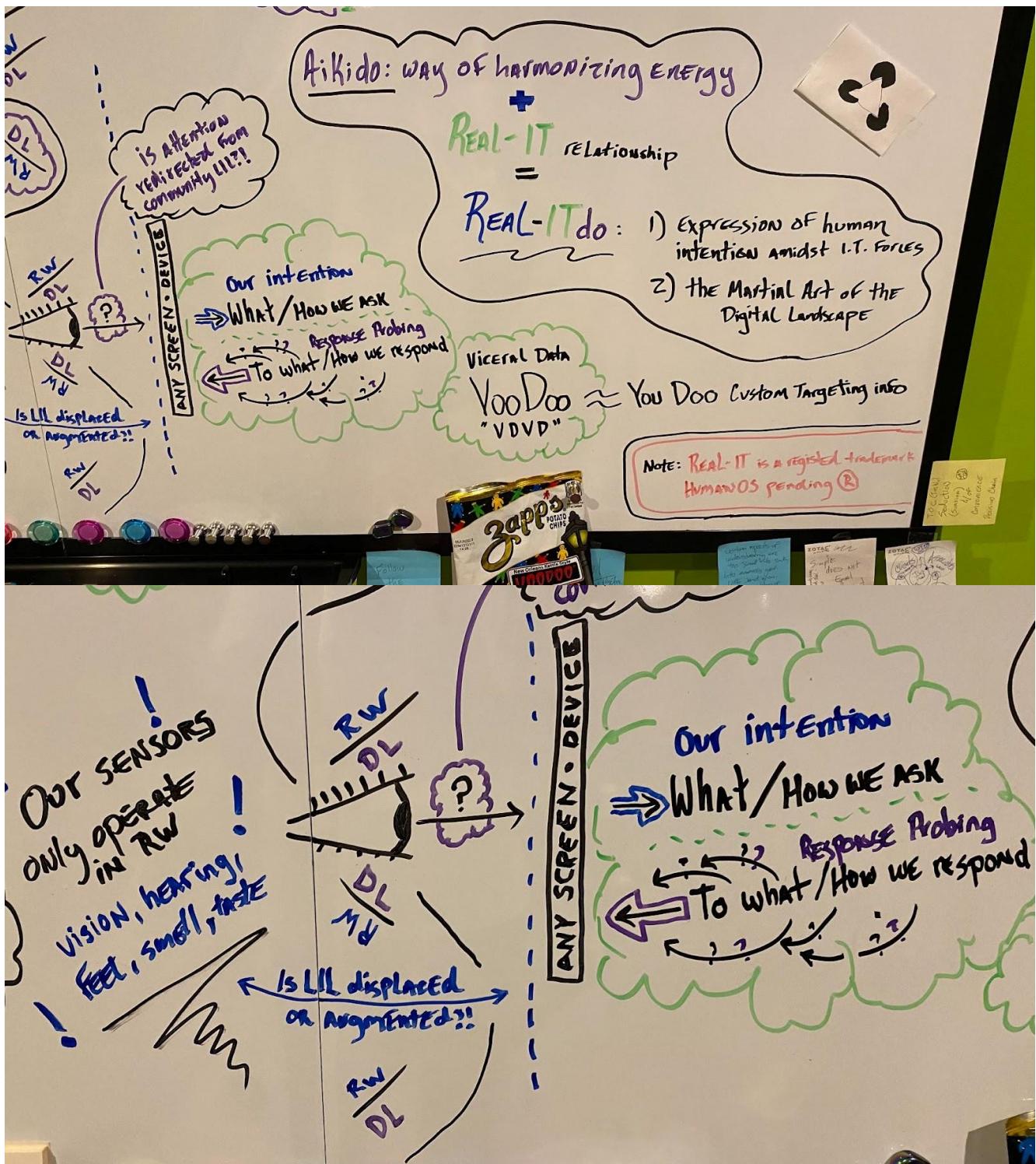
Human OS - Functional / Modality Challenges - Real World / Digital World

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

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





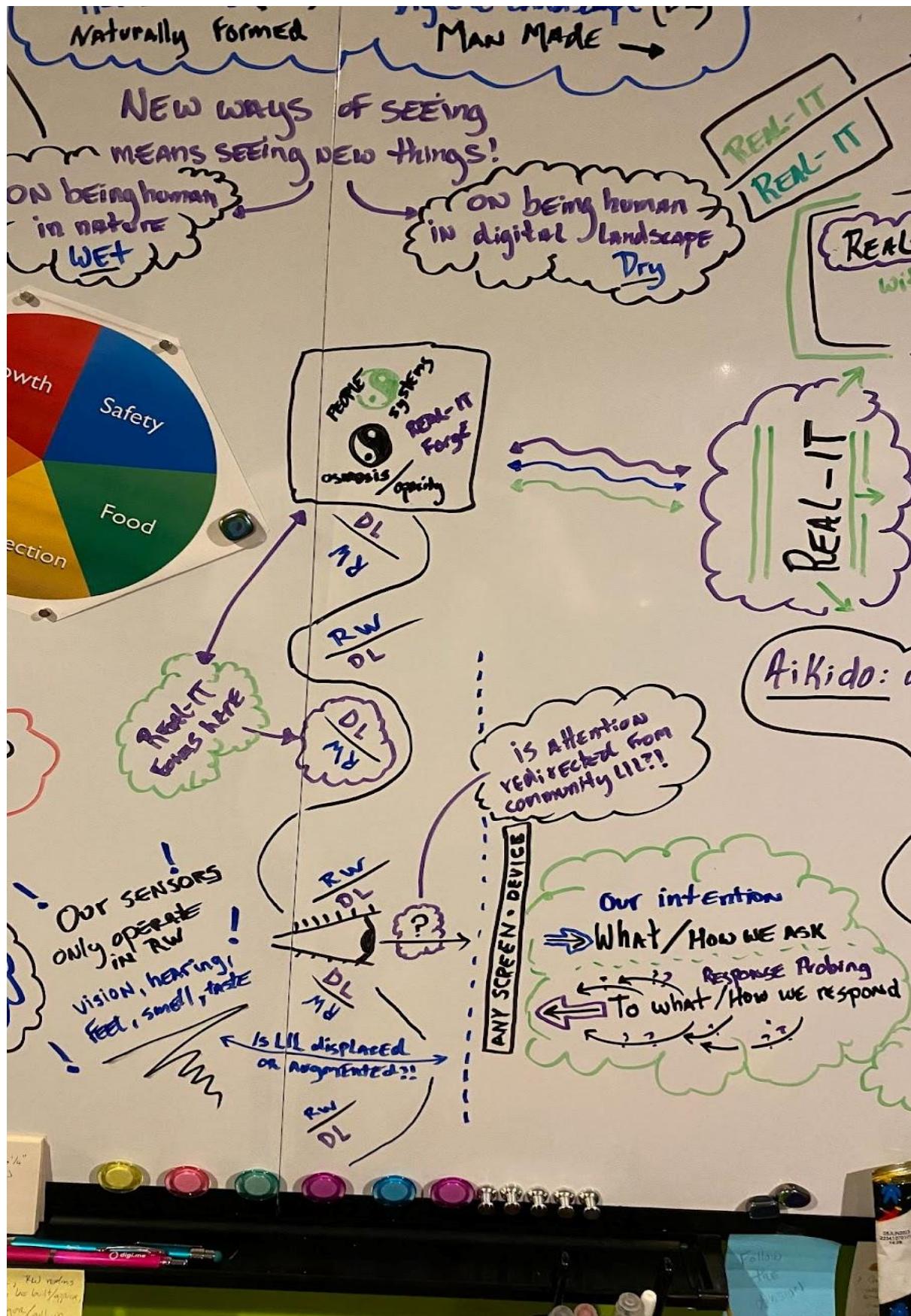


Session Notes

Human OS should be approved

Aikido + Real IT = Real IT do is The Way to go

The comparison between The Real World and The Digital World is yet to be harmonised by The Human OS and relevant techniques and sensory manifestation.



Philosophical Foundations of Identity: Pure and Applied Philosophy

Session Convener: Bruce Conrad

Session Notes Taker(s): Michael Becker

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

The introductory material on Karl Popper is taken from [chapter two](#) of the convener's 1995 dissertation.

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

Notes prepared by Michael Becker (use markdown editor to render formatting)

Philosophical Foundations of Identity: Pure and Applied Philosophy

Bruce Conrad

Ontology: Classification of things that are

As we collect attributes, please remember that there is a living human being the underpins identity."

Questions

What sorts of things do we want to identify?

- Entities (things, governments, people) and their boundaries
- Set Theory: the known relationship between one or more things
- Category theory: directional link-type relations between one or more objects

Is there no right answer to identity?

Who says I am who I am?

Does identity require having a relationship with a relying party?

What does it mean to be a person? Human?

Philosophers

* [Karl Popper](<https://plato.stanford.edu/entries/popper/>): Worlds View

- Proposed the three worlds
 - **World 1**: Real physical universe, assume
 - pre-existence
 - objects can't exist in the same space
 - Can be perceived
 - We create vibrations in World 1 to express concepts from World 2 (e.g., speech)
 - **World 2**: Mind - Person's mind
 - Concepts co-exist in same space

- **World 3**: Collective Mind
 - Concepts that have escaped and take on a life of their own, e.g. advertising jingles, songs, and plays (many World 2 entities that converge)
- * [David Hume](<https://plato.stanford.edu/entries/hume/>): Attributes View
 - Inductive reasoning
 - "memory is the chief – but not only – source of our vulgar notion of personal identity"...bundles which make up what we envision to be the self. [a.k.a. we are made up of a collection of memories (experiences and behaviors), i.e, the collection our attributes]
- * [René deCartes](<https://plato.stanford.edu/entries/descartes/>): Substance View
 - Gave us cartesian coordinates
 - "I think therefore I am" [a World 2 idea]
 - Your identity comes from a substance [World 1]

Discussions

Consider: Hume's attributes vs. deCarte's substance...what makes us?

- * we don't have these discussions often enough
- * we are multiple world 2s
- * we are different
 - * Birth Certificate has World 1 coordinates
 - * Family sovereignty is exercised at birth when you are given a name (an Identifier invented for you for the purpose of identification)
 - In Austria, you can assign a name to a baby, but it is illegal to not assign a name. If you don't assign a name the government will assign one.
 - In Kenya, the second name of a person relates to the context of their birth (e.g. born on the front porch).
 - Dominican judge bans naming kids after car parts
 - Iceland had an official list of allowed names
 - * Cultural context to naming: the woman did not take the husband's name, gave the child the wife's name, and the Dad's Dad could "culturally" stand that the child was not getting its lineage
 - * Collectivism vs Individualism (e.g. transplant effect of regulations)
 - * Government thinks one way, civil society think another way
 - * Joe A: World 1 and World 2 recognize each other, we remember, and then we react on our World 2 and 3

Phil Windley Learning Identity

- ### # Definitions
- * Identity
 - * Agency
 - * Sovereignty

Resources

- * [Ship of Theseus](https://en.wikipedia.org/wiki/Ship_of_Theseus)

- * [21 Grams Experiment](https://en.wikipedia.org/wiki/21_grams_experiment#:~:text=The%20case%20has%20been%20cited,that%20it%20weighs%2021%20grams.)
- * [Dominican Republic judge asks officials to ban odd names](https://www.columbiamissourian.com/news/dominican-republic-judge-asks-officials-to-ban-odd-names/article_2beac437-45a6-5d05-868b-c6aea48fb716.html)
- * [Book: Incorporated Man](https://www.amazon.com/The-Unincorporated-Man-audiobook/dp/B002C4A2SC/ref=sr_1_1)
- * [ID2020](<https://www.id2020.org/>), was not the technical requirements that were used to ecosystem, but rather helping governments understand needs (e.g., balance privacy vs. access and equity).
- * [Book: Learning Digital Identity](<https://www.oreilly.com/library/view/learning-digital-identity/9781098117689/>)
- * [Derek Parfit](https://en.wikipedia.org/wiki/Derek_Parfit), reasons and person, Star Trek Transporter
- * [Book: We are Legion We are Bob](https://www.amazon.com/We-are-Legion-Bob-Bobiverse-Book-ebook/dp/B01LWAESYQ/ref=sr_1_1)

Dead man's switch for identity accounts

Session Convener: Dean Saxe

Session Notes Taker(s): Sarah Cecchetti

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

How do we help families get access to digital resources of a deceased loved one?
Could we bind it to a password manager? Insurance policy?

If I want to have beneficiaries for my personal accounts, and be able to revoke that status, how do I do that? Is that the right way to think about it? Is there a better way to consider the problem space?

There are three buckets of services:

social media

online service accounts (Uber, AirBnB)

banking, health insurance, life insurance

Google has a service where if you don't login for three months, you can designate someone to get access.

Does it make sense to do this service by service? Can we centralize it in some way? Is there a clearinghouse that can reach out to all the digital services you use?

What about an escrow service?

What about MFA? Sometimes it's recoverable, or your beneficiary might be able to access your yubikeys, etc.

Onepassword has an "emergency kit" that is a QR code and yubikey you can keep in a safe deposit box so if you lose all your other factors, you can recover.

There are companies that do this. One is called Trustworthy. It's a service that gets your loved ones access to your digital life. You can list who has access to what. "Trust and Will" is another company.

What other ways can we mechanize this for people? Can we build it into the things they are already doing?

In the US, there is a protocol of events that get tripped off, and propagated to minimize fraud.

Could the US government notify online spaces as well?

Could the death certificate be a verifiable credential that could be presented to online spaces?

We don't know what Apple can or can't do in terms of allowing access to a phone, but Steve had an experience where Apple was able to take an apple ID that was not associated with a device and associate it with a device.

Could a beneficiary delegation be part of the onboarding for the device?

Inside OnePassword, Phil has a note called "when I die" that lists his retirement accounts and internet domains.

So much of this is dependent on the level of certainty of death. How do you walk this solution back if you're wrong?

This is similar to a problem that PillPack had. In Houston county, there are 2000 Maria Gonzaleses, and about 200 of them have the same birthdays. What happens if you mark the wrong one as dead?

Is there a way to express what Death Assurance Level (DAL) you have?

Power of attorney? Revocation of power of attorney that is revocable so you can do a mass multi-account recovery?

What about things you don't want your loved ones to have access to? Is this a policy problem?

MFA & Passkeys for people who have trouble maintaining possession of physical factors

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

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

This could be related to Account Recovery issue which could use IDPro body of knowledge article
<https://bok.idpro.org/article/id/64/>

All systems that require authentication of users share a common problem: users are human. Users forget or lose their credentials, lose, reimagine, break, or sell hardware with embedded credentials (e.g., a phone or laptop). Account access is lost when users lose access to an email address their account is bound to. In some systems, credentials expire and need to be reissued. The common theme is that users need alternative mechanisms to restore access to the accounts whose credentials are unavailable.

The following article establishes a framework for evaluating Account Recovery mechanisms and establishes recommendations for Account Recovery in consumer, education, enterprise, and government spaces by identifying the benefits and risks of common mechanisms. Given the variety of concerns – privacy, security, and access continuity - in different domains, the reader of this document is expected to apply the guidance herein alongside their domain expertise and judgment to design, develop, and deploy Account Recovery mechanisms for their online systems. Due to the intersection between Account Recovery actions and Customer Service teams, the author strongly recommends that the reader also consult the article “Managing Identity in Customer Service Operations” in the IDPro Body of Knowledge.

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

Based on the attached message, the discussion revolves around the challenges of password and multi-factor authentication (MFA) recovery, particularly for individuals with unstable housing or limited access to devices. The key understandings, outstanding questions, observations, and potential action items are as follows:

Key Understandings

- Password and MFA recovery can be challenging for individuals with limited access to devices or unstable housing situations.
- Current cloud providers may not offer adequate solutions for these populations.
- Government agencies or social workers could potentially help with identity reestablishment.

Outstanding Questions

- How can technology be adapted to make password and MFA recovery more accessible for these populations?

- What role can government agencies or social workers play in assisting with password and MFA recovery?
- How can trust be established with third parties for escrow services?

Observations

- NIST digital identity guidelines (SP 800-63A) mention application reference as a potential solution for identity reestablishment.
- Some participants discussed the idea of using a password manager, but this may not be a feasible solution for everyone.
- There is a need for a more inclusive and accessible approach to password and MFA recovery.

Action Items / Next Steps

1. Investigate the NIST digital identity guidelines (863A) for potential solutions to identity reestablishment.
2. Explore the possibility of integrating government identity providers or social workers into the recovery process.
3. Consider the development of a more inclusive and accessible approach to password and MFA recovery that accounts for individuals with limited access to devices or unstable housing situations.
4. Research potential escrow services or third-party solutions that could assist with password and MFA recovery while maintaining trust and privacy.

Notes from Matt MacAdam

Session 6, 2023-10-11 (Oct. 11, 2023)

Organizer: Matt MacAdam

More or less discussing what account recovery or MFA reset looks like if you don't have any devices.

TL;DR: You need server side biometrics or some kind of intermediary who can validate/establish your identity for account recovery.

(comments on US or foreign law are from laypersons and are not legal advice)

- Matt told a story about helping someone do their taxes. They get stuck not being able to complete MFA because the number in TurbTax was “four phones ago”
 - Unstably housed populations frequently lose/break/have stolen their phones, and frequently only have a single device (i.e. cannot recover on another device)
- Solutions discussed
 - “Legacy contact” similar to someone who can recover account in case of death. Trusted friend or relative can maintain account recovery.
 - Works well for some populations with stable social connections
 - Difficult to maintain over time for some populations (social worker moves to another agency, have a fight with friend)

- Solution for social service agencies: Have recovery go with the agency or role and not the person.
- Passkeys “help”—still the problem of MFA to bootstrapping a new device if you lose all devices
- Escrow of additional MFA keys
 - Who wants to assume the risk?
 - Escrow might only be second factor—no account access just from some kind of MFA reset.
 - Most populations aren’t likely to be targeted (no assets, poor credit). Possible exception: Populations often receive government checks which are often a target.
 - Who would do it? Local social service agencies? Government or private? Think of recovery as a “social good”
 - Government has some responsibility for helping people be able to function.
 - What if government agencies had an API into cloud providers for account recovery or MFA reset? Cloud provider could maintain ignorance of identity, government responsible for identity proofing. “Proof of human”
 - Privacy concerns if government can establish access to accounts.
 - US does not have compulsory decryption. Can social agency be compelled to recover account and provide access with a court order?
 - In the US agencies are not required to share information with one another. Social agencies could reject requests from other agencies? Consider recovery “privileged communication”
 - In any case recovery might be forced for intelligence gathering (e.g. without court order), but content obtained in this way couldn’t be used in a criminal trial. (comments based on current US law)
 - Server side biometrics
 - Quick and easy solution
 - US residents are generally resistant, but this is more socially accepted outside the US
 - Snail mail/postal service
 - Mail an MFA code
 - Many people receive mail at a shelter.
 - Needs to be longer so it can’t be brute-forced during transit time.
 - Voice or SMS MFA to a communal phone number (similar to receiving mail at a shelter)
 - Reduced security (maybe acceptable?)

- Some platforms may not allow the same phone number for multiple accounts.
- Other interesting questions/topics addressed
 - Are we talking about automated recovery or human assisted?
 - Generally human assisted—a delay is OK.
 - The type of service matters
 - Cloud providers don't care who you are. May not even _want_ to know. Makes any kind of identity proofing directly with the provider difficult or impossible.
 - genetic/biometric fingerprint key established at birth
 - Compromise is disastrous
 - NIST 800-63-a covers identity proofing
 - Login.gov has a concept of an “application advocate” or “referee” who can help with account recovery (not sure if I recorded this accurately)
 - Basically a mechanism where someone can help someone else with their account
- This problem has parallels with digital legacy/estate handling

SESSION #7

Wallet Security and IETF Attestation-based Client Authentication

Session Convener: Paul Bastian and Markus Kreusch, Bundesdruckerei
Session Notes Taker(s):

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

Presentation Slides: <https://nextcloud.idunion.org/s/abopwiPYdS3YNJW>

IETF Spec Link: <https://datatracker.ietf.org/doc/draft-ietf-oauth-attestation-based-client-auth/>

Github and latest version: <https://github.com/vcstuff/draft-ietf-oauth-attestation-based-client-auth>

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

- motivation through eIDAS 2
- regulated requirements and the existing tools with different technologies
- the three building blocks of device binding, user binding, wallet authentication
- the wallet attestation and the trust model
- presentation on the IETF Draft
- feedback on/open topics:
 - Does Wallet attestation need to be a client authentication method?
 - How to get nonces at the PAR endpoint?
 - Which method is best for replay attack prevention?

State of Idm Policy Interop

Session Convener: Phil Hunt, Gerry Gebel
Session Notes Taker(s):

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

Hexaorchestration.org <https://github.com/hexa-org>
<https://www.cncf.io/projects/hexa/>

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

Hexa Policy Orchestration (Hexa) and Identity Query Language (IDQL) were purpose-built to solve the proliferation of Policy Orchestration problems caused by today's hybrid cloud and multi-cloud world.

IDQL is a vendor neutral format for defining access policies and Hexa is the open source implementation of how IDQL can be translated into the bespoke formats of authorization systems.

This session shared some of the findings from the last two years of research and development.
Text from slides are copied here for convenience

slide 1 Hexa project

- A CNCF Open-Source Project
- APL 2 license
- <https://hexaorchestration.org> <https://github.com/hexa-org>
- Goals
- Translate IAM Policies across cloud systems into a common format (IDQL)
- Centralized policy review and administration
- Foundation for governance/audit, source of authority, change control/provisioning
- Support a wide eco-system BUT encourage consolidation of formats/languages
- Develop libraries and services that can be consumed by policy products*

slide 2 What's the catch

- Huge diversity of policies
- More dimensions than one might think
- Context matters (where/when) a decision is made
- Not just pass/fail, but what can Alice do?
- Understanding subjects vs. actions
- Roles can be
- Something a subject is or has
- A permission a subject gets
- Increasing complexity / capability

- Policy as Code, Testing, Governance
- Probabilities

slide 3 Fundamentals

- Types of languages
- Paradigms
- Use Domains

slide 4 Types of Policy Languages

Imperative

- Security policy administered through APIs that have specific set-points describing what users, or roles can perform what functions (Azure, AWS classic)

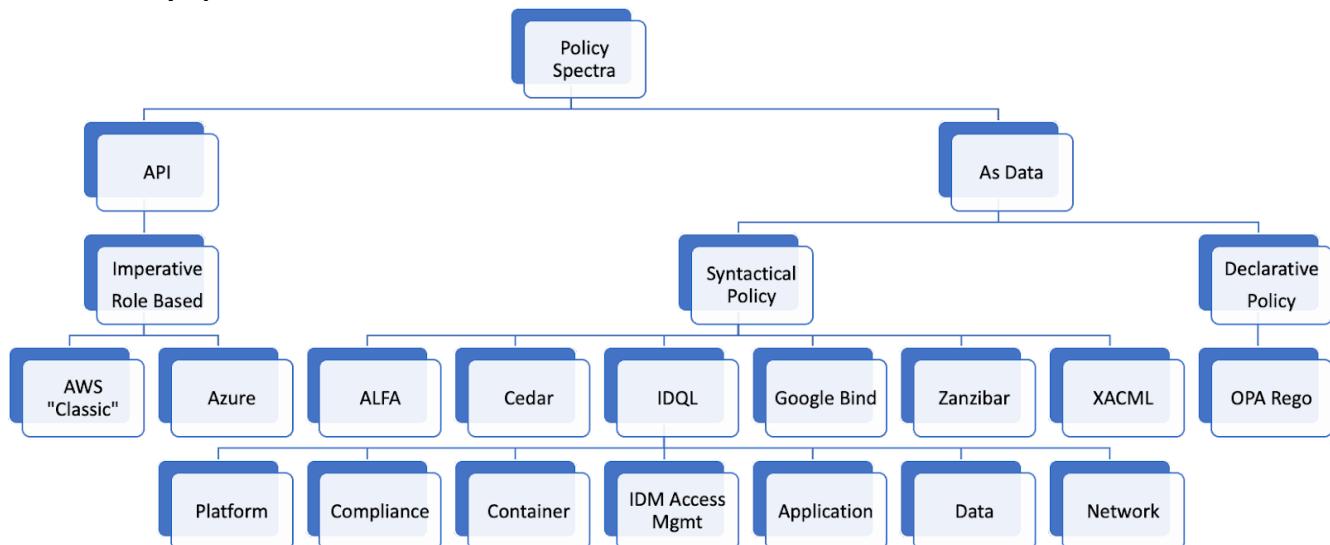
Declarative

- Open Policy Agent 'Rego' which

Syntactical somewhere in between

- policy "tuples" or rules deployed to policy decision systems
- Expressed in XML(XACML), JSON (IDQL), or other custom formats (ALFA, AWS Cedar)

slide 5 Policy Spectra



slide 6 Structural Observations

Every platform vendor has its own

- platform security model
- container security model
- Identity and access model

How should apps integrate with policy systems?

- How much should apps know about OAuth2, LDAP, SCIM, etc?
- Should apps be enforcement points by calling PDPs?
- Should apps depend on proxies or container security layers?

Where should policy be applied?

- Does it make sense to reprocess the same information more than once or even a hundred times in the same request flow?

slide 7 Observations - Practical

- No common APIs or model for implementing policies
- Different ways to distribute policies
- Policy applied to the resource (Google Bind)
- Policy applied centrally through a product (Amazon VPC/Cedar)
- Policy applied through bundles (OPA)
- Policy applied to specific products
- Different policies for different layers and components
- No common way to
 - Define actions, permissions, and roles
 - Identify subjects
 - Identify resources that policies are about

slide 8 Seems impossible, remember the 90's

slide 9 Hexa Project Objective

- IDQL defines common policy syntax format
- CNCF Industry Standard
- Syntactical representation
- Information model for identity and access rights
- Capabilities
- Benefits
- Unified administration, understanding, and auditing of policy in diverse environments
- Compliance evaluation and reporting across multi-tech, multi-platform applications
- Policy change control
- Improved tooling, testing, debugging
- Migration and Portability*

slide 10 IDQL policy tuple

Subject – Identifying the actor of an operation

- How to match the authenticated subject (role, group, sub)?

Action – What action is enable / forbidden

- What operations, permissions, or roles

Resource

- What object is the policy referring to

Condition

- What relationship or attribute condition must be true?

Scope

- What scope of data can be accessed?
 - SCIM/LDAP the attributes that can be read / modified can be set
 - An additional qualifier for SQL queries (e.g. US residents)

slide 11 Translation challenges

- Roles can mean
 - Something a subject is or has
 - Something a subject is granted or authorized (action)
- Platforms can conflate action with resource
 - The resource URN includes the action
- Binding
 - Policy can be applied per object or per API
 - Many systems have an API but not a policy format
- Non-binary result
 - OAuth2 scope
 - Return list of authorizations possible for an entity to support application UI workflow

slide 12 What we've done

Hexa Orchestrator proof of concept

Demonstrate ability to retrieve, map, and set policy

- MS Azure
- GCP Bind Policy
- AWS Cognito and Cedar
- Open Policy Agent (OPA) IDQL interpreter

slide 13 What we're thinking

Hexa Orchestrator Open-Source Project

- Open Libraries to build products on:
 - Policy Definition
 - Policy Mapping & Policy Provisioning API Library (GoLang)
 - Policy Server Web API
- Policy Admin "demo"
 - Web UI demonstrating functions of Orchestrator
 - Demonstration Apps

slide 14 Summary

- Captain Obvious moment
- Authorization and Policy Management are difficult!!
- We are starting to learn what is possible, after a couple of years of trial/error and research
- Look for more sessions on AuthZEN and Hexa/IDQL this week
- Your feedback and participation is welcome!

Trust Spanning Protocol (TSP) Deeper Dive

Session Convener: Wenjing Chu, Sam Smith, Drummond Reed

Session Notes Taker(s): Wenjing Chu

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

The link to the slide deck:

https://docs.google.com/presentation/d/11oC06aIYI4VtFBevE5f8KE5aZnNEU9GPy_Oek52SetA/edit?usp=sharing

To follow the ongoing work of spec development of TSP, visit ToIP TSP Task Force wiki:

<https://wiki.trustoverip.org/display/HOME/Trust+Spanning+Protocol+Task+Force>

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

This session is a follow up from yesterday's Trust Spanning Protocol for Muggles session. If you are new to this topic, I suggest you go view yesterday's intro session first:

https://docs.google.com/presentation/d/11oC06aIYI4VtFBevE5f8KE5aZnNEU9GPy_Oek52SetA/edit?usp=sharing

The deeper dive session walks over these technical topics:

- The big picture: overview diagram explaining TSP
- The message envelope (ESSR envelope): defines in detail how the envelope is constructed. And also introduce a notation to simplify representation.
- Nested messages: explain how nesting works and notation to represent nesting succinctly. And discuss what nesting does for correlation privacy.
- Routed Mode - the bulk of time is spent in explaining how endpoints can use intermediaries through the routed messages for strong correlation privacy.
 - Step by step explanation of A - Intermediary_alpha - Intermediary_beta - B routed pattern.
 - Explain the correlation privacy protection properties
- Lively discussions on finer points of the new notions of security by ESSR, by routed mode of TSP and others.

Thanks to all participants who followed us through the technical details of TSP.

To follow the ongoing work of spec development of TSP, visit ToIP TSP Task Force
wiki:<https://wiki.trustoverip.org/display/HOME/Trust+Spanning+Protocol+Task+Force>

There is a question about how TSP can support for more than two parties.

Answer: TSP is designed to support more than one, two, or fixed number of parties in the communication. Such multicast/broadcast mode is an extension to be spec'd shortly after the main spec. It can have two options:

- Managing a list of 1-to-1 TSP relationships. Note that TSP does NOT create any “connections” - if you heard words like channel or connections or sessions, they are informal use to convey an analogy. All TSP messages are async and can be standalone. So the relationships are all there need to be. It is therefore very practical and low cost to manage N x relationships.
- Use a new class of crypto algorithms that support N parties - which is for future study at this point.

One can also use TSP N member relationship as a “control” medium, and use this to control or bootstrap another multicast (e.g. video) scheme. This is very easy to do. The only cost is of course you would lose the correlation privacy for the video streams because they are not carried in TSP.

W3C VC-Edu Plugfests! Credential rendering! Trust Registries! Schemas! W3C VC-EDU Task Force

Session Convener: Kerri Lemoie, Simone Ravaioli, Dmitri Zagidulin
Session Notes Taker(s): Kerri Lemoie

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

<https://w3c-ccg.github.io/vc-ed/>

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

Plugfest Info:

Recording of Plugfest 3 Demos: <https://us06web.zoom.us/rec/share/8cmLQg-jNI4B3DHbZm6LFM1dlxuy750NSIBk0A9QRqPyzXcWkL31ICOL-VNVT7Ue.Ele5HKMYxy385ddy>

Passcode: X6K.TJ?T

Individual videos submitted for demo day are posted on the project site:

<https://w3c-ccg.github.io/vc-ed/plugfest-3-2023/>

Presentation deck with embedded videos:

https://docs.google.com/presentation/d/1GhkDA7OdRZImjeLBU_osOw7jLz6TE3IJBuWbsVkJGwM/edit?usp=sharing

Discussion:

Plugfests have advanced understanding of protocols & standards

In Japan students print out diplomas at vending machines and then present them. US has less trust - official sealed transcripts

Discussion about use of VCs - like degree or employment credentials -how some are implementing and use cases.

“Atoms of learning” - degree->course->then other credentials can inherit the perceived value of degrees and courses.

What identity do students use in credentials - do we need to store DIDs in VCs? Discussions about privacy and cross-correlation.

What are next steps for plugfests? Please join vc-edu email list.

Standards-Based Digital Credentials Flavors Explained

Session Convener: Kaliya Young and Lucy Yang
Session Notes Taker(s):

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

Session Slides:

https://docs.google.com/presentation/d/1HgBUibPTEahD6CLRqJhGxcfAZm_4DXc2brv-dMK2e9o/edit?usp=sharing

Download Paper:

https://medium.com/@identitywoman-in-business/new-paper-and-infographic-on-flavors-of-digital-credentials-released-b9b6ec5b95af?source=friends_link&sk=d74dfb20f4750e159b5b259424b7edce

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

The “[**Standards-Based Digital Credentials: Flavors Explained**](#)” (Whitepaper), which aims to provide a simplified but technically-accurate overview of the main flavors of standards-based digital credentials (for humans) in the market today to inform policy, business and technical decision makers sitting on the fence regarding what to use for their implementations. **Accompanying it is an infographic** that provides a high-level overview of the four major flavors and two emerging flavors covered in the paper.

One important note from the discussion:

- Provide more clarity about mDL vs. mDOC.

VCs over Ceramic

Session Convener: Golda Velez and James Pham and Aaron Goldman
Session Notes Taker(s):

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

[Ceramic network](#) and ComposeDB: <https://composedb.js.org>

[Demonstration repo for Verifiable Credentials over Ceramic](#)

[Slide deck from session](#)

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

First, quick overview of Ceramic network

- content-addressed by genesis commit, mutable final state
- DID controllers, can delegate control by CACAOs
- pubsub topic channels
- Composable data with shared feed by schema
- GraphQL interface

Comparison of signed stream instance documents with signed verifiable credentials

Overview of solution simply storing extra signature line and rearranging into a valid credential format

See demonstration repo for details.

Further thoughts:

Given the data model Verifiable Credentials use, individual credential instances can be stored anywhere - from offline storage on a hard drive, to traditional databases controlled by companies who rely on Verifiable Credentials, to smart contracts on a blockchain, to more performant peer-to-peer storage, and everything in between. Why, then, would developers choose to store verifiable credentials on Ceramic?

Since Verifiable Credentials are flexible enough to describe a seemingly limitless set of circumstances, yet standardized enough to be able to easily verify the proofs included therein, developers who build on Ceramic not only benefit from the performance and querying capabilities offered by ComposeDB but can also consume verifiable credentials from other issuers and communities built on Ceramic.

Create Your Own did:webs

Session Convener: Markus Sabadello and Lance Bryd
Session Notes Taker(s):

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

See here:

<https://github.com/peacekeeper/did-webs-iiw37-tutorial>

https://dev.uniresolver.io/#did:webs:peacekeeper.github.io:did-webs-iiw37-tutorial:EKYGGh-FtAphGmSZbsuBs_t4qpsjYJZqvMKluq9OxmP

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

PDP & PEP vs. AS/RS Smackdown

Session Convener: Eve Maler, Allan Foster, and Justin Richer
Session Notes Taker(s): Jin Wen, Mark Haine, Alan Karp, Eve Maler

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

[Federated Authorization for User-Managed Access \(UMA\) 2.0](#)

[Presentation PDF](#)

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

[Notes from Jin](#)

[Notes from Mark and Eve](#)

[Notes from Alan](#)

Notes from Jin

Key Understandings

- PEP (Policy Enforcement Point) and AS/RS (Authorization Server/Resource Server) models are not incompatible; they can complement each other in different scenarios and use cases.
- The distribution of policies and attributes across multiple PDPs (Policy Decision Points) is a challenge, especially when dealing with real-time data as it can go stale.
- Transparency for resource owners and data subjects is crucial in authorization systems.

- Governance and accountability are essential aspects of distributed authorization systems.

Outstanding Questions

- How can the balance between centralised and distributed authorization systems be achieved?
- How can real-time data be effectively managed and enforced across distributed PDPs?
- How can transparency be ensured for all parties involved in the authorization process?

Observations

- The discussion highlights the complexity of authorization systems and the need for a more comprehensive approach to address various challenges.
- The participants acknowledge the importance of considering the real-world implications of authorization decisions and the need for a more flexible and adaptable approach.
- The conversation also touches upon the need for better tooling and mechanisms to handle governance in distributed authorization systems.

Action Items / Next Steps

- Explore the possibility of combining PEP and AS/RS models in different scenarios to achieve a more comprehensive authorization system.
- Investigate methods for effectively managing and enforcing real-time data across distributed PDPs.
- Develop strategies for ensuring transparency for all parties involved in the authorization process.
- Collaborate with industry experts and working groups to address the challenges and questions raised in the discussion.

Notes from Mark and Eve

Question: Can the RS refuse access regardless of an AS PEP decision?

Observation: there are PEPs all the way down

The Nomenclature is the same - somewhere a decision is made

"The RS always has the right to refuse service" (just like the RP does)

Policy is checked at PDP

At the UMA AS it makes a policy decision (authorization assessment) and creates a token
(This AS could front a wholly separate actual decision point)

Temporality is the biggest challenge

- token request time
- token evaluation time
- when various evaluation inputs are collected vs. assessed

Many layers including edge layer, App layer, and it is often highly app specific

Also need to consider Accountability, Liability, Responsibility, Authority, Traceability (see [UMA Federated Authorization](#) for one way to spec out "separation of responsibility and authority")

Shape of the problem is a calculus of decisions to provide auditability

**** Insert diagram of Set theory **** Justin? (see [slide 44 in UMA 101 preso](#))

This is all hard because of it being so app specific

Is there a contracted relationship between domains?

**** insert UMA Parties Diagram **** (see [slide 5 in preso](#))

What is the route from business logic to policy description?

Are we delivering least privilege?

Governance is hard across multiple pieces

But we don't have to "toolify"

Parties in the real world

- need to be considered
- promises between parties can be codified in policy

Who is the owner? (is owner loaded .. better to say "whoever it is about")

Keep "Resource Owner" language? - In GNAP it's "End User" – the RO can be an org entity or a person, but the RqP is always a human

Keep "Requester"?

We have seen some migration to "edges" - PDPs in various places

- AS/RS/App

How do we get policies to the PDP?

- Policy and Attribute distribution even
-

WIMSE - IETF - Workload patterns

- join mailing list wimse@ietf.org

This has long been a focus on AuthN

Generic requirements

- Multiple signals
- Multiple decisions

Time is the squishy bit ("temporality" as above)

Previously about "Risk" - now about "Anomalies"

The broader picture of authentication + authorization is signals + decision-making

Signals can be collected at anytime and used downstream (but may go stale)

Decisions can be made by each successive entity

There is always a “stack” of policies that need to be taken into account - legal, operational, access... (see discussion of this in [UMA Julie Adams paper Section 3](#))

4 Things (key moments) - Alan Karp has written on this - see diagram and explanation below

- Identification
- AuthN
- AuthZ
- Access

2 places

- Requestors
- Providers

Temporal

- At Access time
- Before Access time

Move to micro events? (*see diagram just above*)

AuthN was an optimization

Is everything AuthZ an event?

AuthN is proof of presence

Is AuthN just a PIP? It generates input into decision-making

Taxonomy is still a problem

We need a glossary - there is one at ToIP (*activity seems to be centered [here](#)*)

“PDP” actually pre-dates XACML by 30 or so years

Now it is not “yes/no” answers it has become “what can I do?”

So PDP

- decides
- creates RAR blob (perhaps)
- sticks it in a token
- Passes it to RP
- that becomes input to local PDP

Notes from Alan

Ignore the blue headings; they make sense in the context of the talk.

Where and When

| Step | Virtual Problem | | Real Answer | |
|--------------|-----------------|-----------------|----------------|-----------------|
| | Where | When | Where | When |
| Identify | User domain | Before request | User domain | Before request |
| Authenticate | Service domain | At request time | User domain | Before request |
| Authorize | Service domain | Before request | User domain | Before request |
| Decide | Service domain | At request time | Service domain | At request time |

You can choose when and where
you authenticate and authorize

There are 4 steps in the access control process.

1. **Identification:** Assigning a responsible party. Often includes vetting the party with biometrics, presentation of government documents, etc.
2. **Authentication:** Proving that an entity (usually a process) is allowed to act on behalf of a responsible party.
3. **Authorization:** Assigning rights to an authenticated entity.
4. **Access Decision:** Deciding whether or not to honor a request.

Each of these steps can be done at one of two places, the requester domain or the resource domain, at one of two times, before the request is made or at the time of the request. It only makes sense to do the identification in the requester's domain before the request is made. It only makes sense to make the access decision in the resource domain at the time of the request. There's more flexibility for the other two steps.

In an authentication-based approach (NBAC), say with ACLs or RBAC, both the authentication and the authorization are done in the resource domain at the time of the request. For example, the PEP forwards the request and the invoker's authentication to the PDP, which uses that information to decide whether the request is authorized by some policy. The PDP returns the access decision to the PEP.

In an authorization-based approach (ZBAC), such as capabilities, both the authentication and the authorization are done before the request is made in either the requester's or the resource domain. For example, the requester could authenticate to the resource's AS and get back an authorization token. On invocation, the RS validates the token against the request to make the

access decision. However, once an entity has such a token, it can make further authorization decisions in its domain by delegating a subset of its permissions to another entity that it has authenticated. In this case, the authentication and authorization steps are both done in the requester's domain.

It often makes sense to combine PEP/PDP with AS/RS. In one system using certificates as capabilities, the resource's AS was given a capability that it could delegate to an authenticated entity. That entity's request was received by a PEP that validated the signatures. If the request passed that test, it was sent to a PDP that verified that the delegation chain was valid, e.g., nobody delegated permissions they didn't have. If the request passed that test, it was passed to the RS that made any application-dependent decisions, such as whether the request exceeded some limit.

The Synchronic Web

Session Convener: Thien-Nam Dinh

Session Notes Taker(s): Thien-Nam Dinh

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

<https://arxiv.org/abs/2301.10733>

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

- Briefed technical context and considerations of general purpose USG blockchain infrastructure
- Briefed data structure and mechanism behind the scheme
- Received feedback on identity implications
 - constraints of existing registry-centric DID formulations
 - potential application of did:merkle
 - discussed options for DID docs and identifiers





OVERVIEW

Development of scalable blockchain infrastructure to support **cross-platform** definition of self-sovereign identity

Core Infrastructure

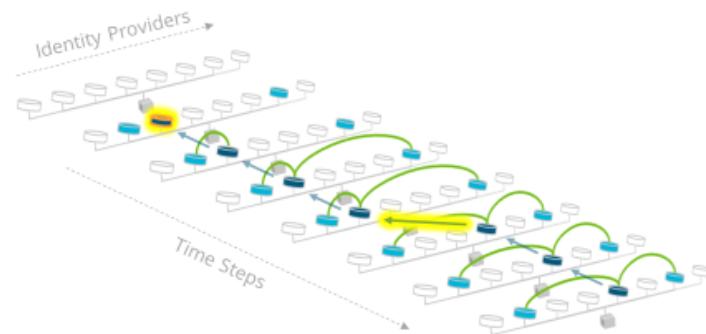
- Supports arbitrary number of clients
- Resistant to tracking and censorship
- Provided as a free and public good

Identity Application

- Optionally controlled by subject
- Capable of transition between providers
- Expressible in Turing-complete code

Status

- Infrastructure in development
- Other applications in development
- Identity application in ideation phase



THE BLOCKCHAIN

- Payload size: 256 bits
- Block time: 1 second



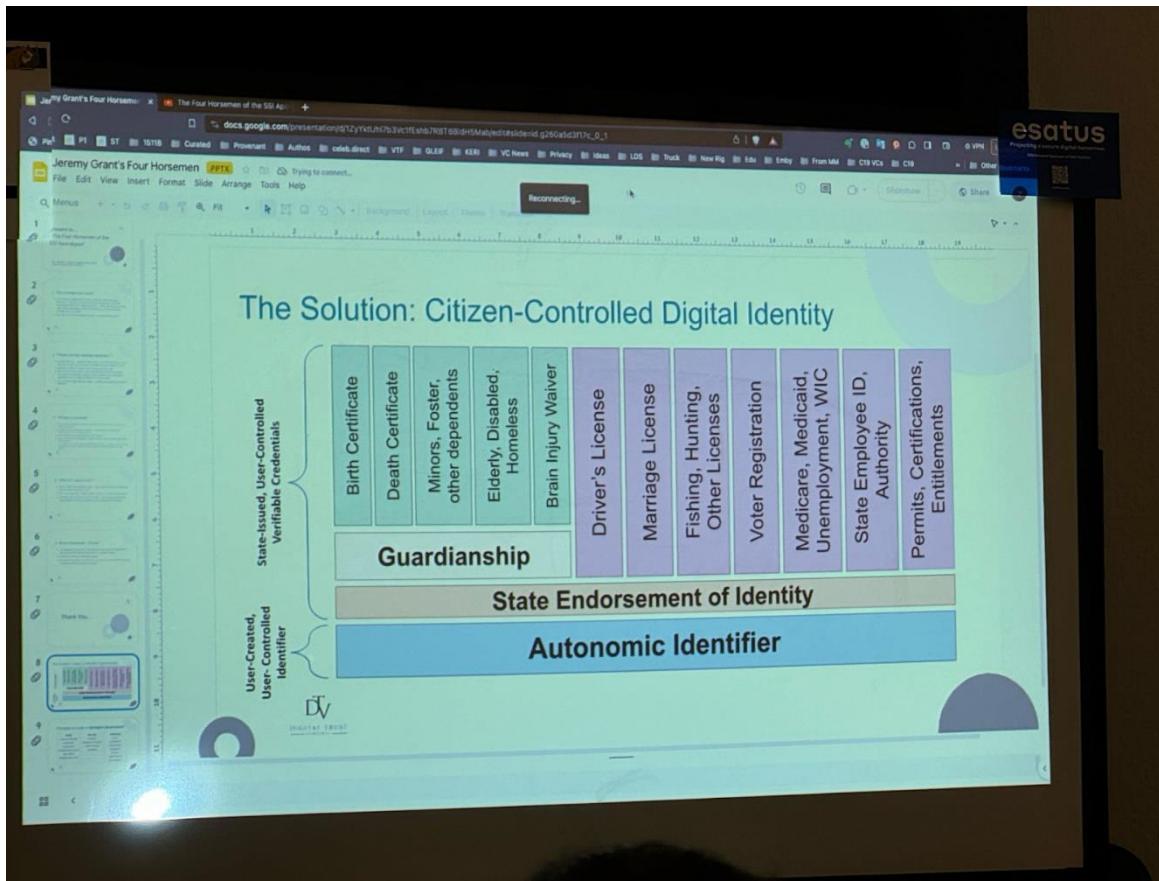
The Solution: Citizen-Controlled Digital Identity: An Alternative to the Mobile Drivers License

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

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

mDL; Autonomic Identifier; Credentials; Individual Privledges

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



Online Travel ssi + data privacy - DIF SIG + ToIP TF Sig Work

Session Convener: Neil Thomson (QueryVision)

Session Notes Taker(s): Neil Thomson

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

Presentation Slides: [Hospitality and Attractions - Poster Child for SSI](#)

Links

- DIF Hospitality SIG
 - [DIF Page](#)
 - [Mailing List](#)
 - Meetings: Weekly Thursdays, 10 to 11 AM (EST) [Zoom](#)
- ToIP Attraction Pass TF
 - [TOIP TF page](#)
 - Meetings: Tuesdays every two weeks (Oct 24): 08:00-09:00 PT / 16:00-17:00 UTC
[Zoom](#)

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

The DIF Hospitality SIG & ToIP Attraction Pass TF overlap, which feature many of the same people participating, who are first and foremost experts in the business of hospitality and attractions and secondly on technology. The Hospitality group is also working on developing a extendable, comprehensive **Travel(er) Profile** to cover the many aspects (which are all PII/PD class information) of travel, food, lodging, activities, medical/health, faith and lifestyle needs. It's a super set that applies to anyone who travels.

While travel, use of hotels, restaurants is a luxury for many, the digital skills level of travellers, covers a very wide range, including many who are digitally illiterate. So making travel a seamless experience for anyone who travels, will have a lot in common with the mainstream of those using online services and personal devices.

The main thrust of the presentation is that Hospitality, Attractions, entertainment and sports bookings, which almost entirely online in 2023 share a lot of the same centralization, interop and data sharing problems as the large social media platforms.

The industry experts see a major opportunity to streamline/simplify the complexity of building travel itineraries for individuals, families and groups, for both the traveler and the industry operators and providers.

As there are many types of operators and providers, in every country and jurisdiction, there are major issues with trust and financial risk as many relationships maybe for a one time trip itinerary. For travelers and concert goers, there are issues with trust of ticket sellers and resellers for both the purchaser and the seller.

The sheer volume of individual services, events and activities in even a one week itinerary are none trivial, with the need to coordinate sequences of events, with constant rebooking, delays, cancellations, etc. This highly dynamic environment is fragmented with many informal models, with financial risk, plus a lot of “service fees” paid to the larger players, in much the same way that an online seller runs into when selling through the Amazon’s of this world.

There were several of the attendees who expressed interest in participating in the related DIF and TOIP groups, so links to the groups and meetings have been included in the minutes

SESSION #8

US Healthcare on Trial: Decentralized Identity Use Case Assessment Framework

Session Convener: Sophia Goeppinger

Session Notes Taker(s): Sophia Goeppinger

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

For further details on the assessment framework or access to the slides presented during the session, please reach out to Sophia Goeppinger at sophia.goeppinger@student.unisg.ch

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

Part I: Introduction and framework presentation

First, Sophia set the stage, giving an overview of the US healthcare system's data flow problems (clinical data flow, product information data flow, and reimbursement data flow). Then, she segued into presenting an assessment framework that she developed over the past months that helps US healthcare stakeholders assess the amenability of a certain use case to decentralized identity. The framework seemed to resonate extremely well with the audience.

Part II: Q&A

Have you already tested the framework? - Jared Jeffery

That is the current research stage. Against that background, Sophia Goeppinger asked session participants to refer to her healthcare stakeholders that could be interested in testing the model. Jared Jeffrey and BC Gov. showed interest.

Adrien Gropper commented that he saw how healthcare stakeholders in the patient identifying business wanted to implement it but nothing happened because of the perverse incentives.

Decentralized identity would have caused two things:

1. Raises the question whether it is individually or institutionally focused. People did not understand that
2. Once you do that the value proposition is clear but it implies that people build consent and transparency on top of the solution. And as soon as people realize that once they open the can which now provides individual consent/authorization and provides a way for the regulators to mandate transparency they shy away

In healthcare it is not just about perverse incentives but guardrails that they set on purpose and paid money to do as with decentralized identity you (a) attack the system's validated system and (b) corrupting their data silo integrity (poking a hole in it).

Can the framework be used to justify a use case across the own organization?

- Theoretically yes. Here the trust boundaries come into play and whether the current solution is expensive for you - and it will be easier to get such a project off the ground as you do not need the involvement of the entire healthcare "mafia." - Sophia Goeppinger
- It is hard to justify decentralization within an organization as you can just go with centralization. - Stephan Baur
- That is what he referred to with that you have to be clear whether the solution is institution- (= any kind of federation) or patient-centric. - Adrien Gropper

Who is the target audience for filling out the framework?

- Both the tech and healthcare knowledge division of all kinds of healthcare stakeholders - Sophia Goeppinger
- Target the regulators and not the participants because of the perverse incentives, such as in India etc., i.e., in places that are constitutional democracies (have some trust in the regulatory process) but really need it and only then come to the US. Regulators know how to best implement it - Adrien Gropper (but regulators participated in the framework creation - Sophia)
- Disagrees with Adrien as regulators have to listen to the healthcare industries and the healthcare industry can actually influence regulators - Debbie Bucci

How to broaden the application realm of the framework:

- Apply it to other industries beyond healthcare (education) - Judith Fleenor
- Use it as a discussion base with other stakeholders to analyze what can be done together - Stephan Baur
- Talk to high trust to get this implemented - Jared Jeffery (Stephan Baur's comment: They are not open to decentralized identity)

It is great that the framework considers that it is not just about the technology but all stakeholders need to have a buy-in and need to know what is in for them as it will destruct their other business model. - Judith Fleenor

How does the framework take the return on investment (ROI) into account for a certain use case, in particular as the return on investment might only show after a few use cases? - Judith Fleenor

The framework does not take the ROI into account as this framework is too applied at an earlier stage as it asks about the application of decentralized identity as a concept/meme/genre and not the specific implementation such as whether through blockchain or KERI. - Sophia

Further research ideas:

- Where do people stop in the framework?
- Look at past use cases that passed and whether the framework applies as these people will not make up stories (simpler than finding new use cases)
- Benchmarking study based on results

IETF Status List and other Revocation methods

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

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

Presentation Slides: https://www.linkedin.com/posts/paul-bastian-1970b1195_jwt-cwt-status-list-presentation-0923-activity-7112832940853587969-XECr?utm_source=share&utm_medium=member_desktop

IETF Specification: <https://datatracker.ietf.org/doc/draft-looker-oauth-jwt-cwt-status-list/>

Github and latest Version: <https://github.com/vcstuff/draft-looker-oauth-jwt-cwt-status-list>

Davids slides:

- <https://nextcloud.idunion.org/s/7BXEeMKEJmweX67>
- <https://nextcloud.idunion.org/s/eJQZ6go5okQHMp3>

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

- Presentation on the basics of Status List
- Motivation to deviate from w3c status list (JWT is more approachable container, multibit, no JSON-LD, IETF more respected)
- discussion on the privacy issue of Verifier tracking
 - there is probably no good solution
 - the problem might not be as big/real
 - the problem may be mitigated by shorter lifetime of credentials
- information on the sizes for various revocation rates/entities
- David presented slides on comparison of approaches for mDL revocation, especially bloom filters

Blockchain-Free Proof of Personhood

Session Convener: Brad deGraf

Session Notes Taker(s): Drummond Reed

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

<https://nao.is/>

<https://greencheck.world/>

<https://memri.io>

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

Brad began by explaining that some of the large scale issues facing humanity are **cooperation failures**.

So we need tools to allow us to cooperate at scale. To do that, we need strong [proof of personhood](#).

Brad then showed how the Greencheck site uses links to social accounts to validate personhood.

There are different competing validation roots. Each group can choose to trust other groups. Each person in a group can be validated back to the roots in that group.

Brad explained that it is done through existing relationships and known people so that it can get this type of system going.

The more links you have to verify an individual, the stronger the confidence that it is a real person.

The proposed solution does NOT require having only a single identity. But there are ways to spot that kind of deception.

Brad said this is all currently Web 2 technology on Orango DB. All of your events are validated when you interact with this system.

Brad's goal is to make this a public utility that is cooperatively owned and governed. This would make a good utility for many others to use.

The goal is not to make it a fully Sybil-proof solution.

The privacy issues was raised if the network graph database is open; all the connections can be seen/inspected. Brad said that the goal was to figure out how to make it more privacy-preserving.

Ed and Brad discuss that DAOs have a big problem with [Sybil attacks](#). Brad believes that personal relationship graphs can be the answer.

Brad described how much concern there is among large funds saying, “All hands on deck to figure out what the best thing to do to help the planet.” Those networks need really efficient ways to research and select the best solutions.

It was asked what other solutions are being offered for proof of personhood. Drummond mentioned that Vitalek Buterin [recently published an essay on the topic](#) in response to Worldcoin.

The question was brought up about how easy it can be made for people and how it can be inclusive for people who are not into tech or do not have access to resources or who have been excommunicated from a community. Brad said that he does see this as potentially a highly scalable community.

It was agreed that user support would be required.

There were more questions about determining the uniqueness of a person within the network. Brad explained that one factor is unique control over social accounts. Brad believes that proof should be captured as a verifiable credential.

ChatGPT Steve is working on a network-based dynamics for determining a “probability of humanity”.

Norbu brought up how severe an attack vector it can become for a person if for example their Facebook account is hacked. So there needs to be a strong recovery process.

An appeal process was also suggested.

To decentralize the process, Brad suggested Holochain.

Brad talked about apps and benefits of this general approach:

- Contact lists
- Group petnames

Serverless, Data baseless, Programmable, Smart Wallets (PICOS)

Session Convener: Phil Windley

Session Notes Taker(s): Phil Windley

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

<https://picolabs.atlassian.net/wiki/spaces/docs/overview>

[https://www.windley.com/archives/2023/03/monitoring temperatures in a remote pump house using lorawan.shtml](https://www.windley.com/archives/2023/03/monitoring_temperatures_in_a_remote_pump_house_using_lorawan.shtml)

<https://solidproject.org/>

Slides:

<https://www.dropbox.com/scl/fi/d23ha1soskjotwsq9ixeb/Picos-and-Helium-IIW.pdf?rlkey=idvocdwgi9qvcj98ptcvengbp&dl=0>

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

We discussed how picos work using a temperature monitoring system based on Lorawan as a motivating example. We discussed how picos might work along with Solid pods to build a system for having products intermediate their own customer service transactions. The references provide more detail.

Are there too many identity.orgs? Could we consider how to accomplish our goals w/less of them

Session Convener: Kaliya Young

Session Notes Taker(s):

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

Kaliya was inspired to put this session up on the wall because someone before opening circle told her about yet another identity foundation that was spinning up.

The session started out with a brainstormed list of .orgs in the space. (see below)
It wandered through some interesting conversations.

Who Does What? Swim Lanes?

Who Listens to the business side of things

Can business world in this community be more helpful / coherent

Formation Processes? Governance?

- Supply-Demand?
- Pipeline of Members
 - Specialization

What are our goals?

Digital ID Capabilities

Human Centric

Time is a trade off between speed of innovation and consensus

Where are the standards in the life cycle of maturity

Self-organise better

INFORMATION is required and it has to be well Structured

Our VALUES - *We are not enabling the surveillance state.*

Industry Associations/Standards

- Kantara Initiative
- OpenID Foundation
- Decentralised Identity Foundation
- Trust over IP
- FIDO Alliance
- Secure Identity Alliance
- Chain Agnostic Standards Alliance
- Content Authenticity Initiative
- Open Identity eXchange
- IDCommons (dormant)

Professional Associations

- IDPro
- IAPP
- ISC2

Lobbying

- Better Identity Coalition
- Web3ID

European Things

- eIDAS
- ETSI

International SDO

- W3C
- IETF
- ISO
- ITU-T

- IEEE

Open Source Projects

- MOSIP
- Hyperledger
- OWF

Travel

- IATA
- ICAO
- SITA

International Organizations

- WISIS
- IGF
- World Bank ID4D
- UNDP
- UNHCR
- OECD
- GIZ

Privacy Groups

- World Privacy Forum
- EPIC
- ACLU
- FPF

Flows of Money

- Government
- Large Multinational
- Foundations
- Corporate Members

Ozero - AuthN in Seconds - Removing Manual OIDC Config

Session Convener: Dick Hardt

Session Notes Taker(s): Mike Schwartz

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

<https://github.com/hellocoop/hello-nextjs-starter>

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

- Hello is the easiest way to implement social login ever...
- The consent prompt from the IDP (e.g. Google, FB) will specify “Hello” (not the end application)
- Monetization strategy is based on the release of verified claim. Email claim is free.
- Don’t use the Wifi projector... it’s super laggy
- Stay tuned for Agama Lab project that calls Hello

Hello makes it easy to deploy an IDP for a developer. Fixes things that drive developers crazy, like changing redirect_uri, getting credentials, and configuring the IDP.

Users choose from social login providers that Hello supports.

Quickstart flow starts up local web server, so it can communicate with Hello, and communicate back to developer local env.

Separated the idea of development redirect_uri from production redirect_uri. Dev redirect_uri's are only available for your organisation (e.g. localhost).

Client does not have to manage keys, to avoid complexity.

Omri raised questions about how to export user data?

Can you get a bulk delivery of data? Importing data one record at a time is very slow.

Is it hard to say goodbye to Hello? You should have a verified email address. Hello will use the sub--so email might change. Migrating off Hello will require account recovery.

Hello verifies the email. App needs to check email (like other social providers) to see if it changed.

Hello has an update profile which the app can redirect for refresh.

Experiments with JSON-LD payloads secured by JWS vs Data Integrity

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

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

See here: <https://medium.com/@markus.sabadello/json-ld-vcs-are-not-just-json-4488d279be43>
<https://github.com/peacekeeper/json-ld-vcs-not-just-json>

World Coin: It's Privacy Impacts

Session Convener: Shin'ichiro Matsuo
Session Notes Taker(s):

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

Time Table

- Introduction (5 min)
- Very high level overview of World Coin (5 min)
- Brainstorming (35 min)
 - What is World Coin's true intention and business model
 - Potential Privacy Impacts
 - Incentive mechanism
 - Governance
- Create a list of privacy impacts (10 min)
- Wrap up (5 min)

Discussion Issues

- What is World Coin's business model?
- A list of potential privacy impact
- Is the incentive mechanism by giving coins appropriate?
- Governance
 - Who regulate?
 - Transparency
 - Technology
 - Organization
 - DAO?
 - Technology Assessment?

- Protocol
- ZKP?
- Implementation
 - Side Channel
- PIA
- How to facilitate healthy conversation with WorldCoin
 - No Contact Information
 - No list of names in the website

What Should DIF (Decentralized Identity Foundation) do for interop?

Session Convener: Brent Shambaugh

Session Notes Taker(s): Brent Shambaugh

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

I [Brent Shambaugh] outlined the challenges that were occurring at DIF. should the interop group exist? What was its original purpose?

what does it mean to move

maybe the casting of interop, artificially creating silos....more silos than is necessary behind different brandings....

there are a lot of reasons good and bad why things get siloed....people writing json and byte code...enough economic incentive...to keep it separate....

the incentive structure behind the grant seeking....the entire industry built behind anything real....just use jwts....

bearer token style...if you could get dids that report to the sameyou have the same thing....if you have 100 block

it seems to me that dids are like the xhtml of 2023.

the results should be open ended....nice to have a schema....going to make up some word...and we are going to use the same word....use a ... having a shared vocabulary....LLM superseded formal logic....OWL

history is a good thing to maintain even if the educational provider, wallet provider, and blockchain go away.

Augmenting OID4VC with DIDComm

Session Convener: Sam
Session Notes Taker(s):

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

DIDComm overview: <https://www.youtube.com/watch?v=TBxWgNmsnvU>

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

UX for Privacy: Questions not Answers

Session Convener: Alan Karp
Session Notes Taker(s):

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

<https://eamonn.org/seven-hard-privacy-ux-problems> is the basis for the discussion - this is not the official position of Google

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

We went through the question in the linked blog post and discussed each one. We spent more time articulating the problems associated with each question, including if the question itself made sense.

1. What exactly is good consent, and how do we make sure users are giving it?

There is implied and verbal and written consent. An example was given of consent for massage therapy, where customers need to be persuaded to make a full disclosure to avoid injury

What is good consent? How can the UX create a meeting of minds?

2. How can we give average, non-technical users the agency to manage the trade-off between privacy and functionality, given how insanely complex the data systems and products are?

Can we do informed consent given the asymmetry of information?

With AI you can't even predict how the organisation might use it. And what we tell you today may not be true tomorrow. And big organisations may not know how they use the data they hold.

Privacy is not about the data itself but it is about the boundaries.

It is safer if the data comes to the algorithm rather than giving data to the algorithm

What is the cost of the data that I'm giving you? I get a benefit in return for allowing you to cross the boundary.

What is good consent? Consent is a "dark pattern".

The entity can co-manage the data. Privacy is only required when you as a node share it with another.

We have built for security but can we also build for privacy.

3. How do we measure whether we are meeting people's privacy needs and expectations? Can we make these measurements in a way that is actionable in informing how we change our products?

What about empowering the vulnerable.

"I have nothing to hide". Incumbent on the others to provide here privacy.

Elevating privacy for the vulnerable can perversely also highlight who is vulnerable

We need a 3d matrix of systems of privacy.

There is a tendency to adopt the lowest common denominator - to do the most extreme requirement to ensure all requirements are met.

Don't define the privacy UX. It could vary over time.

When the layers alter you need to amend it.

"Human colossos foundation". Semantic

Data brokers know the value of the data but consumers do not.

UX could present the value of data by auctioning it to the brokers.

Forcing privacy labour onto the user should be considered.

A car company spends \$400 to get you to test drive their car so the value of an email address which leads to this is far higher than other use-cases.

Grocery stores didn't take cards as they charge 2% and margins were 1%. But the data is worth 11%. Hence store loyalty cards

Data may only have value in a particular system.

4. How can we empower particularly vulnerable people to protect themselves? (e.g. victims of domestic abuse, dissidents in repressive regimes, LGBTQ people in non-accepting cultures, people seeking abortion information in certain US states)

5. How do we avoid adding usability burdens that reduce the product value for the majority of times when people are not particularly concerned about privacy, while still making sure they are empowered to take privacy-protective measures for sensitive user journeys?

Cookie pop ups are a great example of this

Friction is not always bad. It can make the user think if there is a pause.

Sensitive user journey should be the default.

Buying stamps doesn't need my ID. But step up if I want to register a forwarding address.

You need to increase friction to make sure people take a careful decision.

What is the motivation to care about privacy. As much reputation as legislation

When the UK introduced a requirement for consumers to set Betting limits most found the fastest route through ux and set the maximum.

6. What are the privacy threat models, and what are the different ways of adding UI features to counter them? Some of the threat models can be countered by controlling data collection: such as threats from state actors subpoenaing user data. Some of the threat models can be countered by controlling data use, such as threats from people shoulder surfing or compelling physical access to devices or accounts.

Give chat gpt a legal contract and ask it for the vulnerabilities.

Use AI to check the privacy policy.

There is an IEEE P7012 working group on standardised privacy.

Can we have certification for providers. GDPR Art 42/43 allows for certification e.g.
www.accscheme.com

Community list. To check which sites are good.

InternetSecuritylabs.org K-12 report. (<https://noise.cs.uchicago.edu/security.html>)

www.euconsent.eu defines standard language

Menu

7. How do we avoid the unintended consequences of actually making people more vulnerable with well-meaning trust measures? For example, providing transparency of what we know about a user is good for empowering them to take action, but it also adds a new privacy attack vector by providing a convenient UI for a bad actor who has access to the user account. Or adding controls to allow the user to specify topics or URLs that they consider sensitive and not to be tracked, is itself a very sensitive list that could be harmful if revealed. Or if we try to protect particularly vulnerable people by noticing they are vulnerable, that detection of their status might be privacy-invasive.

I will use the EFF answers.

Give Macy's temp access to my address

Spread disinformation to change the value of the info.

Use a proxy but the proxy may not be trustworthy

Does AI means personal data stores will be resurgent.

Macy's can store my info on my device.

The bbc leaves streaming data locally on the solid pod rather than storing user data.

Aries Bifold & APP Attestation

Session Convener: Jason Leach , Clecio Varjao

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

Making the Internet AGE Aware

Session Convener: Iain Corby

Session Notes Taker(s):

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

www.euconsen.eu <https://www.pass-scheme.org.uk/>

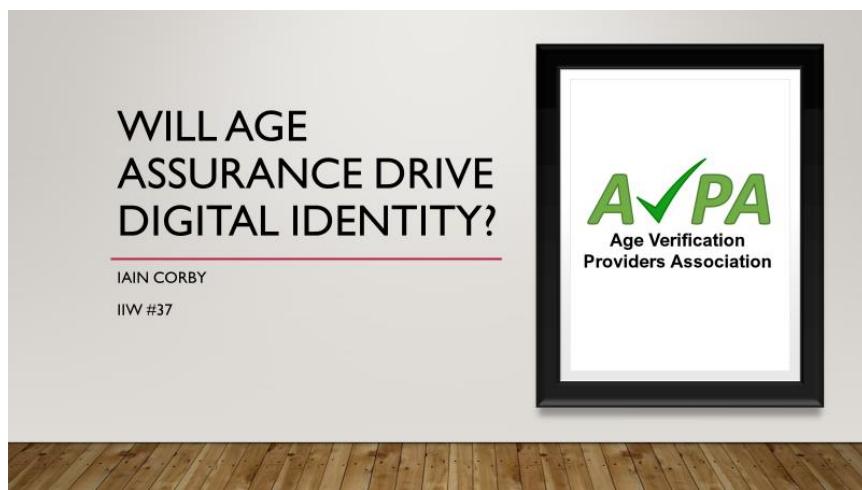
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The presentation on which the talk was based is below.

Debate focused on why in the real world the UK is not fully using ISO 18013-5 to enable in-store proof of age e.g. at self-service tills.

The answer was that

- (1) wallets were not available when the solution was selected
- (2) there was a reluctance to transmit PII from the user to the store (rather than just showing visually that the user had been proven to be 18+)
- (3) 18013-5 does not require biometric authentication before presentation
- (3) this is not the final answer - it is built on mDL 18013-5 principles to allow in future government mDLs - UK, US etc. - to be validated with the same infrastructure.



AGE ASSURANCE

Age Assurance is the ability to prove your age or age-range without disclosing your full identity

It includes both Age Estimation and Age Verification



Photo by sciony_cho on Foter

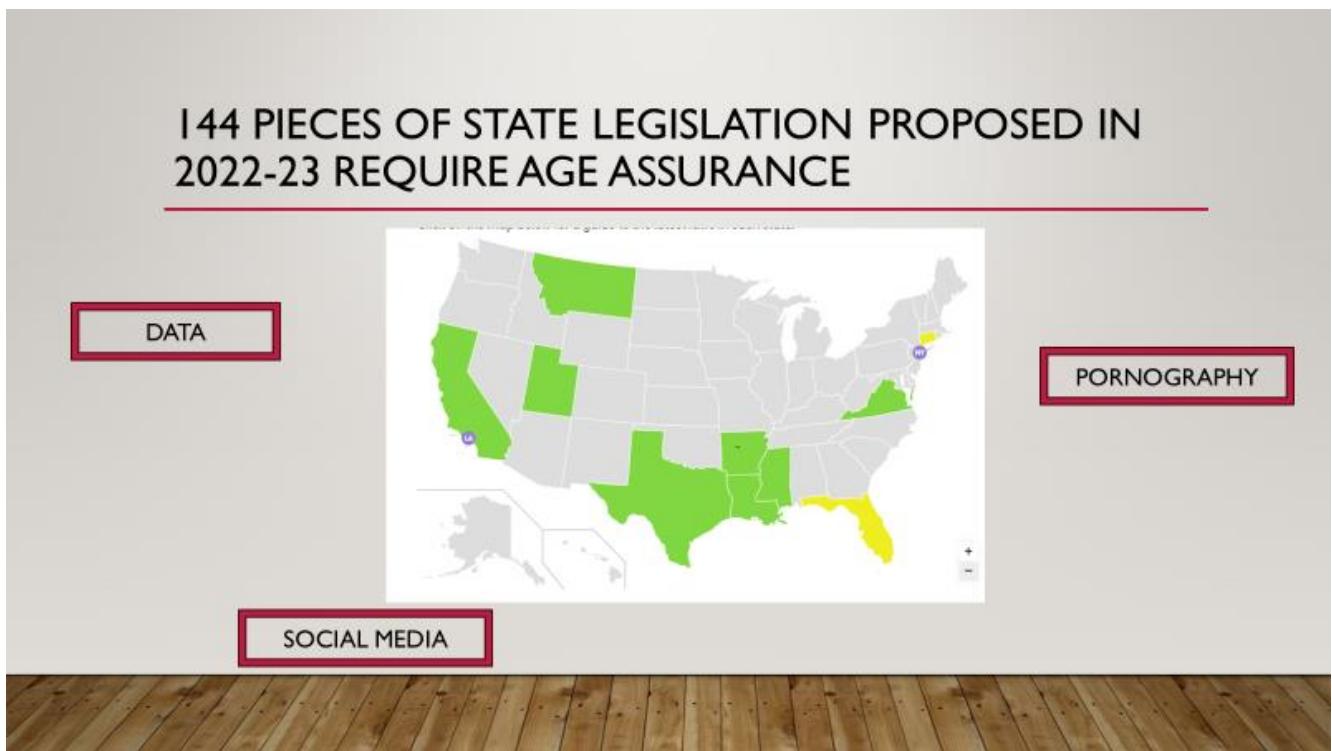
A collage of logos for various companies involved in age verification and identity intelligence. The companies include: AGEVERIFY.UK, agechecked, AGEify, INTEGRITY, AUTOPIX, BlueCheck, envōc, experian, facete, FUJITSU, IDverse, Innovative Technology, LUCIDITI, one id, pale.io, PRIVO, SafeShare, SERVELEGAL, SQR, PRIVATELY, SUPER AWESOME, TRUSTMATIC, Verifi ID, verifymyage, and YOTI.

AGENDA

- The legal drivers for online age assurance
 - US
 - Global
- Standards and certification
- euCONSENT – reusable, interoperable age assurance and parental consent
- Proof of Age Standards Scheme – universal acceptance of a digital proof of age in person
- A roadmap to “self-sovereign age assurance”...



144 PIECES OF STATE LEGISLATION PROPOSED IN 2022-23 REQUIRE AGE ASSURANCE



OpenID4VC as Framework vs. Profiles

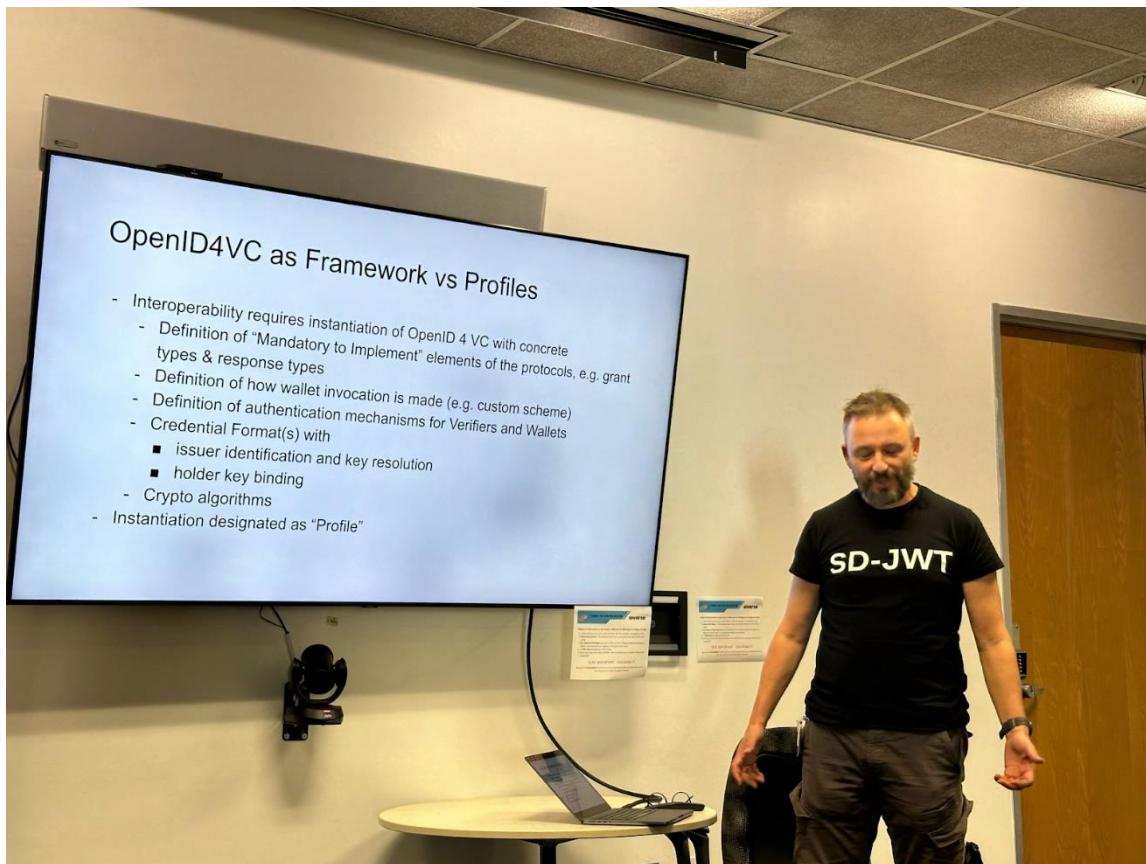
Session Convener: Thorsten Lodderstedt, Kristina Yasuda & Harmen Van Der Kooij
Session Notes Taker(s):

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

HAPI profile: Individual draft: <https://github.com/vcstuff/oid4vc-haip-sd-jwt-vc>

DIIP: Decentralized Identity Interop Profile (Dutch Blockchain Coalition)

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



Abbreviated Language for Authorization

Session Convener: Mark Berg & David Brossard
Session Notes Taker(s):

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

- [NIST 800-162 - Guide to Attribute Based Access Control \(ABAC\) Definition and Considerations](#)
- [Draft standard](#) (OASIS)
- [IIW 2023 - Introduction to ALFA](#)
- [Abbreviated Language For Authorization \(ALFA\)](#)

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

What's authorization

Authorization has often been the ugly little duckling in the IAM family. Focus has often been on identity and authentication. In the past few months, there has been renewed focus on authorization at EIC, Identiverse, and now IIW. New technologies have emerged such as AWS's Cedar. Now is the time to consider implementing authorization for apps, APIs, and services.

There are 3 kinds of authorization to be considered:

- functional: can Alice print?
- transactional: can Alice print doc #123?
- data-centric: tell me which documents Alice can print

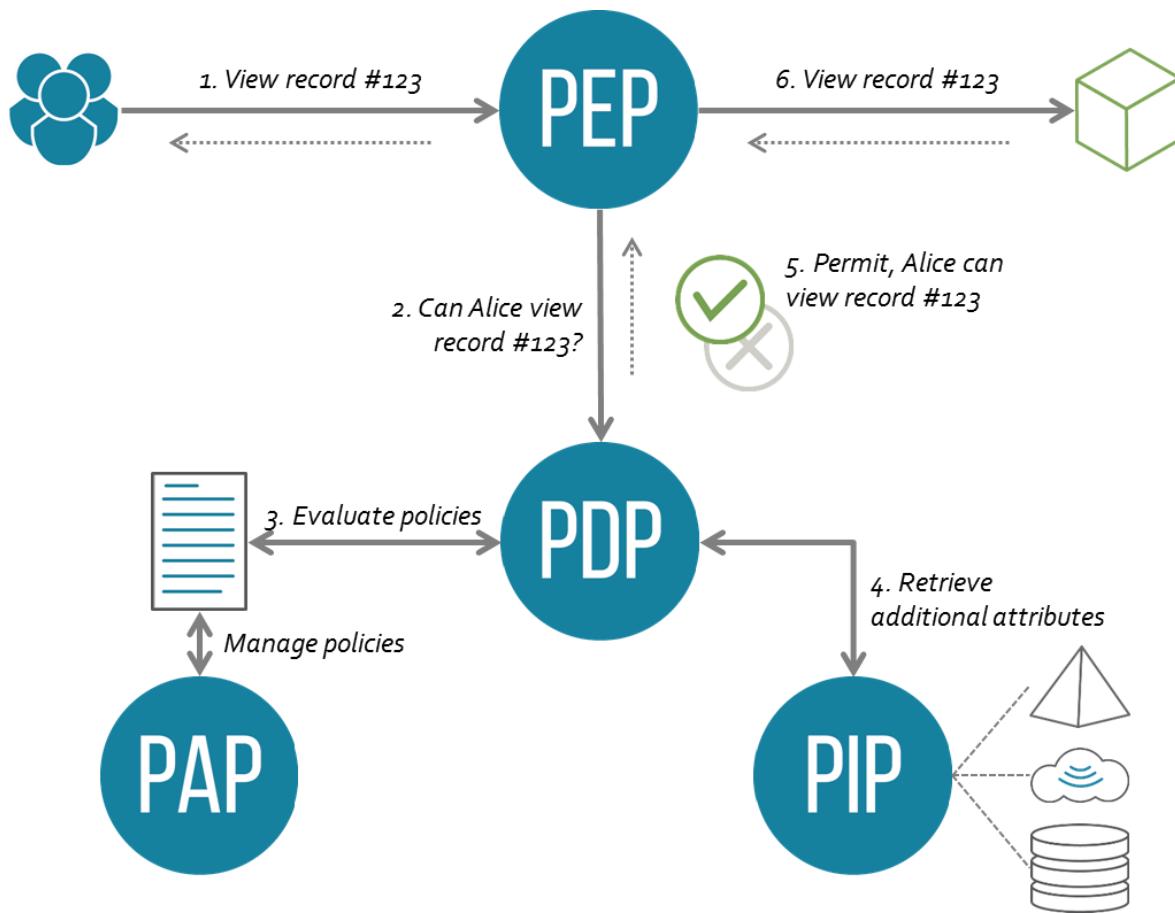
Historically, authorization has been expressed through birthrights, entitlements and permissions assignments at design-time when the user is created or updated. However, we now need dynamic authorization that is decided when the user is trying to access the data/service.

Handling Authorization the modern way

Rather than use RBAC, roles, groups, and permissions, let's turn to policies and attributes. This is what NIST recommends in their [NIST 800-162 publication on ABAC](#). Attributes describe the user, resource, action, and context while policies combine them together in a single legible statement e.g.

“Managers can edit a document they own if it’s in draft mode”

The NIST ABAC approach recommends the following architecture:



| Abbr. | Term | Description |
|-------|-----------------------------|---|
| PAP | Policy Administration Point | Point which manages access authorization policies |
| PDP | Policy Decision Point | Point which evaluates access requests against authorization policies before issuing access decisions |
| PEP | Policy Enforcement Point | Point which intercepts user's access request to a resource, makes a decision request to the PDP to obtain the access decision (i.e. access to the resource is approved or rejected), and acts on the received decision |
| PIP | Policy Information Point | The system entity that acts as a source of attribute values (i.e. a resource, subject, environment) |

What's ALFA?

The Abbreviated Language for Authorization (ALFA) is a language used to express fine-grained, attribute-based access control policies. It's based on XACML, the OASIS standard for externalized authorization and provides developers with a simple and easy-to-use syntax. For instance the above example in ALFA becomes:

```
/*
 * Policies for Managers viewing records
 */
policy managersViewRecords{
    target clause user.role == "manager" and object.objectType == "document"
    apply firstApplicable
    /*
        * R1 - A manager can view any record
        */
        rule managersCanView{
            target clause action.actionId == "view" and document.status == "draft"
            permit
            condition user.username == document.owner
        }
} //managersViewRecords
```

How does ALFA compare to other languages?

| | XACML | ALFA | REGO | CEDAR |
|----------------------------------|-----------------------------|------------------------|----------------------------------|-----------------------------|
| Origin | Standard (OASIS) | Standard (OASIS) | CNCF | Open Source (AWS) |
| Founded | 2001 (current version 2013) | 2012 | 2015 | 2023 |
| Based on | Functional Programming | Functional Programming | Logic Programming (Datalog) | Logic Programming (Datalog) |
| Format | XML | Java-like | Datalog | JSON-like |
| Can retrieve external attributes | Yes | Yes | Not natively | No |
| Focus | All-purpose | All-purpose | Infrastructure - can be extended | All-purpose |
| PDP | Yes | Yes | Yes | Yes |
| Policy Combination | Yes | Yes | No | No |

| | | | | |
|---------------|---------------|---------------|------|------|
| Compatibility | XACML to ALFA | ALFA to XACML | None | None |
|---------------|---------------|---------------|------|------|

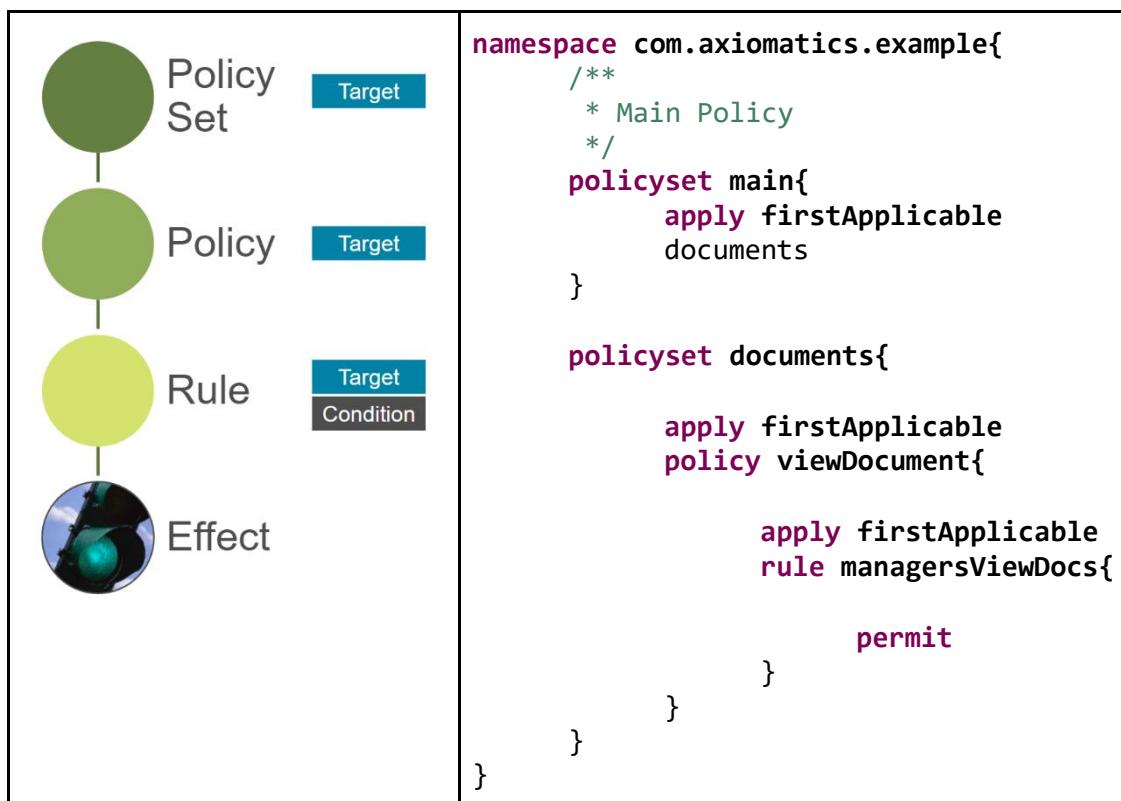
Basic Structure

ALFA uses policy sets, policies and rules on the one hand and attributes on the other.

Attributes are made up of:

- an identifier e.g. user.role
- a datatype e.g. string
- a category e.g. subject (which represents the function or grammatical purpose of the attribute)

Attributes are then used inside rules (R), policies (P) , and policy sets (PS). Policy sets contain policy sets / policies / rules. Policies contain rules. Rules contain the effect (Permit, Deny). The R/P/PS structure is akin to Russian Dolls whereby you can have policies as deep as you like by wrapping them inside another PS. See diagram below.



Combining algorithms

ALFA uses combining algorithms to resolve which policies win over which other policies.

| Combining Algorithm | Effect |
|--|---|
| Permit overrides, ordered permit overrides | If at least one is Permit, final result is Permit |

| | |
|--|---|
| Deny overrides, ordered deny overrides | If at least one is Deny, final result is Deny |
| First-applicable | Result is the first which is not NotApplicable |
| Only-one-applicable | Result is the only one which is not NotApplicable If there are more, the result is Indeterminate |
| Permit-unless-deny, Deny-unless-permit | Permit / Deny access unless denied / permitted |
| On-permit-apply-second | If the first branch says Permit, then return the second (this mimics an if/then/else) |

Use Cases

ALFA can be used to implement:

- ABAC
- Export control, Intellectual Property Control
- Role-based
- Risk-based
- Relationship-based
- Ownership-based
- *-BAC: if there's an attribute, we can model it

Examples

Control access to top secret documents

- Managers can view all the documents
- Users can only view documents in their departments
- Deny access if the clearance is less than the classification

Sample Policy

```

namespace com.axiomatics.example{
    /**
     * Main Policy
     */
    policyset main{
        apply firstApplicable
        documents
    }

    policyset documents{
        target clause objectType == "document"
        apply firstApplicable
        policy viewDocument{
            target clause action == "view"
            apply firstApplicable
            rule managersViewDocs{
                target clause user.role == "manager"
                permit
            }
        }
    }
}

```

Useful Links

- [NIST 800-162 - Guide to Attribute Based Access Control \(ABAC\) Definition and Considerations](#)
- [Draft standard \(OASIS\)](#)
- [IIW 2023 - Introduction to ALFA](#)
- [Abbreviated Language For Authorization \(ALFA\)](#)

KERISSE.org, the KERI Suite Search Engine

Session Convener: Henk Van Cann
Session Notes Taker(s): self

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

https://docs.google.com/presentation/d/1jkJTP5O6QkWm3EHQUlbt2Oy8nzMQMSBkte5xaN_JptE/edit?usp=sharing

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

Practical introduction to using KERISSE.org. Go through the slides for more info.

Targeted Log OUT

Session Convener: Aaron Parecki
Session Notes Taker(s): Jeff Corrigan

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

OAuth, OpenID Connect, Logout, Sessions, SSF, SecEvents

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

Aaron Parecki: Sample scenario: mobile app connecting to an app like Slack. Straight forward; Complications introduced with external IdPs.

e.g, enter email in app, perform ID discovery to locate domain based IdP, could end up with multiple IdPs. IdP could be social, enterprise

Mobile app gets its tokens from the API. When user logs into IdP, what usually happens is that the app BE performs the OIDC transaction. The IdP simply sees that it's a website it's communicating with.

If you login to gmail with your own acct to view your acct security settings you can see where you have active sessions, e.g. logged into this device, this IP, since x time.

If you've used a google IdP to log into slack, those settings would show that you're logged in to slack, (by the clientID), not the device itself. Info breakdown occurs here bc the IdP doesn't have

the breakdown to show anything other than a logged in session to slack. The context of the end device is missing as a result from the IdP's perspective.

In enterprise/workforce identity, there is an IdP for employees, it would be useful to say "this employee lost this device, revoke all active sessions on this specific device but leave the others alone". This should end not only the websession on the device which is active, but also the session within the app as well.

George Fletcher (GF): Existing fingerprint information could/should allow the IdP to be able to distinguish between the two.

AP: It's more complex than that; If it's Workspace with a federated IdP, and I have 5 apps on my phone, drive, gmail, etc. For each of those apps they all use the same system browser so to the IdP they all look identical bc it's the same session which authenticated them, etc.

Discussion: There may need to be a definition of what it means to logged out. There is also a "grant access but don't create a session" scenario (ephemeral sessions in iOS). Global logout doesn't exist consistently exist in every browser.

The purpose of this session is to gain examples to allow us to solve the logout knowledge gaps to the IdP. Maybe provide context about what the actual app is. This wouldn't work well for Consumer ID due to privacy issues but it's fine for enterprise/workforce because there is already MDM and security tools, end user privacy is not expected.

If you logout of google blogger it logs you out of all of the google products.

GF: Today though there is nothing that is blocking you from sending addl information as a part of the auth flow, could also be achieved via RAR. Where in the deployment should the data be kept?

AP: The goal is to be able to target these entities to target logouts:

- Users
- Devices
- App Families

AP: The app could also do the OIDC tx with the IdP, but then instead of that creating the session directly, that is exchanged for app-based tokens.

Question:

Are you proposing to do this in existing frameworks or create new specs?

AP: There are some missing areas where there may need to be mods to specs

The first IdP has a clientID which could be mapped to an appclass. What doesn't exist standardized today is the ability to send/persist the device ID. There is a way where a small spec could be created to add addl context to the authentication, do 'X' to group the sessions together and use a hash of that value as a part of otherTx with the IdP. The IdP could augment its session store with the addl contextual data.

There is device_id, but between that and the IdP there is also a need to have a session_context, something like app_class(name/version/etc) and device_id which then rolls upwards to the IdP.

We would need to define the mechanism for how the IdP actually performs the logout between the tiered IdPs. There also needs to be a way to signal to the IdP which specific session_reference to kill.

Generate session_ref, add it to the session with the app_class, device_id info. Now there exists an id which can be specific.

Is there a collision between RAR and OIDC? RAR isn't made for that but it could work?

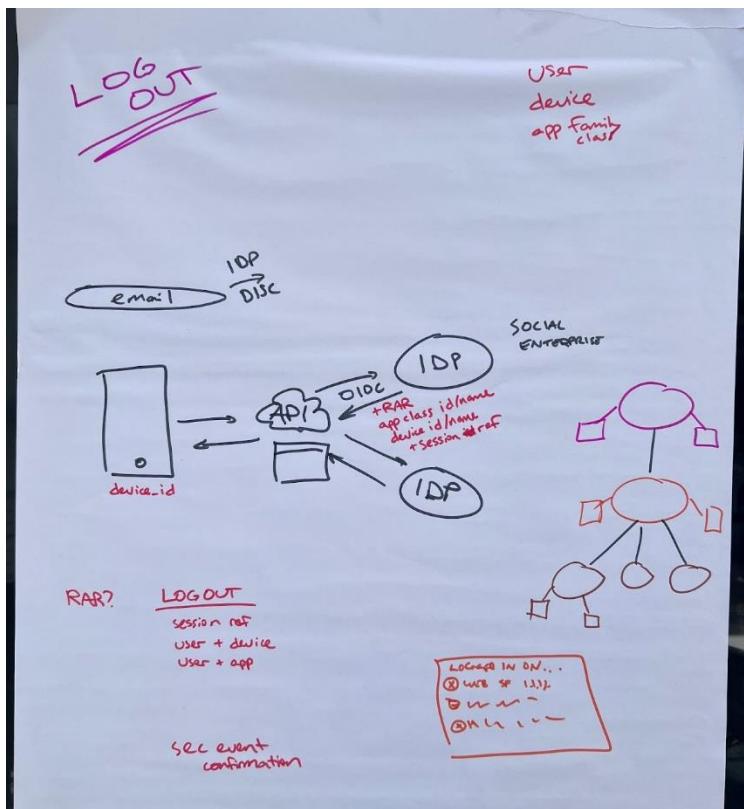
Is this enough info? What about adding geographic region and other metadata like that? AP: That doesn't really need to get passed bc it's already a part of the data since the browser visits the AS. The IdP could drop any portion of the RAR which it doesn't understand.

We would need to go to every app maker to have them include the device_id

Part of the spec for all federated enterprise auth. The first tier would need to send the deviceID. Upwards from there the session_reference with the appClass/name, deviceID, etc. Do we need to create mechanisms to report back to the IdP that the logout was successful? OAuth token revocation is "hope for the best" where the IdP makes an attempt to logout but there is no guarantee.

That's a whole new protocol, might belong in shared signals group as a sec/caep event..

For this to work there might need to be a need to enforce the use of shared signals in enterprise.



Browser API Wallet Query Lang

Session Convener: Sam Goto

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

Should governments be involved in VC ecosystems?

Session Convener: Naoki Yagita & Rintaro Okamoto

Session Notes Taker(s): Naoki Yagita & Rintaro Okamoto

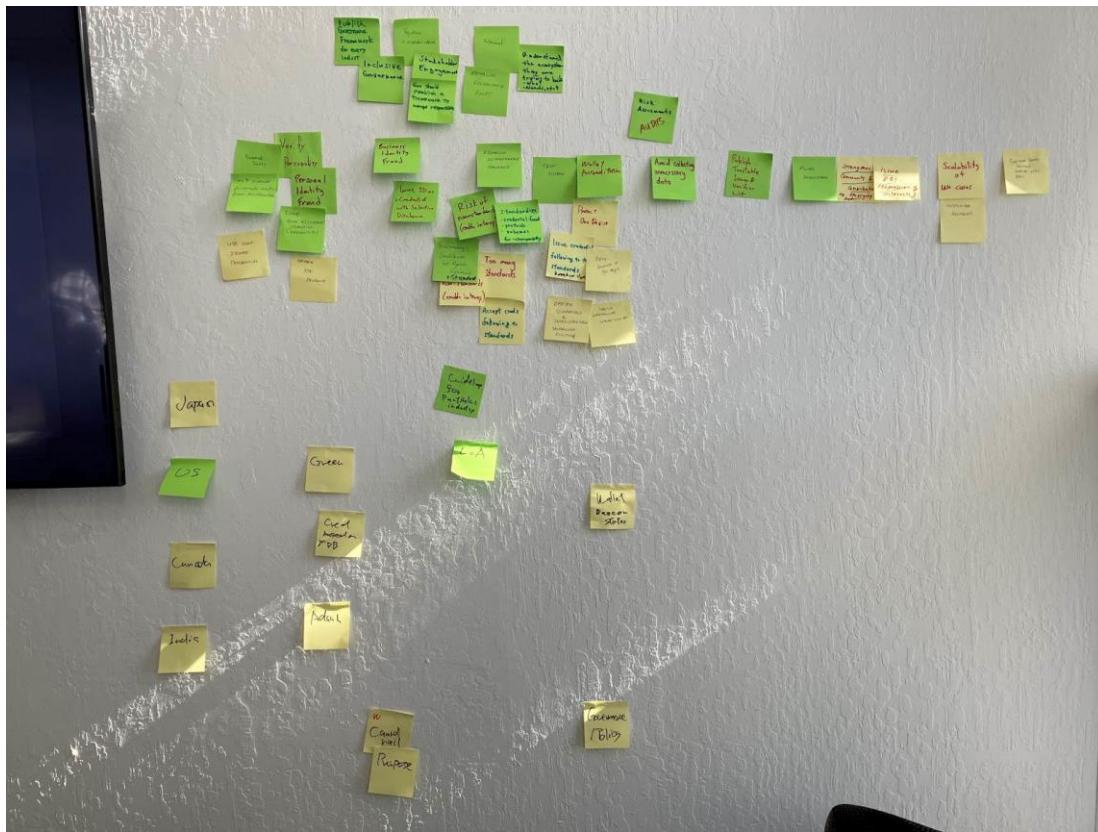
Tags / links to resources / technology discussed, related to this session:

Discussion paper

<https://drive.google.com/file/d/1I5KhbUUH4vs3Rz0Clr6fAc1JIXyzmPat/view?usp=sharing>

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

We made matrix of Things that should be done by governments(Green) and privates(Yellow) x Current situations of each countries



There are several layers e.g. engagements, make base rules (Governments/Privates), Operations(Audit etc.)

It's too early to conclude, however governments should make "Guardrails" in common.

Original images of the Matrix

<https://drive.google.com/drive/folders/1iRTmIwjZRAAsWncDu8z-O-noCBt7lvw8G?usp=sharing>

Secure Organizational Identity

Session Convener: Lance Byrd & Rodo & Alex Andrei
Session Notes Taker(s):

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

Unofficial notes here: <https://ericscouten.dev/2023/iiw/#session-9h-secure-organizational-identity>

Confidential DiD's - Solve Decentralized Key Management and Universal Zero-Trust

Session Convener: Manu Fontaine

Session Notes Taker(s): Manu Fontaine (redirected to Charles Lanahan's notes)

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

Confidential Computing, TEEs, automated decentralised key management infrastructure

Link to slides:

<https://drive.google.com/file/d/1Mt-hJfJ9xHriSBTEFMT6Z6sTdo0OmZ5k/view?usp=sharing>

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

This session is a variation on Day 1 session “Confidential Computing Changes Everything - Enabling a Universal Name System (UNS) and Universal Certificate Authority”, see notes here:

https://docs.google.com/document/d/1DoWnI2UJ5OkRjTzwjF-QdVyECL23MCLJ58hM_vhYYI/edit?usp=sharing

The focus on “Confidential DIDs” is that Confidential Computing enables the creation and protection of random entity DIDs that are both identifiers AND keys at the same time. We call these identifiers StemIDs as they can be used to cryptographically derive (with an HMAC function) an unlimited number of keys for each StemID. This creates confidential keychains that are mathematically united with the identifiers, and hence do not require any external authority to bind them to it. The keys on the keychains can then be used to encrypt an unlimited amount of data for each entity and for an unlimited number of contexts, thereby mathematically uniting entity data, keys and identifiers without external authority.

Experiments with DIDs and DHTs

Session Convener: Gabe Cohen & Daniel Buchner
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

OIX Roaming Between Trust Frameworks

Session Convener: Mark Haine
Session Notes Taker(s): Mark Haine

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

<https://drive.google.com/file/d/1jQedd4ZZLFFUcNAAB8iw3QX7FmD6YRTo/view?usp=sharing>

The presentation discussed is linked above

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

none

Using DIDComm to protect files in cloud storage

Session Convener: Steve McCown, Anonyme Labs

Session Notes Taker(s): Me :-)

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

Here are my presentation slides:

https://www.dropbox.com/scl/fi/xmccu7bdfdnh3tqccx45g/IIW37-McCown-protecting-cloud_storage.pdf?rlkey=k2iywarxf017dwc0eaf46vij&dl=0

The source code should be on github shortly...

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

Overview

Cloud storage services (e.g., Dropbox, iCloud, Google Drive, OneDrive, etc.) are an exciting advancement for data replication, synchronization, disaster recovery, etc. However, current architectures leave the level of security and privacy up to the particular service. Their respective terms of service disclosures show that they control the unencrypted versions of their users' personal files according to the service's policy, which may not be acceptable to users.

In this presentation, a method was shown for using contemporary Decentralized Identity technologies to introduce End-to-End Encryption as a separate service that is layered on top of cloud storage services and which is completely under the control of the user. New technologies, such as this will give users more privacy and security control over their personal data while still benefiting from cloud storage offerings.

IEEE 7012 - Personal Terms and Conditions

Session Convener: Daniel Hardman

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 Credentials Cons. - VC-API SPEC Implemented as Microservers in Docker Compose

Session Convener: James Chartrand

Session Notes Taker(s): James Chartrand

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

VC-API spec: <https://w3c-ccg.github.io/vc-api/>
<https://github.com/digitalcredentials/issuer-coordinator>
<https://github.com/digitalcredentials/workflow-coordinator>
<https://github.com/digitalcredentials/signing-service>
<https://github.com/digitalcredentials/status-service>
<https://github.com/digitalcredentials/transaction-service>

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

We talked about the Digital Credentials Consortium implementation of the VC-API spec.

The DCC - a consortium of 13 universities whose mission is "to create a trusted, distributed, and shared infrastructure that will become the standard for issuing, storing, displaying, and verifying academic credentials, digitally."

To that end, the DCC helps educational institutions setup infrastructure to issue credentials. The DCC would like to increase issuance in order to build momentum and critical mass.

The DCC has a mobile wallet: The Learner Credential Wallet (<https://lcw.app>).

The DCC also provides open source software for issuing credentials.

The first iteration of the DCC issuing software was called sign-and-verify, which evolved over several years, and was used for several pilots.

Over the course of the last year the DCC has moved to a microservices model for issuance and has replaced the monolithic sign-and-verify with smaller, discrete applications - microservices - each of which are express applications with a RESTful API, that are wired together in a docker compose network using 'coordinators' that effectively create a 'pipeline' for issuance where the credential moves through the pipeline from data retrieval to VC construction, through status allocation, signing, logging, and distribution.

To date the DCC has two coordinators:

<https://github.com/digitalcredentials/workflow-coordinator>
<https://github.com/digitalcredentials/issuer-coordinator>

and three microservices:

<https://github.com/digitalcredentials/signing-service>
<https://github.com/digitalcredentials/status-service>
<https://github.com/digitalcredentials/transaction-service>

Further microservices are likely to be for:

- logging
- data access (e.g., pulling data from an institutional store like PeopleSoft)
- alternate signings or status management
- credential templating and validation

One might, for example, create a coordinator where the pipeline includes multi-signings, say both Ed25519 and BBS+. Each signing would be handled by a separate service.

There are several benefits to the the microservices model:

- easier to use only those services that are relevant for a given application
- easier to substitute services
- easier to test each service individually
- cleaner separation of concerns for easier ongoing maintenance
- can use different languages/platforms for different services because services are hidden behind a RESTful API

And possibly most important is that the microservices architecture is conceptually much easier to understand. The DCC found that the monolithic sign-and-verify application was difficult for adopters to understand - and so to evaluate - and difficult to setup. In all cases the DCC had to host and setup instances for DCC member institutions' pilot projects. With the new model, we've had three partners successfully use the microservices with very little help, and perhaps more importantly, the partners are hosting their own instances.

Part of what makes the microservices model work well is that all of the services, and the coordinators, are published in Docker Hub as docker services so that setup is minimal. It comes down to having a single docker-compose file that declares the services and any environment variables. It is effectively a matter of minutes to get a test instance up and running, and a matter of hours (and far less than a day) to install a fully configured instance.

It has become clear over time that removing obstacles to evaluation and installation, however minor they may seem, is very important. One example in this case was removing the need to interact with the github repository (cloning, building) and instead publish prebuilt services to Docker Hub.

There was some discussion of the VC-API spec and specifically of the exchange endpoints, and of the verification endpoint. Notably, the DCC has not implemented the verification endpoint, preferring to handle verification within the web browser so as not to make calls back to a central

verifier (the 'phone home' problem). And not surprisingly there was also quite a bit of discussion of trust registries - how verifiers will know which signing DIDs are legitimate.

There was also a very good discussion of the right of the student to their own documents, and of potential revenue models that institutions might consider in lieu of traditional charge-per-access models that restrict access to the documents.

SESSION #10

International Interoperability Summit - Paris Next Month

Session Convener: Gail Hodges & Mark Haine

Session Notes Taker(s): Mark Haine

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

Draft Presentation:

<https://docs.google.com/presentation/d/1jZ5NqFRI9pvubOx3hoVRXZbloTPHwmZ1/edit?usp=sharing&ouid=117095465340516441049&rtpof=true&sd=true>

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

The presentation was delivered in an interactive fashion and a number of very useful suggestions were received from the session participants. The following notes were captured on the white board:

- What metrics are available or desirable for cross border transactions?
- Can we work out what the minimum technical requirements are for protocols, formats and signatures?
- What level of focus is there on domestic requirements?
- Is regional interoperability actually more of interest to the Summit participants than “global” interop?
- For most it may even be cross-border focussed
- What will the role of digital public infrastructure?
- We should ask summit delegates to give us examples of use cases and the dynamics that matter to them.
- Perhaps Cross-border marriage, death, refugees might be important cases?
- How will governance of cross border use cases be handled?
- Domestic/regional/global interoperability? this might actually be selective
- KPI for success of the summit. Suggest that there should be a very specific KPI for success of summit - ideally only one KPI - “What is the problem statement?”
- Strong advice that the summit should have a significant amount of “listening mode”
- There will be an Open Space event in South Africa next year that will be worth thinking about for potential next steps

Sustainable Privacy Re-Identification Attacks

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

Fitting credentials that are verifiable into NIST 800-63-4

Session Convener: Justin Richer
Session Notes Taker(s): Jin Wen

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

<https://pages.nist.gov/800-63-4/>

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

Key Understandings

- The relationship between the subject and the CSP is important, as the CSP's job is to associate authenticators with the account and establish a subscriber account.
- The trust agreement between the IDP and the RP is crucial for the overall process.
- The IDP's role in the new model is stronger, with a tighter relationship between the subject and the IDP.

Outstanding Questions

- How can the trust between the RP and the IDP be established independently from that of the CSP?
- How can the model accommodate cases where the presenter is not the subject?

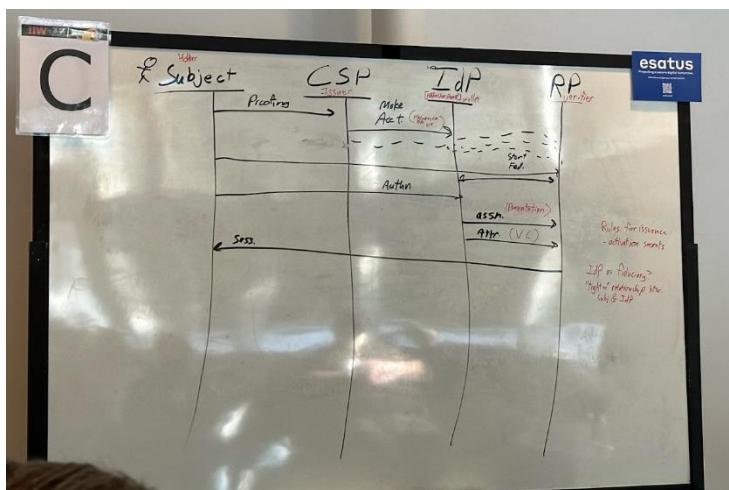
Observations

- The new model may result in different flows, where the proofing and "make it count" steps are collapsed into one.
- The IDP may have a higher bar of responsibilities in the new model, as it acts on behalf of the subject with their direct consent.

Action Items / Next Steps

- Explore the possibility of adding requirements around the issuance process to prevent the movement of credentials between wallets.
- Consider the implications of the tighter relationship between the subject and the IDP, including the potential for the IDP to act as a fiduciary of the user.

It is important to note that this summary is based on a transcript of a discussion, and some points may require further clarification or investigation.



Identity is a Graph Problem

Session Convener: Alex Babeanu

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

IDP Discovery via Wallets

Session Convener: Aaron Parecki

Session Notes Taker(s): Aaron Parecki

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

OpenID Connect, Federated Login

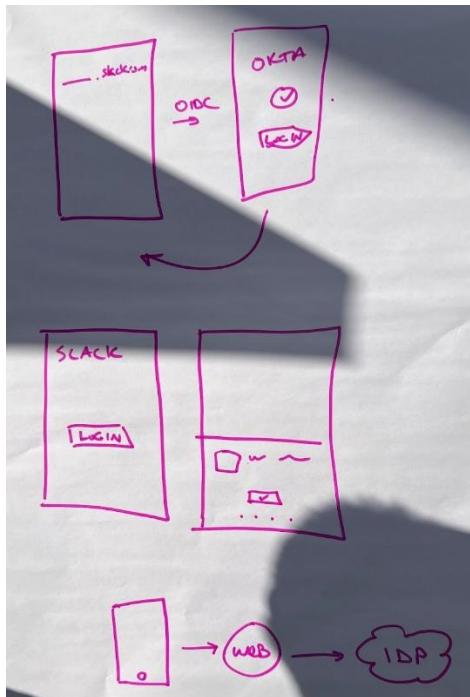
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

We would like a better UX for federated login than asking users to enter their email address or tenant URL in apps!

Ideal UX: Click “Log In”, user is presented with an account chooser, clicks the account, login happens.

We discussed the parallels between the Android VC chooser prototype and the OAuth consent screen. We discussed whether the VC selection mechanism could be used to do IDP discovery to bootstrap an OIDC flow. FedCM was brought up as another possibility for an account chooser. Both have tradeoffs, for example working in native apps vs browsers, whether the selection appears when the user is logged out of the IDP, etc.

Both existing approaches are not exactly the right UX to eliminate manual entry or the NASCAR problem, but would likely require only minor changes. More discussion to be had here!



Accelerating Broad Adoption of Digital Trust Technology: British Columbia's approach

Session Convener: Nancy Norris & Aaron Unger
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

AnonCreds V2: BBS+, more ZKPs, (perhaps) PQ and CODE!!

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

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

#anoncreds #verifiablecredentials #bbs+ #postquantum #zkps

Link: [Presentation Slides from the session](#)

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

The session was a gathering of those interested in the use of ZKPs for verifiable credentials, and particularly, those using/building on AnonCreds v1, and those interested in the use of BBS+ signatures in future verifiable credential deployments.

The session covered:

- What is AnonCreds?
- What is AnonCreds V2?
- To Do List
- Code Overview
- Next Actions

The key differences from AnonCreds v2 vs. v1 are:

- Same object types and same interactions as AnonCreds v1
- Flexibility in the underlying signature scheme
 - Options include BBS+, PS (Pointcheval Sanders), CL Signatures

- More ZKP presentation options to increase data minimization possibilities
 - Equality proofs — two claims from different credentials are the same without sharing the value.
 - Range proofs
 - Signed integer support in predicates
 - Set membership proofs
 - Issuer defined blinded secrets (similar to link secrets, but controlled by the issuer)
 - Verifiable encryption (e.g., credit card number blinded, but decryptable by the issuer)
 - Comparable to the feature that Apple Pay does of blinding all Credit Card numbers for every transaction.

How are the improvements accomplished?

- Define much more information at the schema level about the credential attributes
 - This Enables encoding the data in a way that can be flexibly signed and presented

There is code for AnonCreds v2 available [here](#). The specification will be built out from [here](#). We reviewed the code briefly, and provided a list of things that are on the “to do” list for getting from this starting point to a stable, open source, open specification implementation of AnonCreds V2.

The to do list is (currently):

- Everyone: Evaluate the code and cryptographic primitives
 - Take a look — what do you think?
 - Does this get us to FlexCreds / BBS+ ZKPs / Rich Predicates / Post Quantum / Revocation
- Extract any cryptographic code into libraries
 - The “knox” folder
- Abstract the signature scheme
 - Currently concrete PS, abstract to enable BBS+
 - Experiment — post quantum (Lattice) PS Signatures
- Add always included link_secret value
- Add “DateTime” encoding type
 - Encode date as DateInt, time as Unix Time (with thought about pre-1970 timestamps...)
- Specification and decision making
 - An evolution of the AnonCreds v1.0 Specification, path to standardization
- VC, VP in W3C Verifiable Credentials Data Model Standard format
 - Similar to the AnonCreds v1 approach
- Format of the presentation request
 - Evolution of AnonCreds v1.0?
 - DIF Presentation Exchange?
- Revocation
 - Included in the code, but do we want some other scheme?

Next actions were discussed and connections were made to follow up in the weeks following up from IIW to see how to proceed.

Follow the progress at [Hyperledger AnonCreds](#), and the [Hyperledger AnonCreds Wiki](#).

[Hyperledger AnonCreds meetings are held weekly](#), usually at 7:00 Pacific / 16:00 Central Europe.

Universal Wallet Backup Containers

Session Convener: Sam Curren

Session Notes Taker(s): Tracy Kuhrt

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

Reviewed past progress that is captured at: <https://identity.foundation/universal-wallet-backup-containers/>

Shadow credentials for the high-value credentials that are tied to the hardware

Wallets are unique over other backups (non-transferable, unbackable) - it is not just shadow, but the act of getting me through the process of requesting/restoring

Need indication of whether this is a credential that should be backed up

Specification does not care about what should be backed up (e.g., expired credentials). This is a preference that could be set by the user in a wallet.

Sync is out of scope for the specification. No way to capture just deltas.

What overlap exists with encrypted data store? App could hand it off to the encrypted data store (decentralized web node)

Structure: encrypted GZIP TAR file

- Manifest (can reference where the definition of the standard files contained exists; version-specific URI that points to the specification; top-level metadata about the app that produced this)
 - JSON (sounds like a reasonable answer)
 - YAML
 - Structured Markdown

- Standard file 1 (e.g., list of contacts)
- Standard file 2 (some of the data that is contained in the standard files may not be able to be imported; e.g., moving from a wallet that does VCs and Crypto to a wallet that only does VCs)
- Standard file N
- App-specific Data (can decide on whether to store everything or only items not in the standard files)

Main area of work:

1. Practice encryption/decryption and how easy this is for developers and grandma
2. Key Recovery
3. Format of manifest file

Look at password manager's sync structure

Do we want to allow unencrypted exports? For developer usability; user trusts their backup medium more than they trust remembering their key.

Print out information on how to recover

Social recovery, sharded secrets, multisig

Agility for recovery option

Is this unique enough to wallet that we should not generalize this? Ask Dave Turner (FIDO), Tim Capeli

Look at: Cryptomator

One of the misuse of backup/recovery is that a younger sibling gains access to an age credential from an older sibling

Should there be a shredding of old credential when restore occurs?

Work item of the wallet security working group at the DIF

The P3Pub Protocol (Web-native, lightweight Push-Pull-Publish-Subscribe)

Session Convener: Johannes Ernst

Session Notes Taker(s): Johannes Ernst

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

Protocol: <http://tech.dazzle.town/protocols/p3sub/spec/>

Part of <https://dazzle.town/> <https://ubos.net/>

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

P3Sub is a very simple protocol for HTTP-based publish-subscribe on the open internet. It:

- Doesn't have a middleman (like a message broker);
- Supports both polling and event-based subscribers;
- Switch between polling and event-based modes without missing updates;
- Publishers can give up quickly; subscribers can easily recover without missing content;
- Subscribers can get missed content replayed if needed;
- Web native: works with any content type that can be transmitted over HTTP;
- No need for an "envelope" feed format;
- Can be scaled out easily through fanning.

Johannes gave an overview asking for feedback.

Python implementation

Discussion on application areas, alternative approaches. Example use cases:

- News (like RSS)
- Webcam publishes a new photo when it detects motion
- Subscriptions to identifier metadata, e.g. push of WebFinger or DID documents to clients who can be certain to always be current without polling.
- Subscriptions to key updates, get immediate notification of key rotation etc, no polling required

Developed as part of [Dazzle](#), but intended as a component that can be easily added as an orthogonal component in lots of applications.

[Found post-session this related work: <https://reb00ted.org/tech/20221024-pupupubsub/> but note that what Johannes presented cleverly uses the [Link HTTP header](#) so that this can be used on the open Internet as described above. Everything needed for the P3Sub protocol is provided through HTTP headers so that everything else can be done in the usual way. See the [protocol link](#) at the top for the specific "rel" values used to annotate those links. –Bruce Conrad]

Veramo – DIF Building the community-led supermodular framework for decentralized agents

Session Convener: Nick Reynolds

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 Governance Who? What? How?

Session Convener: Wendy Seltzer (Tucows) ([Wikipedia](#))

Session Notes Taker(s): Rohit Kare, Paul Trevithick

Minor note: IGA (identity governance and administration) is a term of art in IT for who gets a badge, reviewing who has access, enforcing joined/mover/leaver processes, etc. This "Gartner Analyst" sense of IGA appears distinct from the discussion in this session. – RohitKhare

WS: There are many kinds of governance, I'm mostly interested in "ecosystem" governance.

WS: How do we get the stakeholders together to work on collective governance? (e.g. agree to abide by IEEE P7012)

WS: There are several examples of failed experiments (e.g. W3C P3P).

Adrian Gropper (AG): I think this is the wrong question. People don't want a digital identity, they want an address, a reputation, a credential, or anonymity (e.g. for activism, or journalism), or to be left alone, or freedom of association and assembly.

Doc: we've thought about identity for so long is one thing, but what people what is one of the above.

PauliT: It starts with stakeholders with common ground. Each has to have an incentive to cooperate.

Erica: a need for fluidity...sometimes you want a permanent relationship, sometimes not. Lots of ways to interact.

MaryHodder [remotely]. We've all been working in the exhaust of identity (e.g. credentials). Companies use that to create identities. But IRL we do it so naturally that we don't think about it. It's been reductionist (e.g. to use the email) and not working. I think people are ready to put in a little bit of work. What is this common ground? Do we need lots of little governances? Is it identity in context (and thus governance in context).

Drummond Reed [DR]: What do you mean by "identity governance"? We have "digital trust ecosystem".

WS: bring the stakeholders together to find consensus to find the attributes of a user-centric identity. A mixture of tech choices and interoperability.

Joyce: We think of our individual identity and "governance" is about when you're in a group. So now that we're digital and we need identity (at least identifiers)...

AG: the first step has to be whether you're talking about people or not. One of the failings of this community is we seem to insist whatever we develop applies to both people and [entities]. If you're talking about people, it's clear we're governing the relationship between a biometric and an identifier. And if you're not talking about people, there is no self-sovereignty.

WS:I think we're talking human.

Ben Go: most of the time it's 90% the people involved in the standards. We need something.

PaulT: The problem is individuals don't engage in collective action.

WS: power to the people (incl the underserved)

Doc: how can all the relying parties...

DonT: can you describe the governance of Facebook? they have a contract with the user, and contracts with advertisers, and a BOD.

WS: FB is a bit constrained by TOS, a bit more by regulations, a bit by advertisers and partners and the user may think the only choice they have is accept or go elsewhere. This is a sphere of governance.

AG: When you ask the way Don asked, you're going way beyond identity governance. If you want to stick to the prime directive [Star Trek] related to humans and that's the human/universal right to freedom of association and assembly.

Erica: WRT Facebook: crappy situation for end users because their incentives are for.

Manu: focusing on the entrenched platforms. We want to anticipate a future where these no longer exist. I think about the number two. Let's think about incentives for them.

PT: Totally agree. It is very hard for the #2 players. It is hard for them to compete with the top players.

Doc: I agree with Adrian. Respect users. They want to be in a state of anonymity.

Drummond: Don, would Facebook issue all of us a credential of everything they can attest about us. Would they issue that into a digital wallet.

Don: No. Because they consider this their property.

Drummond: there's a lot of value in this data, so they won't give it up

WS: how do we [the people] aggregate enough power to strongly state our human rights.

AG: in the EU Digital Services Act [DSA] segregating the top firms ["gatekeepers"]. Maybe we should look for universal things to diminish the influence of lobbying.

Don: You asked who represents the people, the answer is representative government.

Manu: When I talk about the second tier... I was just trying to clear our mind-space from overly focusing on the titans. I think this was just a tactical move.

Manu: the EU is very interested in universal solutions that will restore a level playing field.

Minimum Interoperability Profile for ACR (authentication context)

Session Convener: Pam Dingle

Session Notes Taker(s): Mike Schwartz / Pam Dingle

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

Pam wrote a white paper describing how to map SAML AuthnContextClassRef to OpenID Connect acr and amr claims. In SAML, the AuthnContextClassRef request param must be strictly enforced by the IDP, whereas in OpenID Connect, the OP may ignore it.

GTRI Trustmark Website from <https://trustmark.gtri.gatech.edu/>

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

- Using OpenID Connect claims param may be tricky for vendors because it's a very powerful capability that may undermine security.
- The OAuth Stepped up RFC [9470](#) (OAuth Step Up Authn) requires acr to be optional
- It would be great if the OP could publish in its metadata what is the acr-to-amr mapping.
- A conformance test would help show which OPs conform with this specification
- Proposing OpenID Connect AB working group to take this on

The many different flavors of Selective disclosure + the Future of Consent

Session Convener: Francisco Corella, Neil Thomson

Session Notes Taker(s): Neil Thomson

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

[Flavors of Selective Disclosure](#) - part of mDL Presentation

[Future of Consent](#) - PDF presentation link

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

This presentation takes two views of Consent and Selective Disclosure

Francisco Corella presented on some new variations on crypto-graphically secured and algorithmic means of presenting a sub-set of claims within a credential, while providing a verifiable link to the Issuer of a credential. This includes the techniques presented in the following slide from the presentation:

Comparison to other methods of selective disclosure

- Based on hash functions
 - Selective disclosure of JWTs (SD-JWT)
 - Oauth working group
 - [draft-ietf-oauth-selective-disclosure-jwt-05](#)
 - Merkle tree with typed nodes
 - US patents 10,567,377 and 11,329,981; [rich credentials](#)
 - Presented at IIW XXIII, 2016
 - X.509 certificate with selectively opened folders
 - US patent 6,802,002
 - Presented at RSA 2000
- Based on proofs of knowledge
 - Anonymous credentials
 - [Camenisch-Lysyanskaya](#) signatures 2002

Neil Thomson (QueryVision) presented on the Future of Consent

Bold Statement:

Meaningful Consent on Data is beyond all but the 1% (e.g., IIW attendees). Privacy is dead; Confidentiality may be possible

This (and other presentations at this session of IIW) have pointed out issues with the concept of requiring informed consent by all online service users (including your mother or grandfather).

- Much of your PII/PD information has already “leaked” online, whether through previous disclosures which have been shared (with or without permission), collected through inference, correlation, or by the user’s behaviour in online applications and services.
 - Privacy has already been violated. The best that selective disclosure can do is define which data you do approve for processing (which is beyond current consent requirements)
 - Confidentiality may be possible (with stronger consent scope definition) to restrict the distribution and exposure of data and data processing result to parties other than the Verifier.
- The ability to infer and acquire PII continues to accelerate as demonstrated by a paper on correlation of VR headset/glove mapping to PII, presented at the ToIP AI and Metaverse TF earlier this year (link to [meeting notes](#), which includes the link to the meeting recording, including this presentation)
- Legal proof of valid consent is impractical. For consent to be valid the subject must demonstrate an understanding of what is being agreed to, plus the potential harms.

For verifiable <things> such as Verifiable Credentials (VCs), this includes understanding:

- The data, including relationships within the data
- The data processing that will be done with the data (including combining with other data)
- The purpose of the processing
- The final result/work product of the data processing and how it will be used

In medical procedures, particularly experimental and drug trial scenarios, this literally requires that a subject matter expert (typically a consent/privacy lawyer) be in the room to question and verify the subject's comprehension.

With that requirement, only 1% of the population (e.g., attendees at IIW) could reasonably meet these comprehension requirements for valid consent.

DEEPFAKES +AI Threats to ID Proofing + verification systems “AI is Rocket Fuel for Fraud”

Session Convener: Andrew Hughes

Session Notes Taker(s): Andrew Hughes

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

<https://kantara.atlassian.net/wiki/spaces/DGDF/overview>

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

- Discussed how ID Verification systems work at a high level
- Discussed how they are vulnerable to spoofing and bypass
- Discussed how AI will speed up attacks and lower costs
- Discussed some of the techniques in use today to use generative AI / simulations to fool systems
- Invitation to all to join the Kantara DeepfakesIDV discussion group (link above) to build a knowledge base and material for communicating the concepts to a broader audience

Notes Day 3 / Thursday April 20 / Sessions 11 - 15

SESSION #11

Stitching Together a Web Wallet - What's there & What's missing

Session Convener: Niels Flensted-Jensen, John Bradley

Session Notes Taker(s): Niels Flensted-Jensen

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

wwwallet.org - uses passkeys to log in/sign up (PWA)

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

A web wallet in this session is defined as a web application, basically an single page application

The high level problems to be discussed:

- registration of web wallets
- issuance of VCs into the wallet
- presentation of VCs from the wallet

The session then centered around the use cases that can drive the browser and ultimately OS vendors to support web wallets. The library scenario where users show up with their private hardware keys.

The general challenge seems to be to convince the browser and OS vendors that native apps may not always be the answer. (Let alone that people would prefer browser apps over native apps out of principle)

Selective Disclosure is useless

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

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

Examples of Ephemeral privacy?

short lived privacy

a zkP?

The bar example of proving you're 21.

The problem is the context of that zkP presentation is easily identifiable, a security camera, or a credit card bill from the bar.

Simple merging of datasets can allow for re-identification of anonymized data.

Privacy washing: anonymized data but which can be reidentified

Safe Harbor: to get into the business of selling data that can be re-identified but the seller is free to do so as it was originally "privacy washed".

Privacy isn't dead, but confidentiality is better.

There is a ray of sunshine:

Bar example - proves they're over 18, correlated by facial recognition and a credit card bill fully correlated.

But can "some technology" bind the bar during that initial presentation to how

SD is privacy through obscurity.

Privacy through confidentiality.

IEEE p7012

<https://standards.ieee.org/ieee/7012/7192/>

Is the cost of doing SD out weighing the benefit?

SD is good, SD is better with contractually protected disclosure. SD without CPD is a waste SD is a false sense of privacy.

Paper on:

Beyond consent... Internet safety labs (<https://internetsafetylabs.org/resources/>)
<https://ieeexplore.ieee.org/document/9031549>

Data Privacy best practice K-Anonymity with a given k size, where you can't release data where the

rows contain the same data are less than k. Data is valuable so you want k to be as low as possible. k could be 2.

Data is merely generalised.

Quasi-identifiers are things like, zip code + age + gender.

You don't know if you're creating quasi-identifiers in your anonymized data set.

4 data points are enough to do re-identification if a cell phone is in use.

QI Linkage Attack

Interaction Profiling Attack

Contextual ... Attack

Down-coding Attack

Complex Predicate Singling Out Attack

Merge attack

If the verifier is in control of the context of the SD presentation contextual data will allow reidentification.

Shouldn't dismiss motive for sharing data to be correlated in order to receive services.

It is the combination of economics and regulation that enforces where or not companies want to comply.

Is there a solution?

Chain link confidentiality - implemented in ACDC (<https://github.com/trustoverip/tswg-acdc-specification>)

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2045818

privacy requires legal economic and technology

Utah is working on a comprehensive privacy policy, ephemeral privacy (SD) vs sustainable privacy

I have some additional notes here:

<https://ericscouten.dev/2023/iiw/#session-11b-selective-disclosure-is-useless-we-have-receipts>

Compassion.IO (How to give/receive help in the virtual world, safely, securely, reliably)

Session Convener: Samuel Hutchens

Session Notes Taker(s): Trent Larson

Participants: Samuel, Jesus with Entidad, Joe Andrieu, Jack Gretsch, Brent Shambaugh, Trent Larson, Thien-Nam

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

American Red Cross had success in Sri Lanka because of the media coverage.

Keva is helping and connects stories

Starts with a stove under \$200 using pellets and yields carbon credits.

KindSpring.org Stories show kindness from strangers.

Since internet interactions are captured forever, so can we capture.

These are stories of 1:1 but also community.

Need more expressivity, like tipping or thumbs-up that don't interrupt the flow. We get that in person with micro expressions.

Mark Zuckerberg did a demo of a VR which showed more emotions.

Building for accessibility shows concern for less able in some areas.

Are there things we can do for people who don't have a device?

Kids had to sit outside a Starbucks to get wifi during covid.

Syrian refugee was helped via decentralized technology. Accenture assumed people have smart phones. Stewards had a device that users could borrow; started with wristband, worked toward a secure component.

Our personal devices are typically only our own. In disadvantaged communities, they may want to share.

<https://www.howtogeek.com/333484/how-to-set-up-multiple-user-profiles-on-android/>

Entidad is supplying phones to households. Often they go through multiple phones.

Party lines were fun, especially when we started using modems.

Pay phones are disappearing, and companies don't allow free restrooms in some areas.

The other side of compassion is cynicism. How do we limit that?

There are often scams after disasters.

Some would rather give directly over organizations.

Sean Conway started IXO based on Cosmos for the Internet of Impact, for gathering money and measuring resulting impact. One region requires a Minister to payback.

Maybe we create a profile where givers can show what they have and recipients can show their needs.

Patren allows for rewarding artists.

Time Banks like Berkshares.

Lawyers work for pro bono to help, with the full weight of their legal profession.

GoFundMe is more targeting real need. Successful campaigns are people who already have the reach.

Santa Monia put a caseworker on the most problematic people, which was cheaper than the emergency services. SLC is building homes for homeless, which is cheaper than serving them other ways. Maybe activists will be more able to link together those who need with those who have. Many view success as having money, but there are many other ways we want to grow.

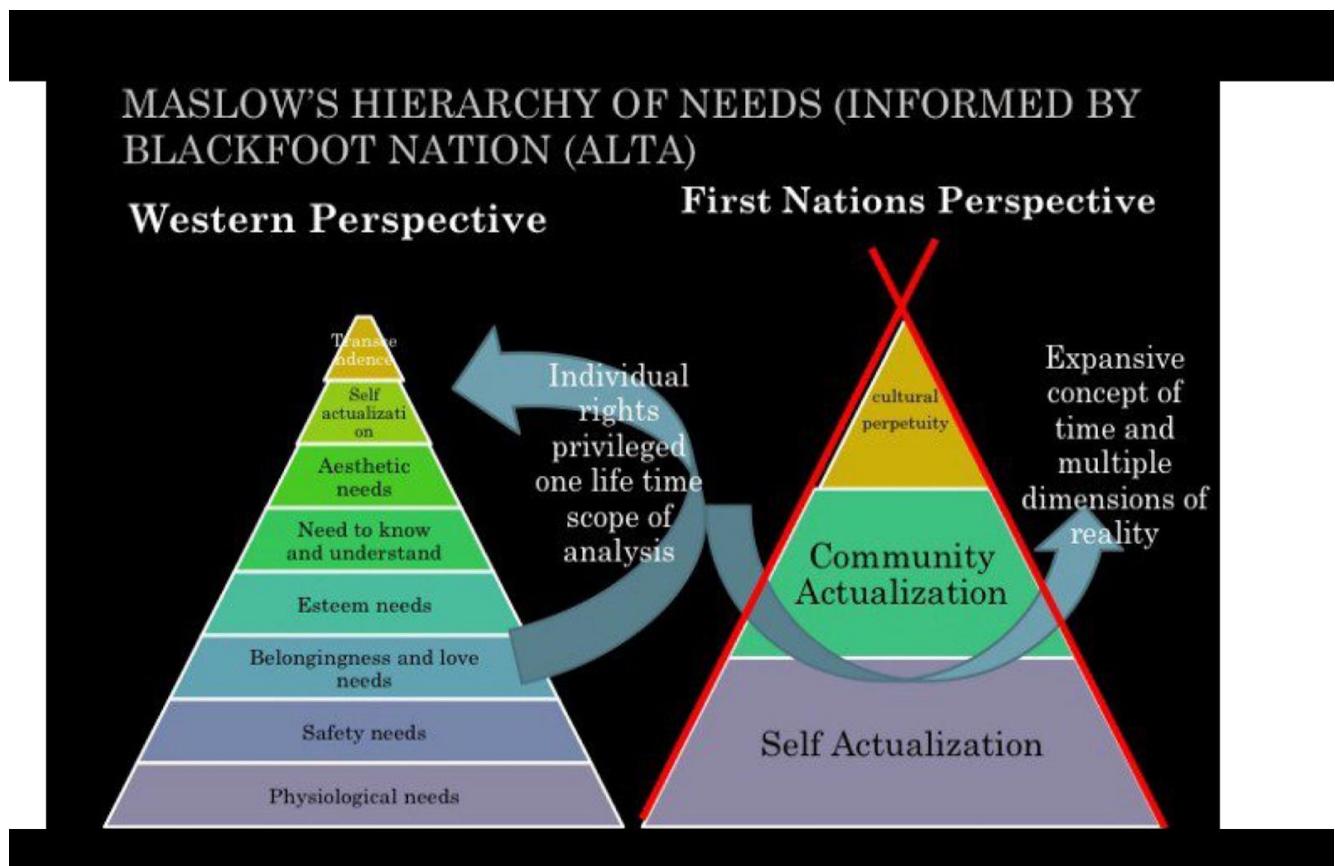
Self-sovereign identity isn't so much about owning my own identity but more about creating new institutions based on our own connections.

Lives of Giving aims to reflect time that's given, hoping to organize & coordinate that more. We could extend the ideas of offering time much like pro bono work, with professionals. Some of that is for standards.

Let's train people to be their most authentic self rather than being a corporate employee.

Maslow's hierarchy of needs was inspired by the Blackfoot nation which had a communal hierarchy of needs. (See diagram below.)

The root of "fascism" is a bundle of sticks: we're stronger when together, but we're actually stronger when each of us are aligned on a shared goal.



OID4VC Interop Profiles Convergence

Session Convener: Torsten Loddersted, Kristina Yasuda & Harmen Van Der Kooij
Session Notes Taker(s): Jin Wen

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

Some backgrounds (with the help of AI tool like perplexity.ai):

JWT VC (JSON Web Token Verifiable Credential) and SD-JWT VC (Selective Disclosure JWT Verifiable Credential) are two different formats for representing verifiable credentials. Here is a comparison of the two formats:

JWT VC:

- JWT VC is a combination of JSON Web Token and a canonical Verifiable Credential[5].
- It uses an external proof, meaning the signature data is not embedded inline with the credential, but detached from the credential[5].
- JWT VC can only have one signature, affiliated with one issuer[5].
- It can only have one credentialSubject object within it, as the JWT sub claim can only contain a single value[5].
- JWT VC uses the "not before" (nbf) claim instead of the "issued at" (iat) claim for the issuance date[5].

SD-JWT VC:

- SD-JWT VC is a superset of JWT and is based on the well-established JWT content rules and extensibility model[1]. It allows for the selective disclosure of claims.
- It supports JWS JSON serialization, which is useful for long-term archiving and multi-signatures[1].
- SD-JWT VC can contain claims that are registered in the "JSON Web Token Claims" registry, as well as public and private claims[1].
- It uses the media type application/vc+sd-jwt[1].
- SD-JWT VC must be encoded using the SD-JWT Combined Format for Issuance[1].
- When there are selectively disclosable claims, SD-JWT VC must contain all Disclosures corresponding to their SD-JWT component[1].

In the context of DIF Presentation Profile [4] (Decentralized Identity Foundation), DIIP (Decentralized Identity Interoperability Profile), and HAIP [6] (High Assurance Interoperability Profile), SD-JWT VC offers more flexibility and extensibility compared to JWT VC. SD-JWT VC supports selective disclosure, which allows for more control over the information shared in a verifiable credential[1]. This makes SD-JWT VC more suitable for use cases that require selective disclosure and multiple signatures.

Citations:

[1]<https://www.ietf.org/archive/id/draft-ietf-oauth-sd-jwt-vc-00.html>

[2]<https://www.w3.org/TR/vc-jose-cose/>

[3]https://bm.linkedin.com/posts/paul-bastian-1970b1195_credential-format-comparison-and-idunion-activity-700804294723349632-jDnZ

- [4] <https://identity.foundation/jwt-vc-presentation-profile/>
- [5] <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/decentralized-identity-verifiable-credentials-deep-dive/ba-p/3690641>
- [6] <https://vcstuff.github.io/oid4vc-haip-sd-jwt-vc/draft-oid4vc-haip-sd-jwt-vc.html>
- [7] <https://identity.foundation/jwt-vc-issuance-profile/>

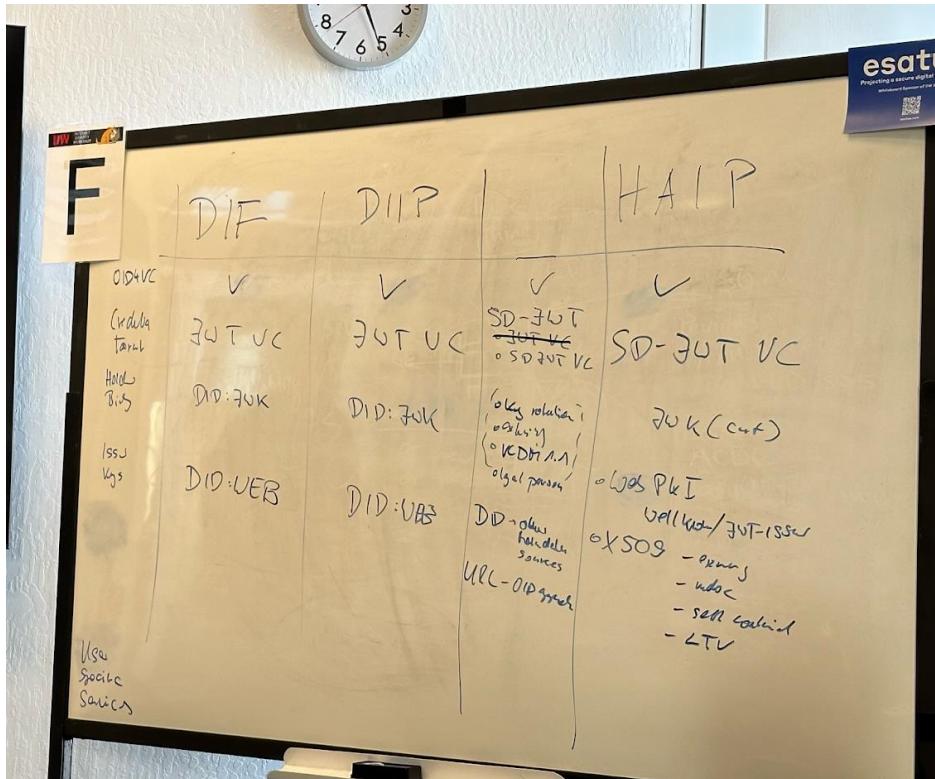
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

This is the continued discussion of Day 2 Converging OID 4 VC Profiles, link here:

https://docs.google.com/document/d/1KwcJYN7DfKk_ZjxFMRcOigVtLSdiiVVK6FdaFUcsZT8/edit

also related session is Augmenting OID4VC with DIDComm / Sam Curren,

https://docs.google.com/document/d/1KwcJYN7DfKk_ZjxFMRcOigVtLSdiiVVK6FdaFUcsZT8/edit



Key Understandings:

- There are three different profiles being discussed: DIF, Dutch Decentralized Identity Interoperability Profile (DIIP), and OpenID4VC High Assurance Interoperability Profile I(HAIP)
 - <https://github.com/decentralized-identity/jwt-vc-issuance-profile>
 - <https://github.com/decentralized-identity/jwt-vc-presentation-profile>
 - <https://www.dutchblockchaincoalition.org/bouwstenen/diip-2>
 - <https://vcstuff.github.io/oid4vc-haip-sd-jwt-vc/draft-oid4vc-haip-sd-jwt-vc.html>

Outstanding Questions:

- Can the different profiles converge into reasonable interop profile listed in the unnamed column in the table
- How can the different credential formats be reconciled?
- Is there a need for key rotation in cryptographic holder binding?

Observations:

- The group discussed the use of X.509 certificates for long-term validation and offline use
- New DID:KERI a decentralized KMS does not rely on blockchain (<https://keri.one>)

Action Items and Next Steps:

- Create a document outlining the different options for credential formats, holder binding, and issuer key management to facilitate further discussion and decision-making.
- Consider separating discussions on natural persons and legal entities to better address their unique requirements.
- Investigate the possibility of using well-known locations for key management and metadata retrieval.
- Continue discussing the use of DIDs and their potential benefits and drawbacks in various scenarios.

The suggestion is to continue the discussion at the OID4VC DD Task Force at OWF

<https://tac.openwallet.foundation/task-forces/OID4VC-due-diligence/>

BUBBLES? Federation in disadvantaged and disconnected environments

Session Convener: Justin Richer

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

VC 'render Method' displaying & rendering verifiable credentials / DCC

Session Convener: Dmitri Zagidulin
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

Bhutan: National ID and SSI

Session Convener: Ethan Veneklasen + Drummond Reed
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 #12

BRAINSTORM: Digital identity as a tool in the fight against online Child Sexual Abuse Material (CSAM)? [Privacy vs. CSAM]

Session Convener: Michal Karnibad and John Wunderlich
Session Notes Taker(s): Andy Lulham

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

Type Here Child Sexual Abuse Material, Privacy, Freedom of Expression

<https://www.iwf.org.uk/news-media/news/extreme-category-a-child-sexual-abuse-found-online-doubles-in-two-years/>

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

Session introduction:

The National Center for Missing and Exploited Children has seen a 329% increase in online illegal content in the form of child sexual abuse material reported in the last five years. In 2022 alone, the same organisation received more than 88 million CSAM files. We will lead a brainstorm examining if and how digital identity can plan a role in helping to solve this problem.

Setting the scene - the two extreme scenarios:

1. Do nothing. CSAM remains visible and easily accessible across all user-generated content platforms. Society has a big problem - it ruins kids' / people's lives, destroys mental health etc. It's reasonable to assume this is not a viable option
2. Do everything: every single UGC platform prohibits content uploads without a digital identity check associated with it (ensuring an audit trail for anyone who attempts to distribute (or appear in themselves) CSAM. A necessity for law enforcement purposes. Not a viable option due to:
 - commercial implications
 - implications on privacy, freedom of expression etc.
 - Clarification: identity checks are/would be done for three reasons:
 - Check the content uploader is old enough to be posting on that platform (not necessarily a legal requirement)
 - To ensure identity is retained for anyone guilty of sharing CSAM content
 - To ensure identity is retained for content uploaders also appearing within CSAM content

- Note: that the significant majority of CSAM perpetrators are known to the victim e.g. teacher, pastor, family member etc.
- Escrow concept: what about this concept? Where a third party has 'signed' and validates an identity. This can only be unlocked using a private key once suspected illegal activity has occurred

Now let's consider the guiding principles of how we address the problem. Two inverse options:

1. Collect identity data of everyone = when you detect illegal activity you have information on the offender. Often considered surveillance only to find a tiny minority
2. Once an offence has been committed, then go and identify the offender

What is happening right now?

- Reality is that ISPs are 'scanning' (moderating) content as standard in lots of countries in the western world

What about what Apple tried to do a while back?:

- There are a handful of databases of hashed known CSAM images. Apple proposed to scan all images against these database before they left a device - received a huge public backlash (later in the session it was said that alongside this backlash the Apple technology didn't actually work)

Opinion: Privacy and anonymity - it is only reasonable that anonymity disappears once a crime has been committed (linked to point 2 above)

Question: there are numerous examples of transacting online where a process takes ~10-20 seconds to process (e.g. confirming a flight booking). Is it really that bad that a similar delay happens for screening purposes when someone uploads content to a UGC platform? Definitely would need regulatory standards and enforcement

Trust: even if it is reasonable for content to be scanned or moderated, how do we know who is doing the screening and how?

Hashed databases: only a handful of organisations have a big, official database of hashed images = do we therefore trust Microsoft, for example, and other similar organisations? Related to this: legislation means the above hashed database process cannot happen locally, and can only be done via a central database.

Theory: AI/ML models to detect CSAM material can also be 'flipped' to create artificial CSAM material. Should this be created and used by perpetrators? But will they just 'consume' them or will they also do other bad things in the background?

Theory: content submitted > content hashed locally > sent to hashed database (encrypted) and if there is no match then the content gets published?

Social impact question: everyone wants bad actors to be caught and material intercepted but what is the social cost for everyone else? What are the implications for them?

Govt or legislator consistency: is it right to assume that the provisions made today will also be carried forward by the next government or legislator. Is that a risk?

Frustrating: comment that their frustration is that they've not read about a technical solution that is genuinely effective in combating the problem. (see above) Apple failed because it's solution to scan images as they left the device didn't work.. not just because of the public backlash.

Pushback (Andy Lulham): that's all well and good but can you always wait for 100% AI accuracy? Surely doing something is better than doing nothing? Are false positives ok if they are then sent to be validated by humans?

Concern: you can have the identity-related legislation but bad actors will move to servers not under these jurisdiction.

Hammer and nail (societal) problem - the content creation and sharing is actually only 0.1% of the human problem - the abuse in the content is typically only a small part of a long process. If 1 or 1000 people see an image, is the abuse the same?

Law enforcement: irrespective of the issue, half of the FBI's files are unsolved CSAM problems. Does that lack of resources mean that the problem shouldn't be addressed at source?

Theory: paedofiles are some of the most determined and persistent criminals. But part of what makes them a criminal means they simply don't believe they'll get caught...

A conclusion: Two key questions / clarifications:

1. How do we empower the people who have been abused by advanced technology?
2. Actually, it's CSAM + privacy, not CSAM versus privacy

The SR-71 Could Not Fly without me

Session Convener: Britt Blaser

Session Notes Taker(s): Britt Blaser

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

[My God, it's full of Mentors! Doc Searls and Ben Bowles.](#)

Clueplane to Cluetrain, A Personal Cross-Country



Doc Searls stayed here this week while keynoting the Conversations Network event, “[Revisiting Cluetrain – 10 years later](#)”. I’ve been working on this blog post for 3 months, and I wanted to present him with some atoms to celebrate the anniversary, so Ben and I cooked up a plaque so suitable for framing that we did. Thanks to both you guys: I wish I could deploy all your clues:

For Doc Searls: Thanks for keeping the Recon tradition alive! Back in the day, negatives were 9"x 9" and the geotagging accurate to the foot. 2100 miles and 600 prints per hour. The cost per frame? Stratospheric. *Ben Bowles, Lt. Col., USAF, Rtd. AKA Doc Searls, version 1.0*

Topaz - Demo Open source, fine-grained, policy-based, real-time authorization service

Session Convener: Omri Gazitt

Session Notes Taker(s): David Brossard

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

- [Topaz / github](#) (stars appreciated! 😊)
- [Zanzibar: Google's Consistent, Global Authorization System](#)
- [Cloud Native Computing Foundation Announces Open Policy Agent Graduation](#)
- Open Policy Agent's [Policy Language](#) (Rego)
- [Introduction | Topaz](#)
- [Open Policy Containers](#) (OPCR) - build OPA policies into immutable container images. A CNCF sandbox project. [github](#) (stars appreciated! 😊)
- [Aserto](#) - primary maintainer of Topaz, also has a commercial control plane product for central management of distributed Topaz instances

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

Overview

Authorization is finally having its moment. Topaz is “cloud-native authorization”. It can also be called externalized authorization. The idea is that authorization is neither part of the authentication ceremony nor the app itself.

Authentication is about getting an access token, setting scopes, and getting claims back. However, this only works for simple apps. Most apps have resources that require a more complex model that cannot be elegantly expressed using OAuth scopes.

Take Google Docs for instance: scopes alone are not enough. In fact, Google uses Zanzibar to handle its authorization (user, action, object). Topaz is meant to address this type of authorization:

1. fine-grained
2. policy-based: use policies to express authorization and extract it from the apps.
3. real-time: in the authN world, you present some evidence and you get a token that has a lifetime (minutes or days).

Topaz is fast, flexible, and easy: ~1 ms decision making.

Fast: This requires all the data to be local.

In ABAC, we have the P*P architecture (PAP, PEP, PDP, and PIP). PIPs are remote data endpoints.

In Topaz's architecture, data is local.

Flexible: support all *BAC models (RBAC, ABAC, ReBAC...)

Easy: we have PEPs for developers. We target developers. SDKs for different languages (Javascript, Typescript, Go, Ruby, Python, Java, .NET, ...) and protocol bindings (gRPC, REST, graphQL)

Why Topaz?

We saw seemingly mutually exclusive ideas. The policy-based approach (ALFA, Cedar, OPA) and the Zanzibar approach.

Topaz uses OPA. OPA uses Rego as a policy language. It's a side-effect free [programming language](#) derivative of Datalog.

Zanzibar focuses on the data model and the globally consistent earth-scale approach. Zanzibar provides many features such as transitivity. Zanzibar uses a graph traversal algorithm. Each edge is a relation. Relations can carry permissions. If there is a path between a user and an object, access is permitted.

Topaz = OPA decision engine + embedded [BoltDB](#) database (gRPC contract) that stores the Zanzibar data model + set of OPA built-ins to access the Zanzibar directory. Along with a set of APIs to get data in and out, load policies, and of course make authorization decisions.

Demo:

Start by defining a model & relations e.g. viewer can be a user or a group. This becomes the domain model.

You can then define permissions.

Topaz contains an ETL process to extract data from common sources e.g. Okta, Auth0, and others. An authorizer takes a policy, runs it in the context of TOPAZ, they are written in Rego.

Sample Policy

```
allowed {
  ds.check_relation({
    "object": {
      "key": input.resource.tenant,
      "type": "tenant"
    },
    "relation": {
      "object_type": "tenant",
      "name" : "member"
    },
    "subject": {
      "key": input.user.key,
      "type": "user"
    }
  })
}
```

Sample Request/Response

Topaz has its own request/response schema/protocol to send authorization requests and get a response back. It also supports OPA's general query format. The reason for Topaz to introduce its own schema is to make it more authorization-specific.

Deployment Model

- k8s: either as a sidecar in the app pod, or its own microservice that can be scale via a ReplicaSet
 - container image can run anyway
 - can be run as a binary (support for linux amd64/arm64, windows, darwin amd64/arm64)
- One control plane (commercial offering) to any number of authorizers (OS).

Future

The future of Topaz is to compile policies into [WASM](#). Topaz becomes a WASM runner.



Cookie Binding as a Browser Standard

Session Convener: Kristian & Sameera
Session Notes Taker(s): Aaron Parecki

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

Microsoft

<https://github.com/MicrosoftEdge/MSEdgeExplainers/tree/main/BindingContext>

<http://aka.ms/bpop>

Google <https://github.com/WICG/dbsc>

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

Cookie theft problem has started to grow in popularity. Malware clones cookies from the victim's computer onto the attacker's computer to be logged in. Now that phishing is solved, attackers are moving on to stealing cookies which bypasses MFA.

This is particularly a problem for desktop environments, because there is no secure storage available unlike on mobile browsers.

Both existing proposals attempt to solve this.

Google Proposal:

Key is created on a TPM, cookies are signed with a key and nonce. There is also a session, because TPMs are slow (~500ms to sign). Built on regular web standards: JS, HTTP headers, etc.

Google proposal focuses on consumer use case. MS focuses on enterprise use case.

Privacy should be a key feature for consumer use cases, but for enterprise use cases we want to know exactly what device and be able to correlate devices.

TPM - lives outside the CPU, has a private key, the private key cannot be extracted. There are OS APIs to create a private key and sign something.

Can we add this to the authentication flow e.g. WebAuthn? Currently the proposal is just for single-origin cookie binding.

Federation use case - can you ensure the same browser is making the request to the RP and to the IDP? Would require cross-domain public key proofs. Maybe add something to FedCM to accomplish this?

The Google proposal is already prototyped in Chrome.

Tie to WebAuthn - if you already have a session, you could put the public key for the session into the ClientData.

The website should be able to decide whether a cookie should be bound. Some sites will not want to bind cookies.

Previous solutions (Token Binding) bound the cookie to the transport layer, so if you moved from home to the office to a VPN, the binding would break. The new proposals bind to the device at the application layer, not the transport layer, so you can move locations/VPN and keep the same cookie binding to the device.

Philosophy of the Crowds - Moral construction in the age of Internet Identity

Session Convener: Thien-Nam

Session Notes Taker(s): Rex Peacock

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

Diamond Age Designs for the Pluralverse

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

We discussed the differences between morality vs ethics, and what it might look like to design systems that are informed by Moral Constructivism, and a world where we encounter many different systems of morality and need to coexist. This led to discussions about the scale and granularity of groups, of moderation, and how we can structure conflict resolution

Progression of Western Philosophy:

- Virtue Ethics
 - Aristotle, Aquinas
- Divine Command
- Deontology
- Utilitarianism
- Moral Constructivism

Structures?

- Limits
- aggregation
- Scale / granularity
- Conflict resolution

Content?

- Pluralism

eIDAS 2 AMA

Session Convener: Paul, Torsten

Session Notes Taker(s): Wendy (partial)

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

Link to slides that were presented at IETF 117 SF about EUDI Wallet (includes a list of use-cases):
<https://datatracker.ietf.org/meeting/117/materials/slides-117-oauth-sessa-state-of-play-of-the-european-digital-identity-wallet>

Link to german eIDAS consultation process: <https://gitlab.opencode.de/bmi/eidas2> (in german)

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

Overview of state of play: eIDAS 2 regulatory text ~ this year. decided by trilogue, European Commission, Parliament, Council

Architectural Reference Framework, under revision to 1.3

Large Scale Pilot ~ mid 2025

Reference wallet implementation

Q&A:

[notetaker joined partway through]

Format? OpenID4VP?

ARF has a diagram at the end <https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline>

Attempt to come up with an agreement among 27 member states on technical requirements for interop

Trust framework,

Response to legal requirement that you reveal PIN?

Requirement to register and authenticate relying party

lots of things left open in the ARF (revocation, trust frameworks, ...)

Wallet API models: return URL or credential. Is latter model compatible with ARF?

A: it's not a technical standard yet; could be raised there.

ARF is a snapshot of the current requirements for the large-scale pilot.

Statement that credential must not be JSON-LD

two separate lines; linked data proofs,

key management not mentioned at all.

Breaking changes are still expected in ARF
Lots not yet in there, attestation

Timeline: ARF due to close at end of 2023; Implementing Acts 24; LSP 25;
standardization in CEN, ETSI

So many things yet to define. Identify, trust.

What will happen if member states can't agree?

Paul, expect consensus but it might be ugly

Torsten, we're trying to educate to help those around the table understand the issues

Consultation process is participatory

What is the implementing acts?

PRD vs architecture diagram

Legal text re unlinkability?

unique persistent identifier. 2 different proposals

Are the identifiers opaque?

up to the member state

Requirements to accept for signing, 2fa purposes

ongoing discussions.

"smells a lot like FIDO" what's the mechanism to suggest FIDO?

Discussion between FIDO Alliance and European Commission

"What are the chances this will actually work in the end?" given jurisdictional/cultural differences

Paul: you'll need to adapt both law and business processes, along with tech

Torsten: layers.

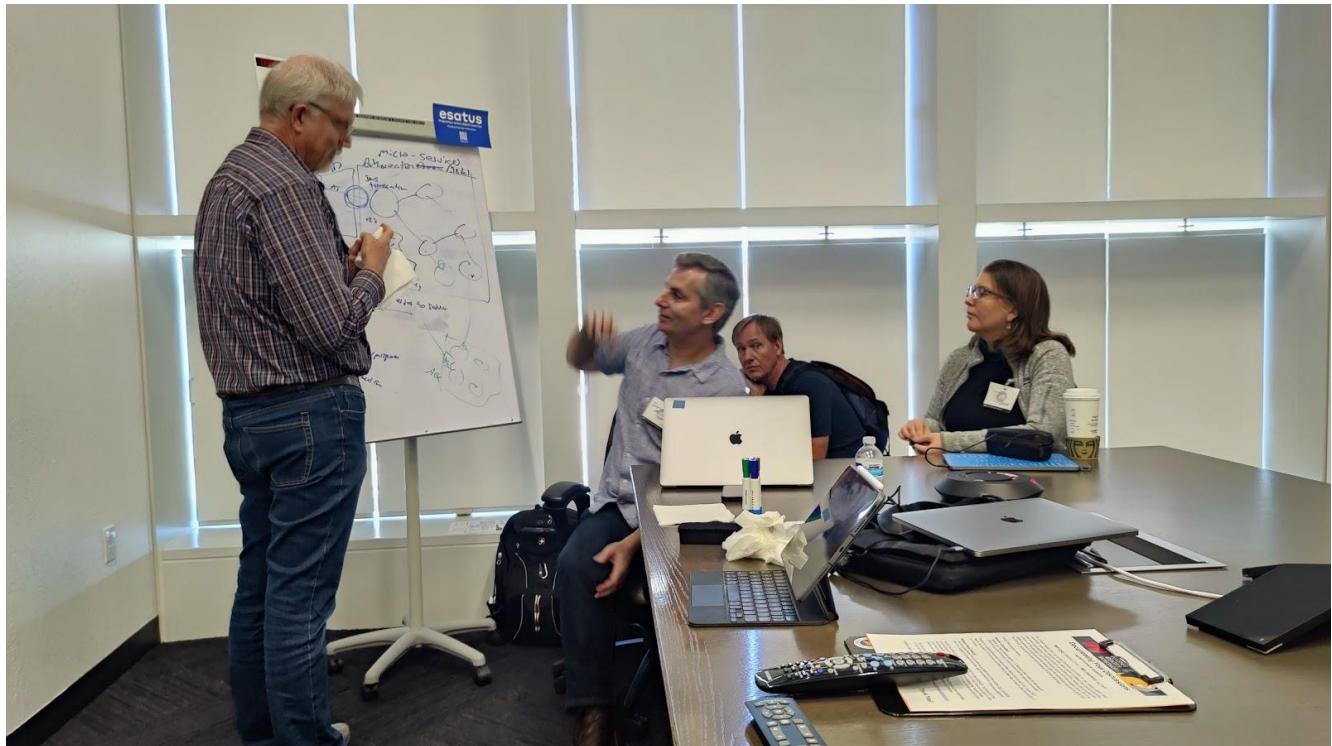
Transaction Tokens Authorization for Multi-workload environments

Session Convener: George Fletcher

Session Notes Taker(s): Mike Schwartz, Atul Tulshibagwale

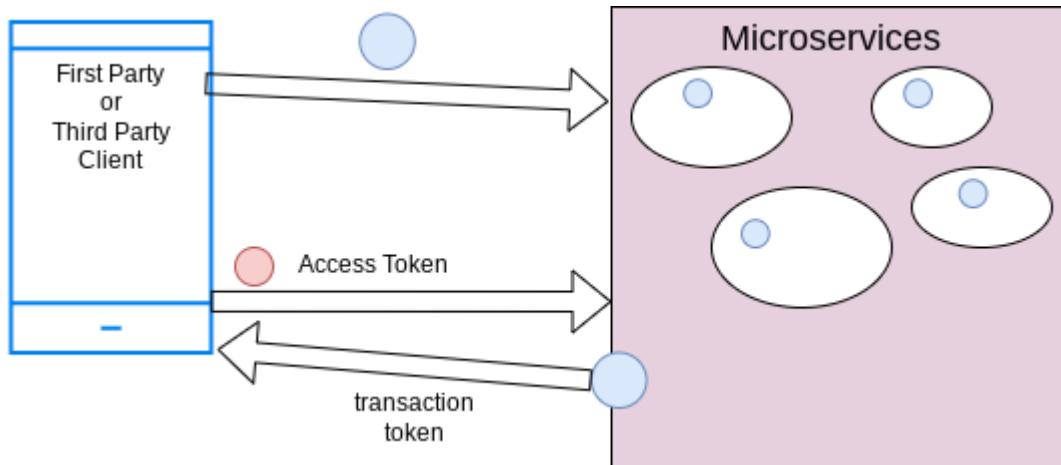
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Notes from Mike:



From left to right, George Fletcher (Capital One), Darin McAdams (Amazon), Bjorn Hjelm (Verizon) and Sarah Cecchetti (Amazon).

Session is presentation of this draft: <https://sgnl-ai.github.io/transaction-tokens/>



Call to endpoint with scope X, may call an endpoint that needs scope Y... then you have to go back to the user and re-authorize... not ideal. Using the access token internally in the microservices is problematic... especially if each microservice has to introspect the token. Also, we can't make the token atomic--we don't want the token to be revoked mid-transaction.

Perhaps we need a new token exchange service that mints a new transaction token:

```
{ "iss": "https://bank.com",
  "sub": "foobar",
  "transaction_id": 12345,
  "transactions_purpose": "some_action",
  "who_asked_for_it": "bank_mobile_app",
  "context": {...},
  "authorization_details": {OAuth RAR request JSON}
}
```

An example authorization could be “add stock to watchlist”, or “authorise wire transfer”. Token buckets is a new idea Justin is working on to bundle a number of related tokens. Potentially you could add immutable claims into the authorization_details. Netflix published a [blog in 2021](#) with a similar design pattern.

Net-net: The proposal is to create a new (possibly OAuth protected) endpoint to mint transaction tokens, for the purpose of a specific authorization.

Notes from Atul:

- Cross-domain trust is being handled separately, so this is just within a single authorization domain
- Number of OAuth scopes coming from the client are going to be fairly limited, because the consent has to be simple
- That means, the authorization domain representing the microservices is different from the authorization domain of the client (which uses coarse grained scopes)
- Instead of using the external OAuth token, we can create a new token for the microservices authorization domain - the Transaction Token
- () The authorization token can be opaque to the left and a JWT on the right (where the microservices are)
- () Calling the client part an authorization domain is incorrect because the client side is untrusted
- (Justin) With “authly” you can create a number of services with the same account. The token used to provision services didn’t have the rights to use that service, so you needed a new token / escalate the rights of the same token
- () Isn’t token exchange the solution to this?
- Adding OAuth tokens internally added a whole lot of complexity
- E.g. token introspection
- () In some cases, you may want to “up scope” the incoming OAuth token, because you don’t want untrusted clients some powerful scopes
- A call chain cannot be rolled back once started

- E.g. if the user changes their password within the execution of a call chain, you may end up with a partially executed transaction if you are using OAuth tokens internally
- () “Solving the Transitive Access Problem” paper presented earlier at a conference in Prague
- () This sounds very synchronous. How do we address asynchronicity?
- At the edge, issue a different type of token, which is focused on the transaction
- A lot of backends have no idea of the services invoked in the call chain
- The txn-token has:
 - iss
 - txn
 - sub_id
 - capabilities / purpose
 - azc
 - originator
 - context
 - authorization details
- () Are you also trying to bake into it the call chain part?
- (Justin) Token buckets will address the call chain part. We don’t want it to keep getting re-issued at every step of the way
- () Is the word “transaction” misleading? Should it be called a “request token”? - many disagreed with this
- () Isn’t this just token exchange? Do we need to call it something?
- () Having standard claims is good,
- (Sarah) If I am a new microservice, how do I know what purpose I’m going to be called for?
- The new service can limit what purposes it can be used for
- This is a complex problem, e.g. what purposes should be supported by a new service?
- () Service meshes have related functionality
- () Why not use a header that says this is a wrapper around the inbound token?
- (atul) not all of the context is inside the inbound token
- Replacement tokens
 - It creates a lot of complexity for the security model
 - It is allowed in the spec today
- () What happens when you have an externalised service that also talks internally?
- The spec doesn’t say anything about how the model is defined
- (Alan) I’d like to think of this in terms of attenuated delegation
- () Isn’t it easier because this is atomic?
- The trust boundary aspect is important, crossing trust boundaries is a whole another mechanism
- Token exchange is just a mechanism, it could be anything
- To cross authorization domains, you are not talking to the Transaction Token service, you need to talk to the AS.
- (Justin) MITRE has written an extensive paper about crossing domain boundaries
- () We also have third-party services that provide APIs. I wonder if Txn-tokens are useful in that case?

- The expectation is that TraTs are within a domain, and I should never see them outside the domain
- () The time limit is one thing, but the “one-time use” property is also required
- () You don’t want transaction tokens to be reissued multiple times
- The simple use case is that once a TraT is created, it’s never re-issued
- The content of the TraT is dependent on the actual transaction in question, the spec is not prescriptive about it
- () By value passing you could make the tokens really long
- () Having all the details in the TraT is important
- Any element of what the user / service is trying to do that is immutable can be inserted into the authorization details
- A few years ago, microservices allowed any user to be impersonated
- () This sounds like Twitter’s Finatra / Finagle context passing
- () Don’t you always need an inbound token?
- No, as long as you can know the service that is invoking the endpoint issuing the Transaction Token

Note added by Alan Karp

Solving the Transitive Access Problem for the Service Oriented Architecture (<https://www.hpl.hp.com/techreports/2008/HPL-2008-204R1.pdf>) is a paper that considers a similar problem. I don’t think it solves the problem discussed in this session, but it may contain some useful ideas

DIF = Decentralized Identity Foundation Update - What's the DIF? How to be involved + Hackathons

Session Convener: Limari Navarrete

Session Notes Taker(s): Limari Navarrete

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

[Updated DIF Overview for IIW, Fall2023, v1.3.pptx](#)

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

Overview of what is DIF and how to get involved. We reviewed DIF’s working groups and highlighted key work items. We also discussed DIF’s structure, the benefits of participation and recent activities including the did:hack hackathon, the creation of the DIF Korea SIG, BBS progress on the IETF standards track and the upcoming DIF Sponsored hackathon:

<https://dihackathon.devpost.com/>

University “Intro to Digital Identity”

Session Convener: Jo Windley

Session Notes Taker(s): Emma Windley

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

Key understandings:

- Creating a curriculum for an intro to DID course as there is no current course being taught at most universities.
 - Topic outline: Lecture, labs, assignments, readings, learning outcomes etc
- Determined it would be a senior level course that would include pre-requisites
- Following slides include all information discussed:

Composable P2P Identity Components on Holochain (not a blockchain)

Session Convener: Arthur Brock

Session Notes Taker(s):

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

Type Here

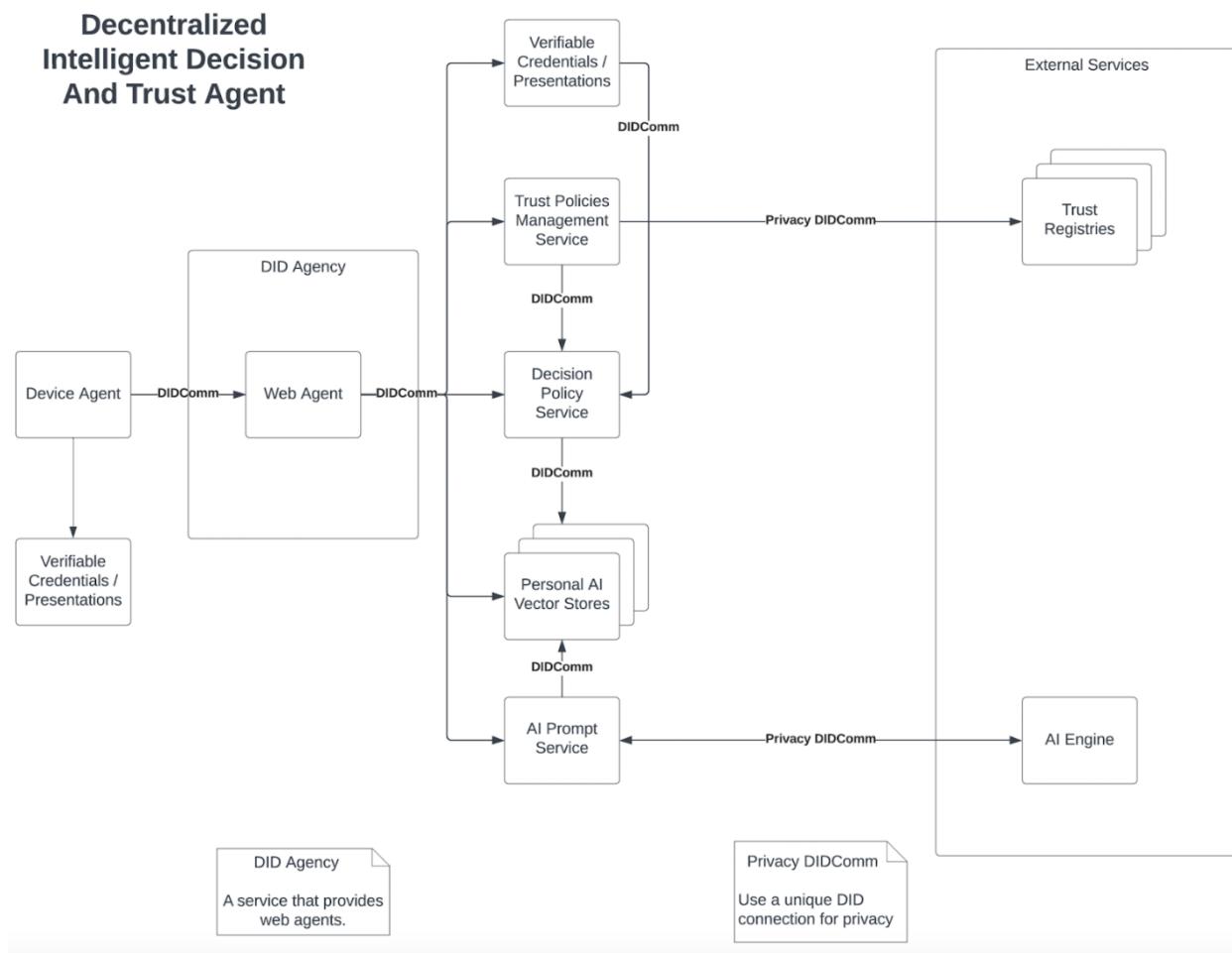
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

No Notes Submitted

DIDATA - Decentralized Intelligent Decision and Trust Agent

Session Convener: Matthew Hailstone
Session Notes Taker(s): Matthew Hailstone

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 main goal of the diagram is to emphasize the need for a decision policy service that can guide the user in decisions made when presentation requests, proof requests, or other requests are invoked on the agent/wallet.

Trust Registries would provide policy, lists of information, or any information that would be paired with credential types or other particular request types that give recommendations or guidance on how to process the data in the incoming request.

Embeddings stored as vectors in persistent storage can be used to interpret or filter data retrieved from an external AI Engine service.

The Decision Policy Service would take data from credentials, presentations, AI vector stores/AI engines and execute policies configured based on supported data models/modules consistent with the listed data types.

References to AI Vector Stores: <https://atoonk.medium.com/diving-into-ai-an-exploration-of-embeddings-and-vector-databases-a7611c4ec063>

<https://learn.microsoft.com/en-us/semantic-kernel/memories/vector-db>

DID Method Enumeration micro-spec

Session Convener: Sam Curren

Session Notes Taker(s): Daniel Bluhm

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

<https://github.com/decentralized-identity/did-method-enum/blob/main/spec.md>

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

Sam Curren discussed the DID Method Enumeration specification being developed with the Names and Identifiers WG at the DIF. The specification outlines how DID Method support is expressed in at least 3 different contexts:

- Feature Discovery in DIDComm
- Drivers in the Universal Resolver (and other resolvers) expressing which DID methods they support.
- Machine Readable Governance

There was some really good discussion on what we need to express and how we can achieve that. Originally, the presented specification targeted enumeration by a simple string, a prefix, or a method + features. After our discussion, we determined that there should be more exploration into expressing other requirements, such as what is expected to be present in the DID Document. Additionally, the features would have to be added to DID Method Specifications per DID Method. Following the discussion, it was determined that it seems unlikely that DID Method authors would update their specification to enumerate features. The most commonly needed feature is expressing which network is supported. So, rather than expecting this to be defined in the specification, a “networks” option will be added to the specification.

Sam will make issues in the repository linked above to track discussion items and to continue the conversation.

SESSION #13

Conceptual History of Society + Identity

Session Convener: Daniel Haro
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

ACDC (Authentic Chained Data Containers) for Muggles

Session Convener: Drummond Reed and 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:

Saidify - <https://github.com/WebOfTrust/signify-ts/blob/90324e26415d13d2f61c4aeb6f2553e61dad7ddb/src/keri/core/saider.ts#L167>

<https://github.com/WebOfTrust/keripy/blob/a6684b021c2e269a8c36ea2c1134f9d37c2b751d/src/keri/core/coring.py#L3521>

What does Presentation Exchange do? ...and which parts of it do we actually need?

Session Convener: Mike Jones

Session Notes Taker(s): Mike Jones

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

The deck used to stimulate conversation during the session is posted at <https://self-issued.info/presentations/What does PE do and what do we need-Part 3.pptx> and <https://self-issued.info/presentations/What does PE do and what do we need-Part 3.pdf>.

The detailed notes taken during the session are posted at <https://self-issued.info/presentations/What does PE do and what do we need-Part 3 Notes.txt>.

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

The session is summarised at <https://self-issued.info/?p=2427>.

21st Century Voters Here to Save the Day

Session Convener: Spencer Shirman, Britt Blaser

Session Notes Taker(s): Britt Blaser

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

<https://docs.google.com/presentation/d/1OeBC4XJ-b7BJKYjHEXbpP1TaICAsTcnA/edit#slide=id.p1>



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

Type Your Notes Here

Key-Based Auth Convox + Convergence

Session Convener: Day Waterbury, Duke Jones
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

Low Code a Path to Adoption

Session Convener: Jesus Torres
Session Notes Taker(s):

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

https://github.com/Entidad/farmworkerwallet/blob/main/Farmworker_WalletOS_OSS_Project.png — the diagram that shows how these fit together.

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

Did.web Improvements Challenges

Session Convener: Dmitri Zagidulin

Session Notes Taker(s): Dmitri, Juan C.

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

- overview of did:web extensions
 - did:webhash & web2.0 paper
 - webhash - each did doc is signed and content-addressed (hash subdir) and hashed-backlink
 - witnessing system separate/mix-and-matchable (probably something that uses cert-trans that's age-based)
 - webplus prototype
 - event log in DID doc (hashed-backlink to previous version)
 - trusted witnessing system makes for verifiability-parity with ledger-based systems
 - did:webs (did:web+KERI) - KERI event log must be parsed to get public key for verifying a KERI signature; open-ended external witnessing provisions by KERI system
 - did:plc (bsky) - one centralized witness/validator for now of all rotation events (which are signed by DID controller)
- core problemspace of did:web + all 4 extensions
 - trust model inherited from ICANN/DNS
 1. certificate transparency/Let's Encrypt --> goes a long way towards securing DNS/ICANN anyways (but otherwise immovable/systemic constraint)
 2. in did:web, web site operator == DID controller
 - all 4 extensions decouple these two actors a bit - separation of concerns, maps better to complex organization systems, etc
 - advantages to decoupling did controller from website operator
 - "custodial" and/or multitenant DID:web
 - verifiable availability - live servers versus caching, portability, end-of-life planning
 - even enables ad hoc witnesses, MIRRORS, and BACKUPS like internet archive
 - core problem: how to distinguish legitimate rotations from exfiltrations/account-takeovers?
 - blockchain-based VDRs actually have this problem too; some form of trusted witness is key to Account Abstraction and other layered solutions
 - all 4 extensions address this differently, all with some form of a **witnessing layer**
 - DEGREE OF & mechanism for backwards compatibility
 - static website or dynamic required?
 - static-static (gitpages, ipfs, control-panel-based web systems); nginx and apache are "dynamic enough" to be infeasible to many potential implementers
 - affects caching and end-of-life features
 - could any of these 4 extensions be extension specs to did:web, or are all breaking changes/new DID methods
 - pro's and con's of forking the codepath _on did method prefix_ versus monadic backwards compat
 - aligning the 4 did:web extensions

- static/dynamic
 - webhash is static-friendly, all 3 others currently need dynamic
- field name differences (translateable/negligible)
- witnessing systems are different, each has its own trust model and shelf-life
 - further analysis warranted!
 - are they mix-and-matchable? could a did:webhash be witnessed by did:plc's mega-indexer, or did:webplus' trusted mirror client?
 - DID Doc history (aka "key event log") - basically addressed equivalently/translateably between did:webplus|webhash|plc, but did:webs is majorly diff (inherited from KERI)
- future discussion
 - how to represent tombstones (did:webhash has an empty)
 - where to put metadata (DID Resolver metadata? in)
 - migration and end-of-life sections?
 - should these sections be recommended alongside "privacy considerations" and "security considerations" in the DID spec registry template? The conveners think so!
 - pathing issues
 - but many web operators can't create `/.^` folders due to security policies of shared server space/domainspace!
 - WHOIS folder inherits these^ problems; should also consider that at TOIP

APAC Digital Identity OpenSpace unConference - Late 2024 - come discuss how to contribute to making it a success!

Session Convener: Heidi N Saul

Session Notes Taker(s): Heidi

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

APAC Digital Identity Open Space unConference 2024 / towards end of the year in Bangkok
<https://www.apacdigitalid.org/> This site includes photos from the first event in March 2023

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

A few of us met and shared contact information and ideas

- Contact DIF Special Interest Groups in Japan and South Korea to help promote
- Ask for some Personal Statements for Attendees from the 2023 event in Bangkok that can be shared on the site and used in outreach to potential Sponsors
- Be in touch specifically with Australian Identity companies and individuals
Check Dates of holidays, national days, other Identity Events etc... for APAC countries in the Autumn of 2024 (ID Week Asia - Hong Kong FinTech - Singapore FinTech Festival - what else?)
- Explore having a keynote speaker and/orPanel - possibly a Government Focused Panel during a pre day afternoon
- Be in touch with GLEIF Asian based work (TY can tell us who)

If you are interested in being involve, have ideas, know of possible Sponsors or something else helpful, please email Heidi: heidi@heidinobantusaul.com

OR Add your name below and we'll include you in updates!

Naoki Yagita (JP)

Kazue Sako

Tze Yuan Lee

Catherine Nabbala

Identity Stories

Session Convener: Erica Connell
Session Notes Taker(s):

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

<https://www.pbs.org/moyers/journal/02202009/transcript2.html>

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

We had about 15 participants in the conversation.

We started with a simple example of narrative story structure:
Character -> want -> obstacle -> resolution

And a set of stories that Parker Palmer discusses in the PBS interview linked above, that shifted the way political volunteers approached spreading the message of Obama as a candidate:

The Story of Self
The Story of Us
The Story of Now

We discussed the stories we have/use now about decentralized identity and the work/tools/technologies that are being developed now.

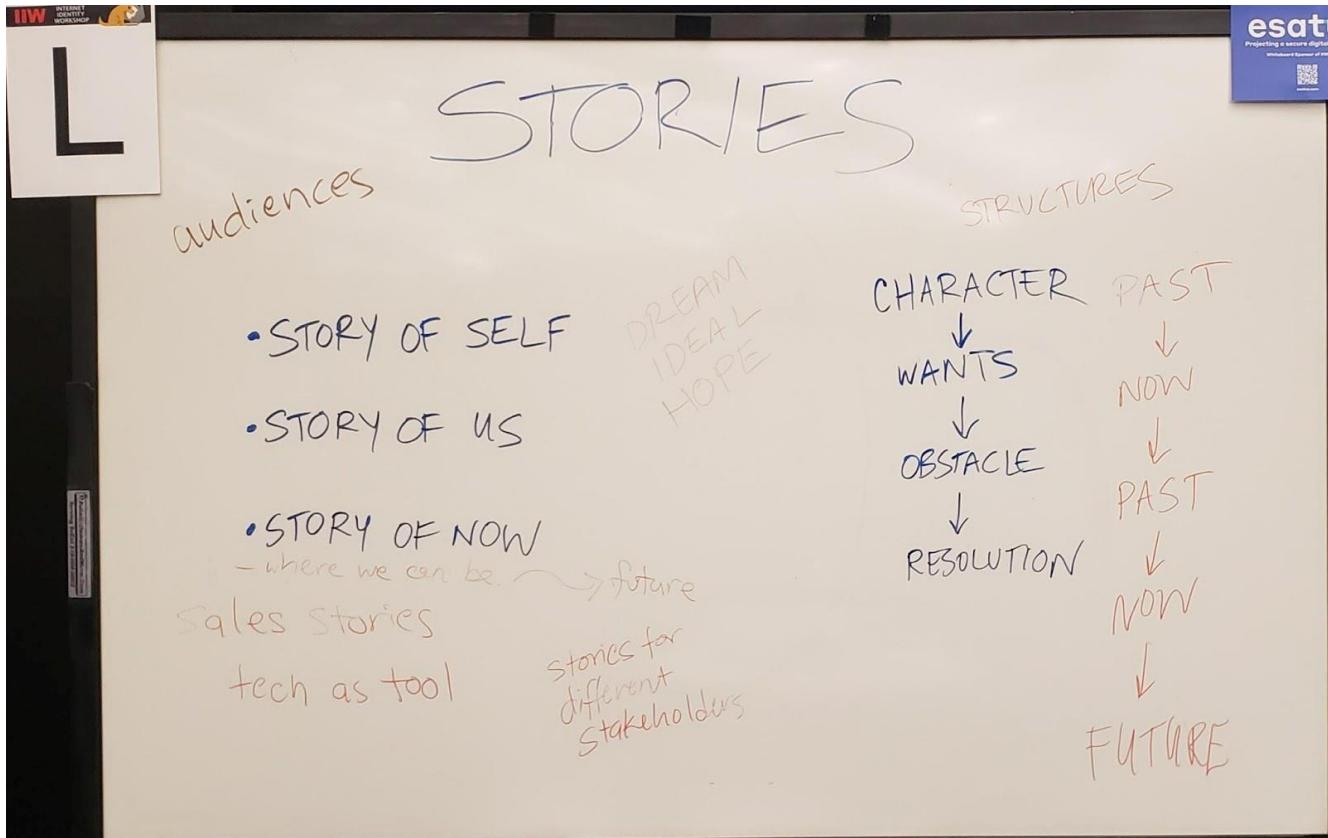
What are the stories we are telling now about decentralized identity?
How do we bring the future to the folks who haven't heard about it yet?

Discussion highlights:

- the challenges in talking about what people might not ever see (the 'under the hood' tech).
- the power of connecting with others telling the human stories that touch people's hearts.
- how fear is used
- other communication structures
 - speeches: past -> now -> past -> now -> future
- connecting people with the hope, possibility, ideals
- selling stories
- knowing your audience, and designing stories with that in mind
 - creating stories developed for different stakeholders
- tech as tools
- marketing considerations

Takeaways:

- there's plenty of work to do developing stories that include/point to/champion decentralized identity and decentralized emerging technologies



Organizational Ecosystem with BC Gov - Lessons learned on adoption and governance

Session Convener: Nancy Norris and Kyle Robinson, BC Gov

Session Notes Taker(s): N/A

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

Link to presentation: [EMDT - EMDT Overview Deck - IIW - October 2023 - Governance.pptx](#)

Link to Governance GH repo: <https://github.com/bcgov/bc-vcpedia/tree/main>

Link to user-friendly view of Governance docs: <https://bcgov.github.io/bc-vcpedia/>

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

Session #14

CLAIM-BOUND VCs - no keyinding? Matching by biometric / names

Session Convener: Paul and Torsten

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

Authentic Data is the Real Sh*t, NOT digital identity

Session Convener: Sophia Goeppinger, Timothy Ruff

Session Notes Taker(s): Sophia Goeppinger, Jin Wen

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

Some of the reference materials could be from here [Secure Privacy, Authenticity, and Confidentiality \(SPAC\)](#)

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

[Authentic data economy paper](#) - He gets credit for that word

Authentic web, not web5 or anything else (the term web5 didn't catch on; arms race of web xyz) - we just need a web where we have authentic things

Identity

- Everyone has a different definition of identity in his/her head
- You only need digital identity in the context of a relationship (to distinguish you from someone/something else) - *Timothy is in agreement with Phil here*

- = uniquely identifiable author/creator of something, NOT just log-in/access control (= identity, authenticity, authorization) → A working definition of identity that encapsulates all the different things: You have an author provably associated with something that they have authored; they digitally sign it with keys that they control and are associated with them; you have provenance to the author → You have authentic data
- E.g., Driver's license: The author of the authentic data is the state (create a driver's license and give it to me), but they may author many other licenses (fishing license, etc.) → The licenses are not identity they give me, but an entitlement, thus, a form of reputation AND it is authentic data because we know the source and it was given to my identity
- → Signatures allow for a mechanism of tracking: The digital signature = author (even if kind of identity, but not everything you sign is identity, e.g., me sending SPAM messages through the network → Can be traced back to me as it was signed by something that I control, but I am not really sending my identity through the network but the message) → This fits authentic data but also includes identity in the very beginning because there is some controller of the thing

Holochain = agent-centric model NOT a data-centric model

- We are confused that data can have independent truth, that it has first-order existence
- Data is also asserted by an agent; if you lose the provenance of your data, you lose data integrity
- Data needs to be sourced to be real, and centralized databases/systems don't give us that (we don't know where the data is coming from/who put it there)

Digital identity is a subset of authentic data - *Timothy*

The real problem is reputation (not authentic data) - Sam

- If I want to interact with someone, I need to be able to trust, and that is ultimately subjective (has subjective components)
- Reputation = a contextual predictor of future behavior that enables an interaction (consistent behavior over time) → Enables scalable predictability!
- As humans, we have built-in reputation systems: Recognition systems, biometric systems, remembering people violating reputation
- Should be expensive to require and cheap to get rid of (non-linear relationship)
- Need a human-class reputation over the internet to have human-class interaction on the internet → Internet is broken b/c we don't have a reputation system → We can't have a reputation system without authentic data → We can't have authentic data without security without provenance (all cascades from the fact that we can't interact unless we trust who we are interacting with and we can't trust unless we have all of the other things)

AI model collapse:

- There is about 6 months left before good-quality data for training these model is all vacuumed up

- There is a degradation of quality if AI is trained on other AI data (synthetic data)
- As little as 5% of the training data that is synthetic causes the degradation (5% of contamination is sufficient for complete collapse) → It is a collapse; not just low quality comes out, but gibberish
- BUT all these engineers know about it - so they will not let it come to that (fed it less fresh data)

→ Demand for authentic data goes up dramatically

→ Synthetic data becomes toxic to large AI engines

Authentic data

- ***Timothy***

1. Verifiable provenance: The source where it comes from; who digitally signed it (a chain or one) → Need provenance chain
2. Integrity: Hasn't been tampered with, revoked, or expired → Need integrity verification

→ If we know the provenance and integrity of some data comes from non-AI sources (human-generated data), the value of that goes up dramatically as synthetic data is toxic data to large language engines (need the highest octane: authentic)

→ Right now, there is no provenance chain, but in a future, there can be

→ We cannot tell whether someone used AI for an article, BUT if someone has a reputation for not using AI and they digitally sign something and we can verify it comes from that source, then we can start to say this is a clean source

- ***Sam***

- = It is attached to the source, and you can authenticate it to the source
- **Two definitions of authenticity in the dictionary:**
 1. It is true/is it genuine → We don't talk about this; this is about the value of the information INDEPENDENT of the source (this fits more authoritativeness)
 2. It can be provenance to a source

→ You can have high authoritativeness but weak authenticity b/c you can independently verify the truth of it regardless of its source, BUT on the internet, independently verifying is an expensive process

→ Authentic data is indispensable for anything to happen b/c the only way that we can know that it is true is by ascribing a reputation to the author (so that you know that you can reasonably trust him)

Facts that are independently verifiable don't benefit from authenticity!

- **4 As for data usefulness - Sam**

1. Author = identity → All data has an author; otherwise, it's not data that we can control in any way (yes, they are facts, but we don't care about that as we would have to independently verify those, and that is expensive, e.g., proofing all the physics laws and recreating the experiments to independently verify instead of trusting their authors) → Facts that are independently verifiable do NOT benefit from authenticity
2. Authentic = I can securely attribute the content of the book to this author; = secure attribution
→ Implies data integrity (= authenticity = a dependent variable b/c if it didn't come from them and they changed it, then it didn't come from them; you cannot securely attribute data if it has been tampered with) → Timothy makes the dependent variable explicit → Assumption: You have security (= a dependent variable) i.e., you cannot establish authenticity unless you can do it securely (need entropy with that) → Cryptography does that → There are layers (limited amount of authenticity)/to a degree: Authorship doesn't have to be a natural person, it can be an identifier, a pseudonym; reputation allows you to do something (you can link the source of the statement to a cryptographic identifier but you don't have to link that cryptonym to a natural person b/c of reputation of that cryptonym)
3. Authorized: (a) Is the author authorizing the use of the data for the purpose for which it is being used, or (b) am I authorized to use the data for the purpose I want to use? → Authorization allows us to control the flow of data
4. Authoritative = data that is true in some meaningful sense (cannot just use data that is found anywhere) → It is the veracity of the data (= you trust this author to be objective when they sourced the data) → There is a spectrum of subjective and objective: Soft vs hard science
 - Can be subjective
 - Better: It is objective within a certain context, i.e., community
 - Need to classify the data to its degree of authoritativeness (language models should learn more from more authoritative data than less authoritative data - i.e., weighing the information by its authoritativeness) value of the information

→ Sam extends what Timothy has been saying

→ Trust comes back to reputation

Current AI models lack the capability to do verifiable data provenance (if you have authentic data you can use transparent AI to process it)

→ Relates to Sam's journey:

- Started in machine learning
- Short stint in reputation → realized he needed to do something in digital identity before he could do that and get back to machine learning/AI

→ Has to fix the whole world before he can do the work he wants to do

Key takeaway

- Authentic data is everywhere. The problem with digital is that we don't know if it's real or not (don't narrow it to identity, b/c then you miss/don't solve the larger problem: we can't tell fake from real in digital things as digital is remote)
- Need to solve digital identity to have authentic data; you need authentic data to have reputation → Feedback loop between digital identity and authentic data (circular dependency): For authentic data, you need verifiable provenance, and THAT requires identity (you don't know who put it in unless you have an identity for them) → Identity is the root for figuring out identity
- BUT the space of authentic data is bigger than just the digital identity application. Identity is probably something that I want to present authentically → It will be one of the first applications as it is critical
- **Vision:** Everybody signs, and everybody verifies (base of zero trust)
- **Bottom line:** You cannot have the space of authentic data without identity to provide the provenance of the data (identity enables authentic data to be authentic, but then you have authentic data a whole bunch of use cases come from there)

Notes - Jin Wen

- Large language models (LLMs) like ChatGPT do not learn from authoritative sources like dictionaries, so they often have poor definitions compared to authoritative sources.
- Rhetoric used to be a core part of education but has declined over the past 100 years, leading to poor quality discussions and prevalence of logical fallacies.
- There is a lack of authentic provenance and data processing in current machine learning models, making it hard to trust their outputs.
- Authentic data requires 4 attributes: authority, authenticity, accuracy, and applicability (did i get it right?). Missing any makes the data not useful.
- Digital identity is needed to establish data provenance and authenticate the author.
- Explainable/transparent AI is needed to process authentic data in a trustworthy and provable way.

PLAN: Pico Labs Affiliate Network

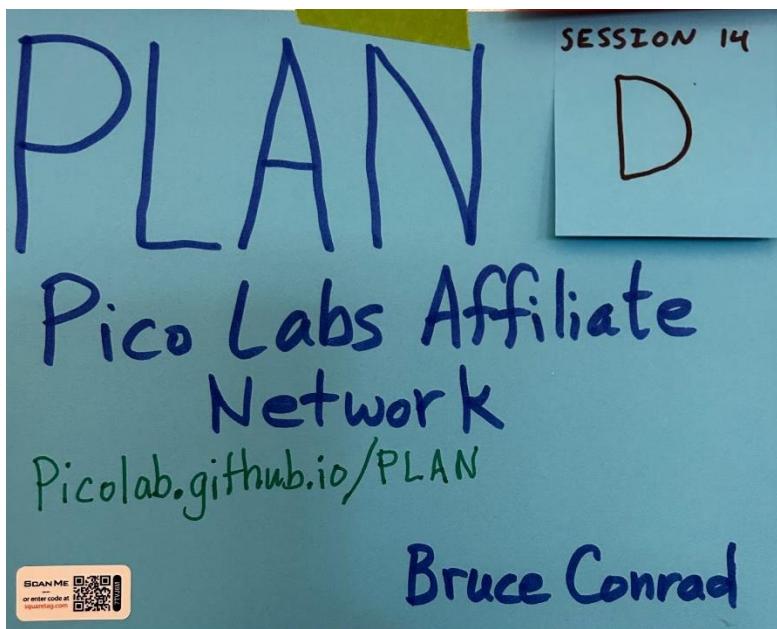
Session Convener: Bruce Conrad

Session Notes Taker(s): [convener]

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

View reasons to join and call to action on this web page: <https://Picolab.github.io/PLAN>

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

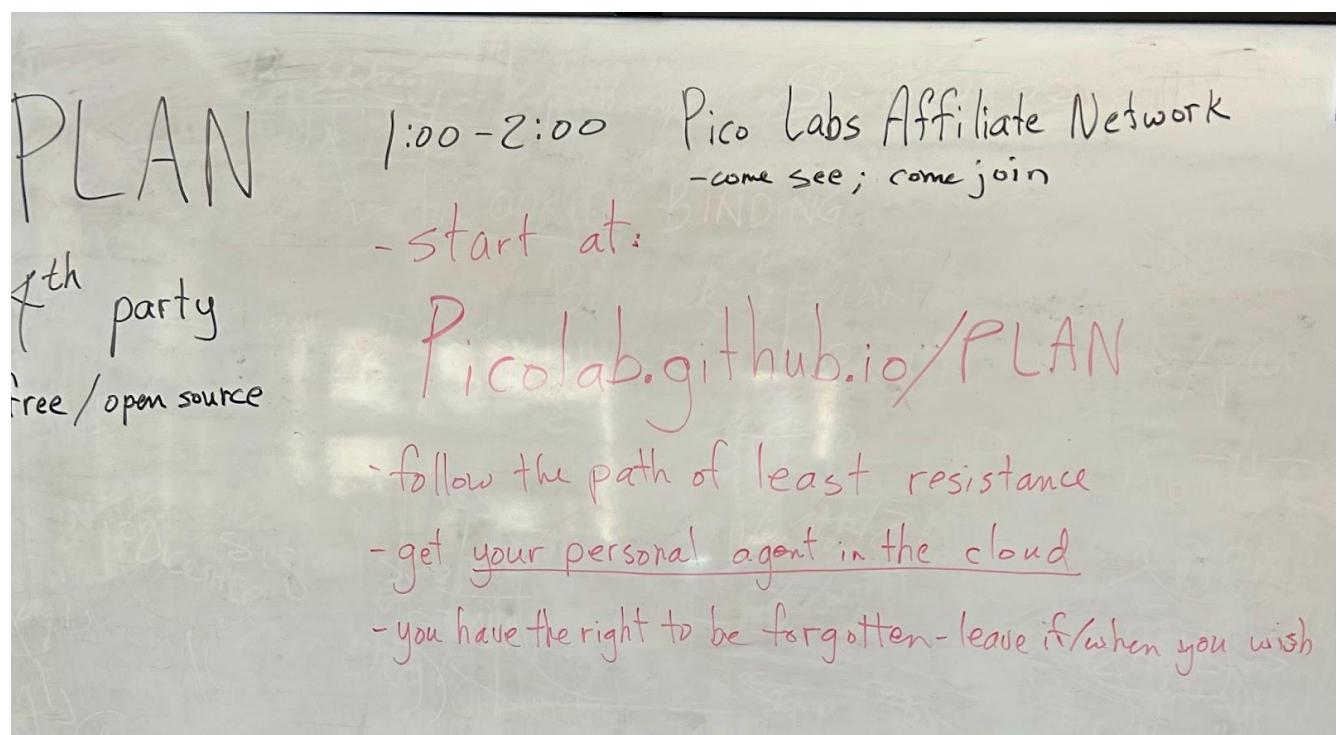


Caption: Above is a photo of the session poster, featuring a QR Code which, when scanned displays this message "Session 14 in space D from 12:30 to 2:00 pm, Thursday October 12, 2023. More information: <https://Picolab.github.io/PLAN> and session notes: [link to session notes]"

Several people visited and we talked about joining the Pico Labs Affiliates Network to get a pico running in the cloud as their own personal agent. In response to the question of "how much does this cost" the answer is that it is free and open source. A pico engine hosting thousands of picos in typical usage can run on an AWS EC2 instance for about \$10 a month.

Pico Labs would prefer that you [install and host your own pico engine](#), but to reduce the friction of getting started, we host and fund this PLAN where you can come and get a pico for your personal use.

White board near the end:



Caption: Above is a photo of the whiteboard, featuring the following steps:

1. start at Picolab.github.io/PLAN
2. follow the path of least resistance
3. get your personal agent in the cloud
4. you have the right to be forgotten – leave if/when you wish

The only information asked for is an email address that you control, and we do not use that email address for any purpose other than hosting your personal agent.

See [Doc Searls' blog post about "4th party"](#) which is the role your personal agent will play in your relationships with other things on the web and the Internet.

For more talk about picos and the possibilities they open up, visit [Phil Windley's blog](#), and find "picos" in the tag cloud. Lots of stuff there.

Intersubjectivity: An Open Discussion

Session Convener: Will Abramson, <https://drwip.com>

Session Notes Taker(s): Will Abramson

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

The Consequences of Language: <https://mitpress.mit.edu/9780262544863/consequences-of-language/>

Telling is Listening, Chapter 21 of The Wave in the Mind: <https://www.ursulaklequin.com/the-wave-in-the-mind>

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

This session introduced the concept of intersubjectivity:

Intersubjectivity can be thought of as the subjectivity that emerges between participants engaged in interaction. Through talking and listening. Through words and expressions. Through language.

It is the process through which minds tune in to one another. A continuous interchange between two consciousnesses. The gradual synchronisation of our cogs of thought and perception. They harmonise and begin to dance to the same rhythm. A melding of minds. An outcome that can never fully be achieved, for our minds and their subjective experiences are in a state of dynamic flux. Constantly being updated with new information, meanings and expectations.

It is rich. Complex. Fluid. Beautiful. Intrinsically human.

Then raised questions around its applicability to digital systems of interaction:

- Can we design for intersubjectivity within digital systems?
 - What might the architecture of these environments look like?
- Is it possible to achieve intersubjectivity with a digital environment, do we want that?
- Can machines, digital systems, agents be thought to have intersubjectivity?
- If repair is a fundamental component for achieving intersubjectivity, what mechanisms are we building for repair within our digital interactions?
- Language is infinitely generative. How might we bring some of the properties that language enables into these digital mediums?
- What if we thought of the tools we are creating for digital identity as constructing a new language through which humans can interact across digital mediums?

Notes on Intersubjectivity – image below

Infrastructure of Intersubjectivity p.82

Intersection of 2 independent enchronic frames
Turn taking & Sequence generation

Moves tied to each other by relevance & accountability, Semiciotic process

Sign → object → interpretant
object constantly defined → Hypothesize P41

IS supercharges possibilities for shared understanding p31

Language + IS
G constituting

Norm supported behaviour patterns across class boundaries, race, gender & age
↳ Subliminal p21
↳ Material
↳ Inference-vulnerable

Language is activity with infinite generative possibility ↑

Action usually has mediating artifact
Structuring, constraining & incentivising a set of actions. Limit agency enable systems of activity.

Agency defined in terms of actors flexibility & accountability

Agency 'component loci': Control, composition & subprehension

Interaction structured through P41 Agency: Capacity to signal & interpret Status: Rights & duties to signal & interpret in conformant ways whose signs direct attention to individ & uncertainty perceived objects that are interpreted & reacted to through action & expression

Subprehension: not surprised by what happens next. Similar to anticipate, but not conscious def by conventions of activity. calibrated through past experience. learnt conventions roles rights duties

Social — Rights: Things you can do / act without expectation of surprise / sanction

Accountability — Duties: Things you must do, if don't can expect sanction / surprise

What are digital infra of intersubjectivity
How might we design them?

Event of communicating Event kinds
↳ Grammar links Es to En domains p152
↳ Enable communication about past/future events, referential
Diff time-space-personal coordinates p160
Provide inf < experience ↳ Diff cultures & interactive medium, people to constrain & enable diff participation, talkers
Participation: peoples access to one another as a precondition for interaction, & thus intersubjectivity

Status - position within social structure.
labelled, contested, claimed
Can infer rights & duties

Mutual: A continuous interchange between two consciousnesses. U.L Guinn wave in mind

Tyranny of Accountability ↳ No adequate model in universe

Consequences of Language

Intersubjectivity = activity accountability (social) ← regulated by norms

P.5

break down in trust
↳ Infer purposes for inconsistencies with expectations for actions.
↳ Hold accountable through language

p25

Interaction structured in an unfolding sequence of semiotic processes through P41 Agency: Capacity to signal & interpret Status: Rights & duties to signal & interpret in conformant ways whose signs direct attention to individ & uncertainty perceived objects that are interpreted & reacted to through action & expression

Subprehension: not surprised by what happens next. Similar to anticipate, but not conscious def by conventions of activity. calibrated through past experience. learnt conventions roles rights duties

Social — Rights: Things you can do / act without expectation of surprise / sanction

Accountability — Duties: Things you must do, if don't can expect sanction / surprise

Authorization Exchange (AuthZEN) working group session

Session Convener: Allan Foster and Gerry Gebel

Session Notes Taker(s): Gerry Gebel

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

Here is a summary of the discussion points from the IIW in-person session on Oct 12:

Since we had some new folks in the room, Atul and Omri reviewed the presentation that was shown at the OIDF workshop on Monday of this week. Allan also recounted the two Identiverse meetings that led to the formation of AuthZEN.

We also talked about the initial work that has been scoped out so far, namely the PEP to PDP flow and transport of policies from admin service to decision engine. Other aspects such as management of data used by decision engines was also mentioned. In addition, there was agreement that we need to document use cases, deployment patterns, best practices, and guidance.

How will the output of AuthZEN relate to OAuth 2.0? There was quite a bit of discussion on this topic since OAuth is used in so many access control scenarios, whether this group approves of that approach or not. Ultimately, the use case and recommended patterns that AuthZEN produces must clearly articulate situations where and how fine grained or externalized authZ systems work with OAuth based models.

Who is the audience, stakeholder, buyer that we should be thinking about? Are they developers, product owners, CISO, auditors, other? Eve suggested that we think like a startup and what is the product market fit for any new standard.

Community outreach and evangelism will be important. Enterprises like Netflix, Airbnb and Workday were mentioned as possible collaborators that can help get the word out into the industry. Typical drivers are to make money, save money or reduce risk - we need to map to these motivations.

Logistics and next steps:

- Weekly zoom meetings will start on Oct 17
- We will attempt to record meetings
- Once OIDF formally approves AuthZEN, there will be a new email list and all participants must sign an agreement regarding IP
- There is an OIDF Slack channel, but is not ready for us to use yet
- More details to follow as we learn them.

Demoscene Dark Matter: Identity of a Digital Arts Subculture

Session Convener: Andre Kudra

Session Notes Taker(s): Andre Kudra

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

Presentation used:

https://kudra.de/demoscene/231012_IIWXXXVII_Fall_2023_Demoscene_Kudra.pdf

Demoscene Dark Matter paper published at Generative Art 2021:

https://kudra.de/demoscene/Generative_Art_2021_Demoscene_Kudra_Excerpt.pdf

Meteoriks – the Demoscene Oscars: <https://meteoriks.org>

Demoscene archives: <https://demozoo.org>

Demoparty list: <https://www.demoparty.net>

Next Demoscene outreach at cyberevolution conference November 2023 Frankfurt:

<https://www.kuppingercle.com/events/cyberevolution2023/demoscene>

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

What's the Demoscene?

- It's about demonstrating talent and skills of coders and capabilities of computing machinery
- **Demosceners** produce **Demos**, digital audio-visual works rendered real-time by computer programs
- Internationally active non-profit digital subculture
- Rooted in the home computer revolution in the 1980s but vibrant to this day
- People attach strong identity with the Demoscene, which is one of the reasons it is seen as culture

Sceners' Motivations

- Some sort of pain or alienation feeling drives creative expression
- Motivates to create things, with any type of aesthetical means, or usually with technical devices
- May be a solo task at first, but when uniting with like minded others, positive reinforcement occurs
- Encountering the Scene can be a revelation
- Strive for frequently meeting at Demoparties anywhere
- Community events for showcasing mutual creativity, in a sport-like contest

It's People, not just Tech

It is the other people that make them stick to it, not the celebration of technology or their Demos, which are inevitably their important cultural works.

Demos we watched and discussed

VX2 by Spectrals (PC Demo)

<https://demozoo.org/productions/277304>

<https://www.youtube.com/watch?v=hrlkv6eDKx0>

Arcade by Spectrals (PC Demo)

<https://demozoo.org/productions/292559>

<https://www.youtube.com/watch?v=ZWIK9J-58aw>

Memories by HellMood / Desire (256b PC Intro)

<https://demozoo.org/productions/277060>

<https://www.youtube.com/watch?v=Zqe6xhckJFM>

Way Too Rude by Logicoma and Loonies (64kb Amiga Demo)

<https://demozoo.org/productions/277035>

<https://www.youtube.com/watch?v=s66OgcwqalA>

Freespin by Reflex (Commodore 64 / 1541 Wild Demo)

<https://demozoo.org/productions/296068>

<https://www.youtube.com/watch?v=zprSxCMIECA>

FirST Love by Overlanders / The Union (Atari ST Demo)

<https://demozoo.org/productions/298763>

<https://www.youtube.com/watch?v=3QginSr9V7A>

Area 5150 by CRTC & Hornet (IBM PC & CGA Demo)

<https://demozoo.org/productions/311767>

<https://www.youtube.com/watch?v=fWDxdoRTZPc>

The Martini Effect by FLEX (Amiga AGA Demo)

<https://demozoo.org/productions/292543>

<https://www.youtube.com/watch?v=QtHH408shWo>

Eon by The Black Lotus (Amiga OCS Demo)

<https://demozoo.org/productions/202831>

https://www.youtube.com/watch?v=i1O4_58HVIg

1E78 by Desire (Atari 7800 Demo)

<https://demozoo.org/productions/202481>

<https://www.youtube.com/watch?v=xxBfRT7cQ0M>

Human Rights impact of Digital Identity Protocols

Session Convener: Adrian Gropper

Session Notes Taker(s):

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

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

Unfortunately, many of the notes on the board were accidentally erased.

The main point was that forcing the subject of a digital identity to use a certified technology was a restriction of their right to engage an agent or other proxy through delegation.

This discussion is sure to continue. See for example: <https://www.eff.org/vi/document/10-16-2023-aclu-eff-epic-comments-re-tsa-nprm-mdls>

I

1T Human Rights impact of Digital Identity Protocols

esatus
Protecting a secure digital tomorrow

Presentation
Scope

VC → Substitution for a biometric
in the VC.
↳ contains

- direct → Issue → Verifying of custody → breaks the human rights of freedom of assoc.
- proxied → Agent → Verifier
- held in chain of custody + be optional.
 $I \rightarrow H \rightarrow Vc$.

Consumer Apps in Decentralized Identity

Session Convener: Matt Murray

Session Notes Taker(s): Matt Murray

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

This session was an open conversation around applying decentralized identity and applying it to applications under “Consumer applications”. Looking to facilitate the conversation of existing interactions with Decentralized Identity in consumer apps, current shortcomings and what we can do better.

While there are existing applications in the enterprise and government sector we see less in the consumer realm. First we discussed those consumer applications which workshop participants currently use that include decentralized identity, of which there were none that members discussed.

Next we discussed current issues with the marketing and getting funding for these projects

- Understanding the audience
 - Too technical of content
- Explaining everything all at once
 - All the benefits of decentralization + decentralized identity
- Trouble Explaining business value
- Complexity → Increased cost and difficulty explaining
- Recovery problems with wallets and key phrases

We then discussed key steps of communicating this clearly:

1. Find a subset of benefits specific to your app and focus on a couple
 - a. Portability
 - b. Authenticity
 - c. Composability
 - d. Privacy
2. Apply Decentralized Identity clearly to a specific use case
 - a. Don't talk about all possible applications, make it use case specific
3. Anchor to familiar experiences
 - a. Related to current online experiences

We then ended the session with an open question of: what applications would we like to see when everyone has decentralized identifiers?

- Incentivized Acquisition
- Reputation Portability
 - Context Specific Identity

Identity through IOT deploying aca-py on balena cloud

Session Convener: Patrick St-Louis
Session Notes Taker(s):

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

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

No Notes Submitted

did:peer:4 - A document in the DID + Demo

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

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

<https://github.com/dbluhm/did-peer-4>
<https://github.com/decentralized-identity/peer-did-method-spec/pull/61>
<https://github.com/dbluhm/did-peer-4-ts>
<https://dbluhm.github.io/did-peer-4-ts/>

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

I gave some background information on the did:peer:4 method specification and the history of the did:peer method itself (versions 0, 1, 2, and 3). With the context of what had been implemented in the past, I walked through the specification and how did:peer:4 addresses several challenges experienced with the previous versions. After this walkthrough, I demonstrated the creation and resolution steps using the web app I wrote. An example can be found here:

<https://dbluhm.github.io/did-peer-4-ts/?did=did:peer:4ZQmd8CpePci817KDsbSAKWcXAE2mvjCQSasRewvbSF54Bd:z2M1k7h4psgp4CmJcnQn2Ljp7Pz7ktsd7oBhMU3dWY5s4fhFNj17qcRTQ427C7QHNT6cQ7T3Xfr35Q2GhaNFZmWHVf04vL7F8nm36PA9Y96DvdrUIRUiCuKnBFrn1o7mxFZAx14l4t8vUWpuDPwQuddVo1T8myRivH7wdxuoYbsva5x6idEpCQydJdFjiHGCpNc2UtizPQ8awSXkctGCnBmgkhri5gto3D4i3EREYq4Z8r2cWGBr2UzbSmnxW2BuYddFo9Yfm6mKjtJyLpF74ytqrF5xtF4MnGfg1hMBmh1xVx1JwjZ2BeMJs7mNS8DTZhKC7KH38EggDtUZzfihpjmmUfkXg2KFFEA3EGbbVm1DPqQXayPYKA5YPS9AyKkcQ3fzWafLPP93UfnhtUPL8JW5pMcSV3P8v6j3vPXqnnGknNyBprD6YGUvtgLiaQDBDUF3LSxFQJCVYYtghMTv8WuSw9h1a1SRFrDQLGHE4UrkgRvwaGr64aM87T1eVgkP5Dt4L1AbobeK2ceLArPscrdYGTpi3BpTkLwZCdjdifSfTy9okL1YNRARqUf2wm8DvkVGUU7u5nQA3ZMaXWJAewk6k1YUxKd7LvoFGUK4YEDtoxN5vb6r1Q2godrGqaPkifL3RoYPPoDYymf9XhcgG8Kx3DzaA6cyTs24t45KxYafeCw4wqUpCH9HbpD78TbEUR9PPAsJgXBvBj2VVsxnr7FKbK4KykGcg1W8M1JPz21Z4Y72LWgGQCmixovrkHktcTX1uNHjAvkBqVD5C7XmVfHgXCHj7djCh3vzLNuVLtEE8J1hhqsB1oCBGiuh3xXr7f29wUJcQ1HYHqxLJkdYKtoCiPmgKM7etVftKkmTFETZmpM19aRyi3ba076LdpQtbw636r7a3qt8v4WfxsXjetSL8c7t24SqQBcAY89FBsbEnFNrQCMK3JEseKHVaU388ctvRD45uQfe5GndFxthj4iSDomk4uRFd1uRbywoP1tRuabHTDX42UxPiz>

The Input DID and Input Document can be edited live. Try it out!

SESSION #15

ToIP (and everyone's) GLOSSARY - How can we all speak the same language (learn acronyms)

Session Convener: Drummond Reed

Session Notes Taker(s): Jin Wen

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

ToIP Glossary Workspace:

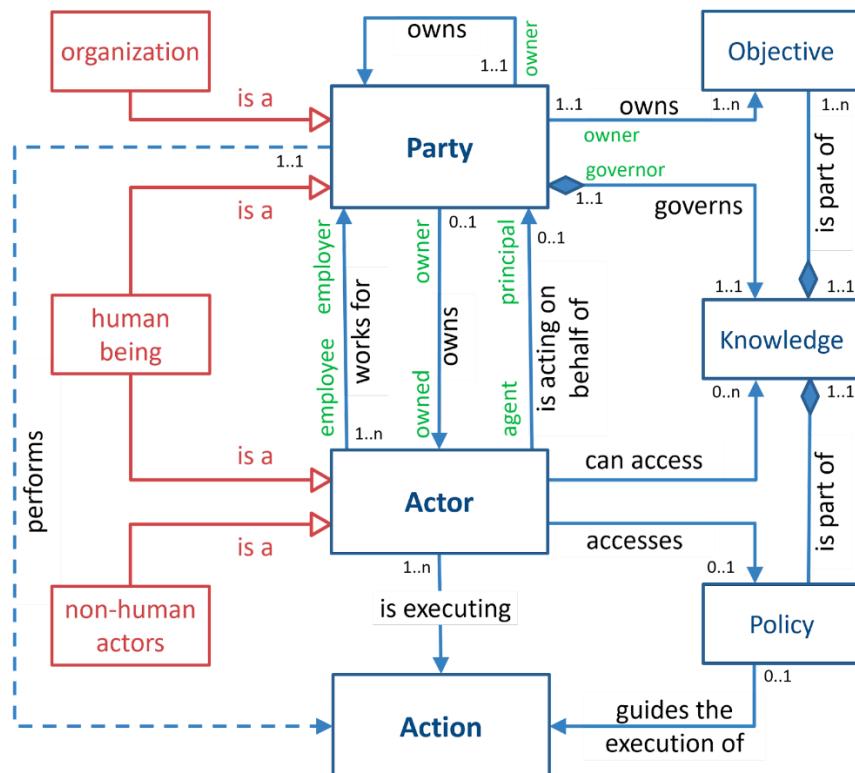
<https://docs.google.com/document/d/1fZByfuSOwszDRkE7ARQLeEISYmVznoOyJK4sxRvJpyM/edit#heading=h.xq6siu0ex25>

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

Drummond started by stating IIW originated from identity common
(<https://www.idcommons.org/working-groups/iiw/>)

currently ToIP glossary is shared in Google Workspace, with upcoming implementation using a new tool call tev2-test (<https://github.com/aviarytech/tev2-test>)

EU funded glossary is called eSSIF-Lab Glossary, for example, the definition of Party:



<https://essif-lab.github.io/framework/docs/terms/pattern-party-actor-action>

Drummond then took an example of “identity” from ToIP workspace

<https://docs.google.com/document/d/1fZByfuSOwszDRkE7ARQLeEISYmVznoOyJK4sxRvJpyM/edit#heading=h.xq6siiu0ex25>

Key Understandings

- The Trust over IP Foundation started a Concepts and Terminology Working Group to develop a common glossary for the decentralized digital trust space.
- They initially used a shared Google Doc as a "workspace" for people to contribute terms and definitions. This allowed easy collaboration and interlinking of terms.
- They are now converting the "workspace" to an official glossary with one definition per term. Terms are scoped for decentralized digital trust.
- Brian demonstrated tools to convert glossary content from markdown to machine readable and back to human readable formats.
- There is interest in eventually hosting the glossary on a wiki using MediaWiki for full version control and tracking of changes.

Outstanding Questions

- What is the best long-term platform for hosting the glossary? MediaWiki or other tools like Tinderbox?
- How to best support both open contribution and curation/governance of the glossary?
- How to represent the evolution of terms over time?

Observations

- A shared glossary is critical for aligning terminology in the decentralized identity space.
- Easy contribution and interlinking has helped quickly build content.
- Machine readable formats enable additional tooling and use cases.
- Full version control and tracking of changes is desirable.

Potential Action Items

- Evaluate MediaWiki and alternatives like Tinderbox for hosting the glossary
- Develop processes for open contribution along with curation and governance
- Add functionality to show the history and evolution of terms over time
- Engage more groups like DIF, CCG, and OpenID Foundation to contribute and use the glossary
- Schedule a Concepts and Terminology WG call with Eric to discuss Tinderbox

TOKEN BUCKETS

Session Convener: Justin Richer

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

No Notes Submitted

POST-CAPITALIST Funding & Governance

Session Convener: Day Waterbury

Session Notes Taker(s): Trent Larson

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

meaning: how to fund the migration to a post-capitalist world

Transitional Compromises

- Capped Returns - return in \$ but only to a point
- Dividend Flips - pay back a greater-than-your-share dividend for a while, then it becomes a pro-rata dividend

"Exit To Community"

Most people here want to provide a digital public good, because we don't have good funding for digital public goods.

Yesterday UCSC seminar robotocist got funding from B&M Gates Foundation for kids mobility, then kids trusted the robots more than a physical therapist and had more empathy.

Sleep deprivation will deplete empathy in humans.

Maybe separate ownership from governance.

IKEA pays profits to the IDEA Foundation with a defined purpose..

Firebrand Bakery has a mission in a Perpetual Purpose Trust. Has worker ownership and VC investor ownership. Owner + Trust has 60% of the ownership.

We've surpassed 6 of 9 planetary boundaries.

In a study of grant organisations, smallest stayed flat, middle-tier shrunk 7%, and largest grew 21%. Middle-class being squeezed out?

Brewster Kale was able to provide housing to increase quality of life and reduce costs (rather than paying rents and mortgages).

We exist in a tenant economy for housing, energy, water.

The book "Change the World Without Taking Power" is recommended.

<https://libcom.org/article/change-world-without-taking-power-john-holloway>

Feels like this is a local system to provide basic sustenance in a voluntary, small-scale way.

Demo Decentralized Identity Use Case Assessment Framework US Healthcare

Session Convener: Sophia Goeppinger

Session Notes Taker(s): Sophia Goeppinger

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

For further details on the assessment framework, please reach out to Sophia Goeppinger at sophia.goeppinger@student.unisg.ch

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

Part I: Demo

This session was a continuation of “US Healthcare on Trial: Decentralized Identity Use Case Assessment Framework” held the day before. Due to the keen interest shown by participants from the earlier session to delve deeper into the assessment framework, this session provided a comprehensive exploration of its functionality and the various questions it entails.

Part II: Comments made during the demo were as follows

Do you make the stakeholders filling out the framework define who the end-user is? - Jared Jeffrey
Yes, the stakeholders are asked to define that at the very beginning of the use case assessment framework when they flesh out their use case. But I should also make it more explicit in the companion guide. - Sophia Goeppinger

Who is supposed to answer these questions? What is their role?

Both the tech and healthcare knowledge division do the framework together.

Are the questions weighted differently because one statement might kill the entire endeavor? - Jared Jeffrey

Yes! The relative importance column is for that - Sophia Goeppinger

Do the US healthcare stakeholders understand what all the statements refer to? - Wendy Seltzer
The framework is currently tested with all kinds of US healthcare stakeholders to precisely find that out. - Sophia Goeppinger

Which type of US healthcare stakeholders are currently testing the framework? - Jared Jeffrey
The framework is currently being tested with the following stakeholders:

- Provider
- Payer
- Patient organization
- Health IT vendor

- Manufacturer
- Emerging technology start-up

A policymaker is still missing. They were involved in developing the framework but have not answered any follow-up outreach.

Is there a notes section for each statement? - Dmitri Zagidulin

Yes. It is called “pivotal insights.” - Sophia Goeppinger

Many healthcare stakeholders will have trouble answering some of these questions, is there a way to add an additional column stating something like “and here are some resources to help you answer that.” I know it is a little bit political to see which resources and vendor, etc. to recommend but it could be amazing. - Dmitri Zagidulin

That is a wonderful idea. I will add that. - Sophia Goeppinger

This is a great framework. It reminds me of some of the work we are doing at W3C with standards work. A different way of looking at some of these questions is “Is your problem suitable for a standards organization?” And using it in that context, particularly in terms of stakeholder alignment and alignment of incentives. If you are missing some of those you should be going off and gathering the inputs before getting to work there - Wendy Seltzer

I’m completely blown away by the framework and I’m working with a group trying to put together a similar document in the education space: a questionnaire how to determine if your educational institution is ready to implement DIDs and VCs. This is so much more thorough. - Dmitri Zagidulin
And so many questions can be translated to other sectors. - Sophia Goeppinger

You should add another question asking “What is the core tech stack of your department.” And ask that all minimum viable ecosystem stakeholders because decentralized identity can fail just because their tech stacks are not aligned. It doesn’t mean that they have to be on the same vendor. Class research just published information on interoperability scores for various vendors from A to F on how well they do on data exchange. This might be valuable to this. - Jared Jeffrey
Yes, I should add that. - Sophia Goeppinger

Biometric Holder Binding - The Good Bad Ugly

Session Convener: Daniel Bachenheimer

Session Notes Taker(s): Daniel Bachenheimer

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

https://drive.google.com/file/d/1HFke5m8VVqitEQ5QTwiz9ZWw1UpB5oxw/view?usp=drive_link

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

Dan started with a depiction of the Identity Lifecycle in general and highlighted the elements in the lifecycle where biometrics play a role.

Assurance levels associated with the different phases of the identity lifecycle was introduced.

Then we discussed Identity Proofing, which occurs during the initial registration phase, which is primarily about establishing uniqueness within the target population - but is often [mis-]used to mean verification. Here the example of Aadhaar was discussed to show biometrics-based uniqueness establishment on the order of 1.3 billion unique identities.

The NIST Digital Identity Guidelines were then highlighted and Dan pointed out some of the feedback he provided to NIST where he felt improvements to the draft would be helpful

The discussion then moved to the premier globally interoperable verifiable credential in use today - the ePassport and how, when, and why Biometric Holder Binding came about

We then discussed the Strong Authentication means in the EU context - where biometric recognition may be one of the two factors required

Stephen Curran asked about Open Source biometric matchers; Dan mentioned that Interoperable ISO standards-based, biometric templates do exist but most large scale production systems use proprietary matchers and templates to achieve high performance (i.e., reduced error rates). Others responded that there are open source matchers available but agreed that, due to higher error rates, their adoption has been limited.

The remaining discussion was focused on some of the challenges of Biometric Holder Binding - especially when the holder is operating remotely.

Real - IT Party Frontal Guerrilla Rebellion

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

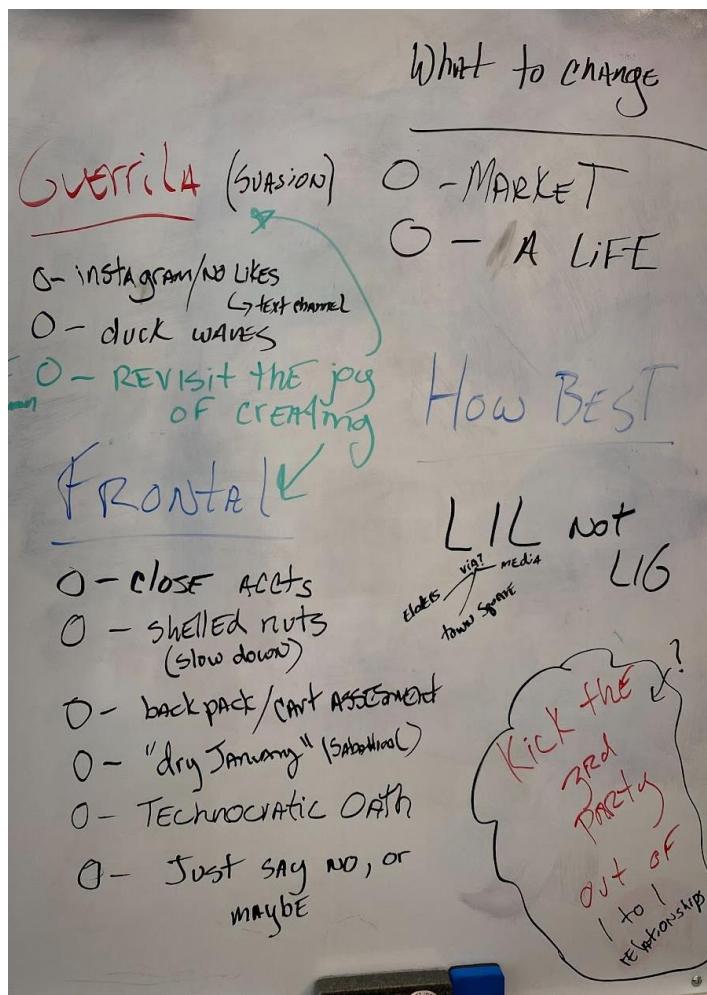
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

In view of the current tensions in the socio-techno-political fabric of people's lives, the paths possible for relief, at a greater or lesser level, are not typically identified or itemized in ways people know.

The challenge of changing a market is resolved differently than changing a life.

LIG / LIL

Even though life is global, the importance of knowing that living is local plays a lot in the methodology of approaching communities and establishing expectations of healthful treatment by systems and governance. More detail in associated image.



KIRA - Key Infrastructure with Remote Attestation (Confidential Computing)

Session Convener: Manu Fontaine

Session Notes Taker(s): Manu Fontaine (redirecting to Charles Lanahan's notes)

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

Confidential Computing, Key infrastructure, remote attestation, verifiable infrastructure

Link to slides:

https://drive.google.com/file/d/1WkX_tD6B8QIOGeP8sYOBZu0EOzs_1nvW/view?usp=sharing

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

This session is a variation on Day 1 session “Confidential Computing Changes Everything - Enabling a Universal Name System (UNS) and Universal Certificate Authority”, see notes here:

https://docs.google.com/document/d/1DoWnI2UJ5OkRjTzwjF-QdVyECL23MCLJ58hM_vhYYI/edit?usp=sharing

We coined the KIRA acronym as a tongue-in-cheek tribute to KERI. The fundamental message for this session was that there cannot be any decentralized anything without a key infrastructure strategy. Confidential Computing enables the creation of verifiable infrastructure, which can be used to create a verifiable decentralized key management system. Making the provenance, integrity and confidentiality of keys and cryptographic primitives verifiable is strictly necessary for any signed credential to actually be verifiable.

Demo Hour / Wednesday October 11

Thanks to our Demo Hour Sponsor!



The IIW Speed Demo format involves each person Demoing giving a **5-minute demonstration** of their service, product, physical device, **10 times** to 10 different small groups, rotating through to view them over the course of the hour. **Demo Hour takes place on Wednesday after lunch from 1:30 - 2:30.**

There will be 20 Demo Tables in the Grand Hall each with a # Sign on it that corresponds to the Demo taking place at that table. People rotate through the tables/Demo's in a self organized way ~ that's a little loud, seemingly chaotic and free flowing, but works!

See the list of Demos via the Demo List below and decide ahead of time the Demo's you'd like to see. You'll be able to see 10 of the 20 Demo's over the hour.

| TABLE | Demo Description | More Info |
|-------|--|--------------------------------|
| #1 | Province of British Columbia - the BC Wallet: Clecio Varjao, Product Manager British Columbia's Digital Identity and Trust Program URL: https://digital.gov.bc.ca/digital-trust/ The BC Wallet app has an increasing number of digital credentials available. They can be used in combination with a new mobile verifier feature in BC Wallet. This allows anyone with a smartphone to verify another person's digital credentials. Come and see it all in action. | More Info Here |
| #2 | 2060.io - Building DIDComm chatbots: Ariel Gentile and Fabrice Rochette URL: https://2060.io Using 2060 to create rich decentralized verifiable chat services, combining text, pictures, video and voice notes with the power of Verifiable Credentials. | More Info Here |
| #3 | Agama Lab Demo: Michael Schwartz, Founder/CEO Gluu URL: https://agama-lab.gluu.org Agama Lab is a low code developer tool which enables you to build custom web OpenID authentication flows. Register for free, manage and publish your projects from your own Github account; deploy Agama projects on Janssen Auth Server or the Janssen distribution of Keycloak--Agama is the easiest way to orchestrate the identity journeys that solve your specific business requirements. | More Info Here |
| #4 | Cedar: Jeff Lombardo URL: https://www.cedarpolicy.com/en Cedar is an open source language for defining permissions as policies, which describe who should have access to what. It is also a specification for evaluating those policies. Use Cedar policies to control what each user of your application is permitted to do and what resources they may access. | More Info Here |

| | | |
|-----|--|--------------------------------|
| #5 | Farmworker Wallet OS low-code wallet engine: Jorge Flores URL: https://tac.openwallet.foundation/projects/fwos/ Farmworker Wallet OS (FWOS) is an open-source digital wallet engine implemented with the Mendix low-code application platform. The FWOS wallet engine can be embedded into any Mendix application to support privacy-preserving digital trust interactions between peers. | More Info Here |
| #6 | Infisign Inc. / Infisign Identity Lifecycle Management: Aditya Santhanam (CPO, Infisign Inc.) URL: https://www.youtube.com/watch?v=gcAEEgfA7js Infisign is a cutting-edge identity and access management (IAM) platform that revolutionizes digital security by leveraging decentralized identity, passwordless authentication, federation, and privileged access management (PAM) capabilities. With its unique approach, Infisign addresses the challenges of traditional IAM systems and offers a comprehensive solution for modern identity management. For the demo, Infisign will showcase its Identity Lifecycle Management capabilities, which will help enterprises manage their employee identity and application subscriptions during onboarding and exiting. | More Info Here |
| #7 | Aserto / Topaz : Omri Gazitt URL: https://www.topaz.sh , https://github.com/aserto-dev/topaz 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. Topaz is ideal for building fine-grained, policy-based, real-time access control for SaaS or internal applications. | More Info Here |
| #8 | IDLab's Digital Trust Test Bench: Patrick St-Louis - DevOps Specialist URL: https://www.idlab.org/en/digital-trust-test-bench/ My demo will test an Aries Mobile wallet against the Aries-Agent-Test-Harness integration. This will demonstrate issuance and verification interoperability between a mobile wallet and 2 aries reference frameworks. | More Info Here |
| #9 | IDunion: Paul Bastian and Christian Bormann URL: https://idunion.org/?lang=en Demonstration of OpenID4VC + sd-jwt + status list featuring issuance and presentation following the OpenID4VC High Assurance Interoperability Profile | More Info Here |
| #10 | GLEIF: Kevin Griffin URL: https://www.gleif.org/en/vlei/introducing-the-verifiable-lei-vlei GLEIF will demo the successful proof of concept conducted with the European Banking Authority (EBA) using a VLEI credential to gain access to a web portal and authorizing XBRL-CSV report packages with embedded signatures. | More Info Here |
| #11 | CS DMV Wallet APP / SpruceID in collaboration with other parties: Oliver Terbu (Spruce), Elissa Maerklein (Spruce) + Google + Ping Identity + NIST URL: https://spruceid.com/credible and https://www.dmv.ca.gov/portal/ca-dmv-wallet/ (it is actually California DMV's product) Description: Demonstration of CA DMV wallet app that interacts with different verifier applications using different protocols (Mobile Document Request API, ISO/IEC 18013-7 OID4VP) and different credential formats (ISO/IEC 18013 mdoc, W3C JWT-VCs) to share mDL. | More Info Here |
| #12 | OpenID Foundation conformance tests for OpenID for verifiable credentials: Joseph Heenan URL: https://openid.net/how-to-certify-your-implementation/ OIDF has tests for checking that wallets (and, later, verifiers and issuers) correctly & securely implement OpenID for Verifiable Credential Issuance / OpenID for Verifiable Presentation specifications - we demo them, explain their limitations and how you can test your wallet. | More Info Here |
| #13 | GoDiddy.com - Universal DID Services: Markus Sabadello - Danube Tech URL: https://godiddy.com/ GoDiddy.com is a hosted platform that makes it easy for SSI developers and solution providers to work with DIDs. It is based on open-source projects Universal Resolver and Universal Registrar. | More Info Here |

| | | |
|-----|---|--------------------------------|
| #14 | Trinsic Connect - Reusable, verified ID: Michael Boyd URL: https://pearbnb.app/ & https://pocketrides.app/ Pearbnb and Pocketrides are two applications using Trinsic Connect to verify new users on their platforms. Pearbnb can onboard a user with the credentials in their wallet, or they can direct them through an identity verification flow. Once a user is verified on Pearbnb, they can instantly onboard to Pocketrides. | More Info Here |
| #15 | Center Identity / Location-based key generation/recovery assisted by Ai: Matthew Vogel URL: https://centeridentity.com Current methods for key recovery are difficult, but we will demonstrate how easily a private key can be generated and recovered with the visual memory of an end user and assistance from artificial intelligence. This makes user-centric identity feasible as passwords become obsolete in light of our new approach to securing digital assets! | More Info Here |
| #16 | Provenant-Origin for Qualified vLEI Issuers: Daniel Hardman, Cliff Holsenbeck, Randy Warshaw URL: www.provenant.net GLEIF's vLEI credentials combine three concepts: the organization's identity, a person's identity, and the role that the person plays for the organization. Come see how organizational credentials can be issued using Provenant's Origin software for Qualified vLEI Issuers (QVI). | More Info Here |
| #17 | Pocketcred.com: Mahesh Balan URL: https://www.pocketcred.com/post/member-as-api-the-interoperability-and-patient-access-final-rule-and-verifiable-credentials The time is ripe for allowing people to have access to their own health data. With the emergence of Verifiable Credentials as a real-world standard being implemented in many fields; with the work being done by the open wallet foundation as well as projects such as the one by TBD.DEV for decentralized web nodes, it is now possible for people to securely carry their own health data for provider to provider. This demo is a small proof of concept for this idea. | More Info Here |
| #18 | Microsoft Entra Verified ID: Kristina Yasuda URL: https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-verified-id & https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/decentralized-identifier-overview Demonstration of Verifiers using Microsoft Entra Verified ID APIs to receive credentials from various Wallets. Main use-case that will be shown is verifying a driving license JWT-VC from the CA DMV wallet, but there might be another super cool one that can only be seen if you stop by! | More Info Here |
| #19 | Digital Credentials Consortium - VC Issuing with Admin Dashboard: Kerri Lemoie - MIT URL: http://dcconsortium.org Open source software for issuance and management of Verifiable Credentials, including batch management, notification, credential status, and support for wallet exchange through deeplinks and CHAPI via a VC-API conformant issuer, organized as services in a Docker compose network. | More Info Here |
| #20 | 3edges.com - 3Edges and verifiable credentials: Alex Babeanu URL: https://www.3edges.com/ Edges is a no-code graph-based dynamic authorization platform, which uses knowledge graphs to enforce authorization. We will demo how 3Edges now understands W3C Verifiable Credentials (VC), what they look like in a graph and how they can be used for authorization. | More Info Here |



Danube Tech @DanubeTechNews · Apr 19

...

🔥 Live from Day 2 at #IIW! Our CEO, @peacekeeper and @ankurb , led a session on Advanced Topics in DID Resolution and just presented our SaaS platform, Godiddy, during the Demo Hour sponsored by Danube Tech. Stay tuned for more updates! #DigitalIdentity #DIDResolution #Godiddy



5



10



1K



Identity.com @identity · Oct 13

...

🤝 The heart of #IIW's discussions over the past couple of days: The future of identity goes beyond technical advancements. It's about crafting a seamless and empowering user experience, bridging technological gaps, and building a collaborative, global framework that prioritizes...

Show more

Diversity and Inclusion Scholarships



Thank You to Our Diversity & Inclusion Scholarship Sponsors SprucelD and tbd

Through these sponsorships we gave reduced price & complimentary tickets and/or travel and lodging reimbursement to 7 new attendees to IIW.

We care about increasing support for women, black, and other starkly underrepresented technologists in our ecosystem. We can't build identity for everyone when demographics are homogeneous.

We are also interested in increasing participation from people that represent developing economies, as a counterpoint to the sweeping claims some SSI companies make about the technology's potential while their actual connections to those communities are limited.



Event Photos taken by Doc Searls

Doc Searls has several hundred photos of IIWXXXVII on his Flickr account

Day 1: <https://www.flickr.com/photos/docsearls/albums/72177720311953806>

Day2: <https://www.flickr.com/photos/docsearls/albums/72177720311996140>

Day 3: <https://www.flickr.com/photos/docsearls/albums/72177720312075080>

Read Phil Windley's Internet Identity Workshop 37 Report Here

https://www.windley.com/archives/2023/10/internet_identity_workshop_37_report.shtml



A photograph showing a group of approximately eight people sitting around a large, round, light-colored table. They are all facing inward, looking at their cards or at the person to their left. The table is covered with various items, including a small stack of cards, some glasses, and what looks like a can of beer. The people are dressed in casual attire, such as shirts, jackets, and a vest. The background is dark, suggesting an indoor event space.

Heidi Nobantu Saul 🐞 @nobantu · Apr 19

A lively game of Cards Against Identit being played at the end of @idworkshop Day 2 ~ hilarious to sit on the sidelines listening!

#iiw #iiw36 #cardsagainstidentity

2 1 11 419

Remembering Vittorio Luigi Bertocci



Vittorio ✅
@vibronet Follows you

Infrequent updates on cloud, identity & shampoo. Host of [identityunlocked.com](#).
Anime character. Bookworm. Toxic narcissist. May or may not be notable.

A collection of Photos taken at IIW of Vittorio - by Doc Searls
<https://www.flickr.com/photos/docsearls/albums/72177720311811349>



Attendees at IIW 37 gather with their drinks to toast, share stories, remember and celebrate Vittorio

Mike Jones reposted



Vittorio ✅
@vibronet

...

Today the OAuth step up authentication challenge protocol becomes RFC9470.

rfc-editor.org/info/rfc9470

We now have an interoperable way for resource servers to tell clients when the authentication with which the current access token was obtained is insufficient and (crucially) allows the RS to express what requirements would be acceptable... and a way for clients to use that info to influence the next authentication ceremony with the authorization server. Both are obtained with ultrasimple primitives easily added to existing SDKs, achieving sophisticated runtime behaviors without the need for complex eventing systems.

One unexpected benefit of this document is clarity we didn't know we needed. The discussion made clear that we all have different ideas and expectations about what step up authentication really means. The non normative sections of RFC9470 capture the salient point and outcomes of that discussion, hopefully facilitating communications and preempting common errors.

On a personal note. This will be the last spec I drive from idea to RFC in my life, and I couldn't have had a better coauthor than [@_b_c](#). From his world class competence to his encyclopedic knowledge of this space, but above all through his genuine desire for the best outcomes for everyone, Brian is just incredible and a joy to work with. Thank you for this wonderful last ride, dear friend.

11:19 AM · Sep 8, 2023 · 69.1K Views

10

87

436

80

↑



Brian Campbell

@_b_c

...

I wrote a short reflection about working with @vibronet on RFC9470, his recent cancer diagnosis, and the personal importance of unsophisticated humor.

identity.
Step Up from Lighthearted Joke to RFC Homage
Learn more about Vittorio Bertocci and his contributions to the Identity community. And of course, check out his hair.

pingidentity.com

Ip from
Hearted Joke
Homepage



12:41 PM · Sep 21, 2023 · 53.4K Views

3

25

101

10

↑

Link to Brian's Post: <https://www.pingidentity.com/en/resources/blog/post/vittorio-bertocci-identity-community-contributions.html>

Phil Windley reposted
Auth0 by Okta @auth0 · Oct 11
Vittorio Bertocci was a force to be reckoned with, leaving an indelible mark on the identity industry and capturing hearts along the way.

Unforgettable. Remarkable. Impactful. ❤️



11

126

410

36K

↑

You reposted



Justin Richer Ⓜ @justin_richer · Oct 7

...

The world has lost a brilliant soul and a truly great person today. I feel like I was only just starting to get to know him when he was taken from us.

@vibronet shall ever remain a singular and unique in all the world.

We'll miss you, Vittorio. Rest in peace, my dear friend.

0

6

61

4.1K

↑

t1 Phil Windley reposted

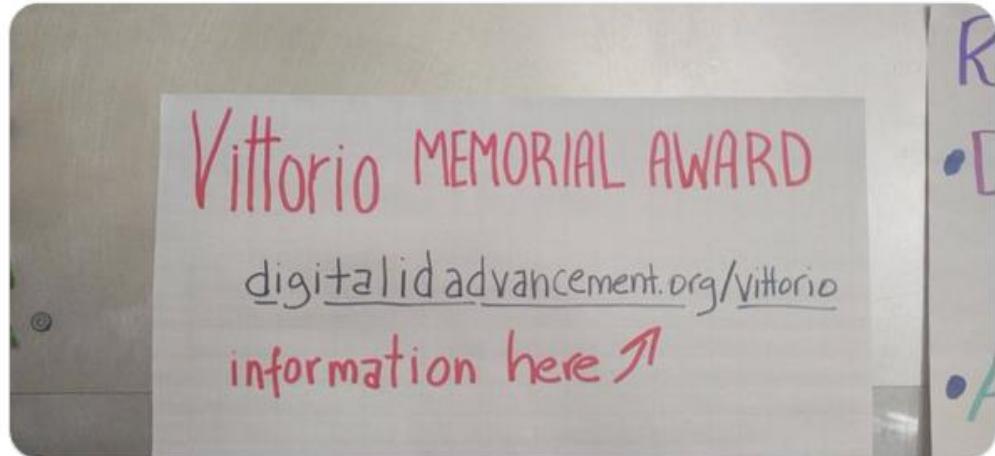
e^{iπ+1=0}

Jeff Lombardo @IdentityMonk · Oct 11

...

multiple organizations around #standards and #identity just launched an award in the name of Vittorio Luigi Bertocci @vibronet

digitalidadvancement.org/vittorio Subscribe and contribute as a way to promote the legacy and values he cherished



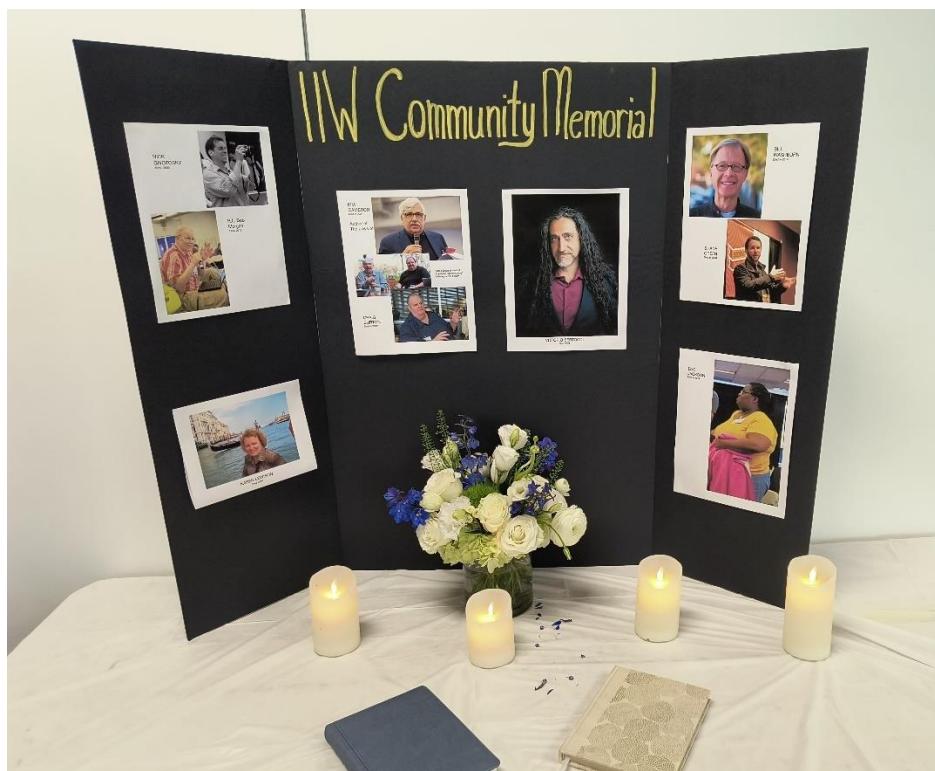
0

t1 5

22

774

Bookmark Up



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://identsphere.net>

If you want your blog to be included please email Kaliya: kaliya@identitywoman.net

A BlogPod was created at IIW - Link to IIW Slack -

<https://iiw.slack.com/archives/C013KKU7ZA4>

If you have trouble getting in, email [Kaliya@identitywoman.net](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://identsphere.net/blogcatcher/>

IIW Community dot.org's in the IIW Space: <https://identsphere.net/blogcatcher/orgsfeed/>



Phil Windley @windley · Oct 12

Louie at Bagel Street Cafe in Mountain View has been the bagel supplier for #iiw for 15 years. His bagels are the best.



1

2

18

635

1

Hope to See you April 16 - 18, 2024

IWXXXVIII / The 38th Internet Identity Workshop

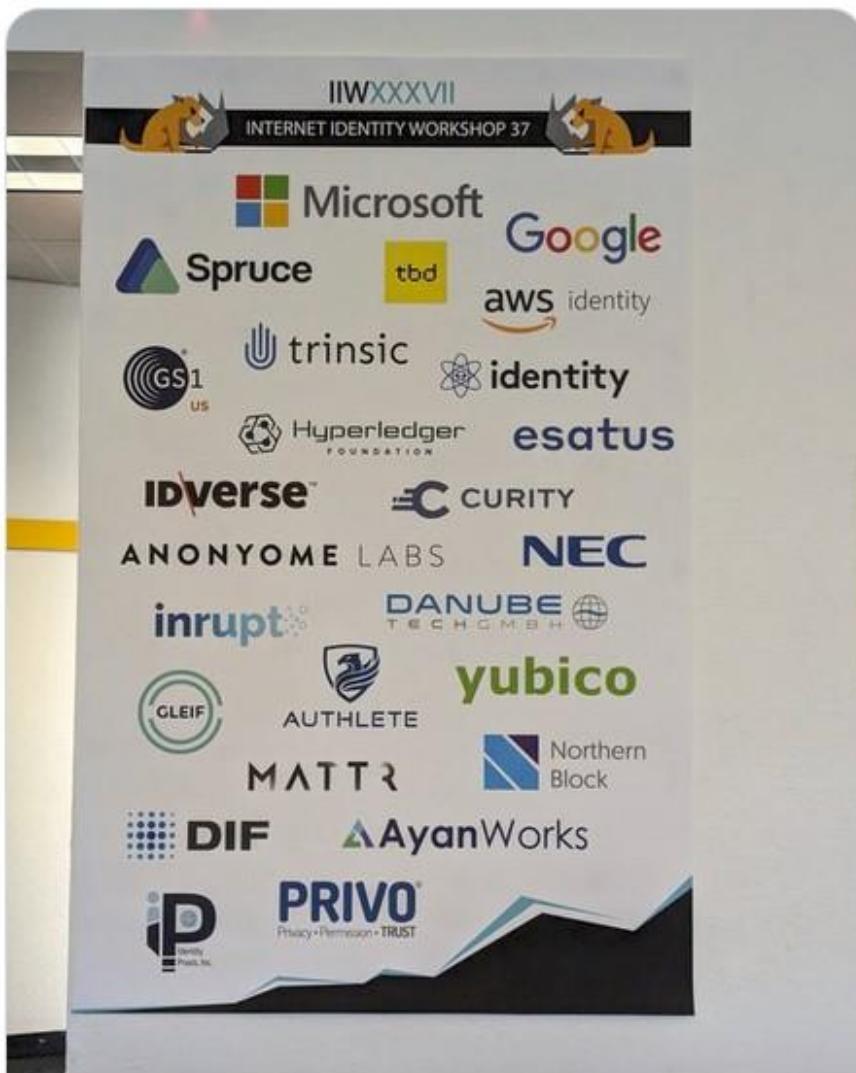
REGISTRATION OPEN



Atul Tulshibagwale @zirotrust · Oct 12

...

Thank you, @idworkshop #iiw sponsors! Getting into the last session now.



www.InternetIdentityWorkshop.com