



November 15-17, 2022

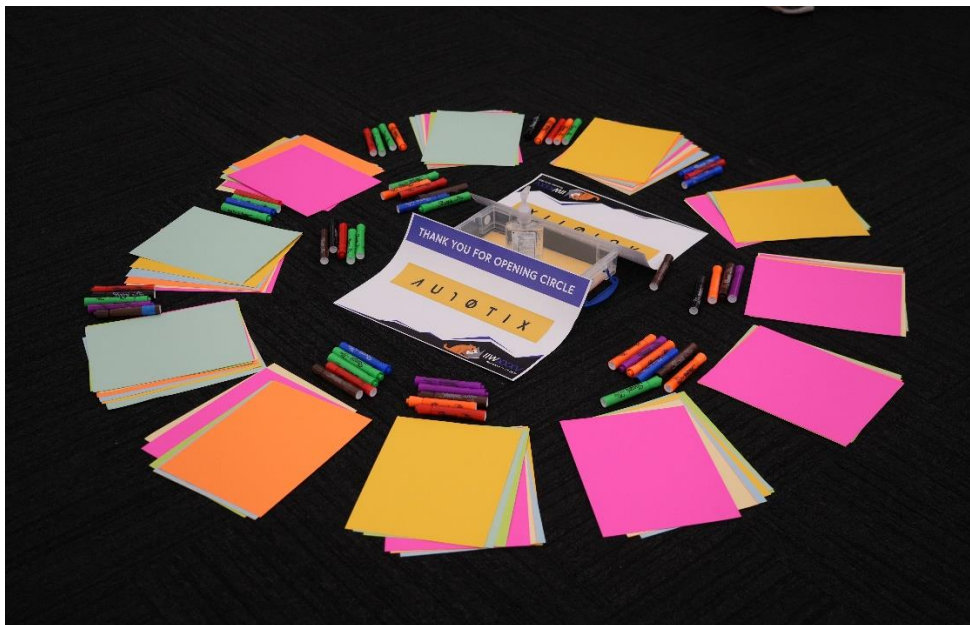
Book of Proceedings

www.internetidentityworkshop.com

Collected & Compiled by
HEIDI N. SAUL & Alli Kelley

November 15, 16, & 17, 2022

In Person at the Computer History Museum / Mountain View CA



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

IIWXXXVI In Person in Mountain View, CA

April 18 - 20, 2023

Registration open in January 2023

Thank You! Documentation Center & Book of Proceedings

Sponsors: CURITY and JOLOCOM



@curityio

@GETJolocom

Contents

| | |
|--|----|
| Thank You! Documentation Center & Book of Proceedings Sponsors: CURITY and JOLOCOM ... | 1 |
| About IIW | 7 |
| Thank You to our Sponsors! | 8 |
| IIWXXXV Daily Schedule | 9 |
| IIW35 Agenda Creation = Schedule & Workshop Sessions | 11 |
| Tuesday Nov 15, 2022 ~ Day 1 | 11 |
| Wednesday Nov 16, 2022 ~ Day 2 | 13 |
| Wednesday Nov 17, 2022 ~ Day 3 | 15 |
| Notes Day 1 / Tuesday Nov 15 / Sessions 1 - 5 | 19 |
| SESSION #1 | 19 |
| OpenID for Verifiable Credentials | 19 |
| OAuth 101 - an IIW 101 Session | 20 |
| Guardian Agent vs. Expert Agent Session Convener: Adrian Gropper | 22 |
| Unlocking Capabilities of Ethereum Keys Session Convener: Sam G | 25 |
| Making digital creds that last for decades: Using DID URLs as permanent pointers to Schemas, Visual Design, Trusted Issuer Lists, Revocation Etc. Session Convener: Ankur Banerjee (cheqd) | 25 |
| Dazzle | 28 |
| Avatar ID Session Convener: Michael Llang | 31 |
| Practical Examples (Use Cases) of SSI, My Data Session Convener: Bryan Jin | 32 |
| Mastodon and Protocols Session Convener: @bengo | 32 |
| CESR-OX - Journey of becoming a KERI contributor | 34 |
| Brand Impersonation and the VLEI Session Convener: Timothy Ruff & Karla McKenna | 35 |
| Digitized vs Digital Credentials Session Convener: Heather Flanagan | 36 |
| SESSION #2 | 38 |
| The T.OIP Reference Architecture for universal interoperability | 38 |
| Introduction to OpenID Connect an IIW 101 Session Session Convener: Mike Jones | 40 |
| FedCM 101 Session Convener: Heather Flanagan, Sam Goto | 41 |
| Putting the Fun into Functional Authorization Models Session Convener: Charles Cunningham | 43 |
| Secure Secret Storage Session Convener: Kyle Peacock | 44 |

| | |
|---|----|
| Linking DID - LEIs DID - GLEIF Registry Session Convener: Danube Tech - Markus | 45 |
| WEB5 - Platform - Development - Open Q&A / Daniel @ Block..... | 46 |
| DIDComm V2 and SICPA Announcement Session Conveners: Drummond Reed, Daniel Hardman, Sam Curren, Vlad Vujovic | 46 |
| Altruism - Capitalism: Where does sustainability lie? | 47 |
| Business Models of IDtech Session Convener: Zack Jones..... | 51 |
| Hello for WordPress Session Convener: Dick Hardt at..... | 52 |
| vLEI Update and Progress | 54 |
| Identity & Reputation for A.I. Models and Agents Session Convener: Doug King | 54 |
| SESSION #3 | 55 |
| SD-JWT (Selective Disclosure for JWTs) Session Convener: Kristina Yasuda | 55 |
| UMA (User Managed Access) IIW 101 Session Session Convener: Alec Laws | 55 |
| 'On the Internet nobody knows you're a dog.' On the Internet with Trust....? Session Convener: Wenjing Chu | 56 |
| Blockchain is Poison for the SSI Brand with The Downfall of FTX Session Convener: Trinsic & Martin Riedel (Identity.com) | 56 |
| An Analysis of Global DID Data Session Convener: Zaïda Rivai..... | 57 |
| Trust Anchor Trusted Registration with Privacy Preserving Account Recovery..... | 61 |
| VC - EDU Updates & Plugfest | 63 |
| Roger and We | 63 |
| User-Centric Identity for Voting & Election Systems Session Convener: Matthew Vogel..... | 69 |
| Passkeys | 69 |
| Beyond VCs Data XCHG + Trust Triangle | 71 |
| SESSION #4 | 72 |
| Open Wallet Foundation..... | 72 |
| FIDO 101 / An IIW 101 Session..... | 73 |
| An Introduction to Content Authenticity: an open standard for understanding content on the internet | 74 |
| Biometrics is Only the Beginning to Your Identity | 75 |
| Verifiable Issuer Lists aka: Trust Registries, is the VC legit?..... | 80 |
| The BEST DID Method (sidetree v2)..... | 80 |
| SSI in Web3 using Magic Link Wallet Self S Identity | 81 |
| Enterprise Identity and Interoperability | 81 |
| Privacy Enhancing Mobile Credentials (Listening) | 82 |
| Hyperledger AnonCreds - AnonCreds From A to W3C to ZKP..... | 82 |
| IdP Discovery and FedCM..... | 83 |
| SESSION #5 | 85 |
| The TAO of the Trust Spanning Layer KERI/ACDC/CESR/PAC WebofTrust / Zero Trust..... | 85 |
| Intro to SSI 101 / An IIW 101 Session | 85 |
| zk-SPARQL | 86 |
| NFT's & VCs in iOS & Android with Full Verification | 86 |
| SSI in (US) Healthcare ?!..... | 87 |
| Signing In The Rain: HTTP Message Signatures..... | 90 |
| Credential Profile Comparison *started at last IIW! | 91 |
| Trust Establishment for Machine Readable Governance | 91 |
| OIDC Web to App Flow Challenges and Solutions | 92 |
| Privacy Enhancing Mobile Credentials (authoring) | 93 |
| Can a FIDO Authenticator be used for Payment confirmation | 94 |
| Notes Day 2 / Wednesday Nov 16 / Sessions 6 - 10 | 97 |
| SESSION #6 | 97 |

| | |
|--|-----|
| Hello - Fasten Health, hello.coop..... | 97 |
| Web3, SSI, Web 5..... | 98 |
| Holder Binding and Wallet Authentication | 100 |
| Architecting Enterprise Cloud Agents to interact with Third-party Policy Engines | 103 |
| "Why aren't we at Afrotech?" Identity and DEI | 105 |
| Where OID4VC fits in the ToIP Stack | 107 |
| Interop Status - 17 issuers + 8 wallets!!! / CHAPI + VC..... | 108 |
| user agents, given a pico..... | 109 |
| Session Management Models | 110 |
| CCG - What is it and what are we doing? | 112 |
| SESSION #7 | 113 |
| Intro to the Mee Project | 113 |
| Mind the GNAP..... | 113 |
| How can we build provably trusted products? | 116 |
| Verifiable Credentials - Ask Me Anything | 119 |
| Secure SSI with QR Code. Why QR Code is not safe. | 120 |
| mDL <> VC - Can we all get along?..... | 121 |
| Tech Bill of Rights..... | 121 |
| It's not perfect, but at least it's a step forward? | 122 |
| Trust Registries vs. Machine Readable Governance / @darrello + @telegramSam - Re-Match_LD | 123 |
| Self Sovereign Chat with OpenChat..... | 124 |
| Client Discovery / Automatic Registration in OAuth2..... | 125 |
| Mapping FedCM to OIDC Capabilities | 125 |
| SESSION #8 | 128 |
| Human Rights Protocol Considerations in IETF GNAP | 128 |
| FIDO Alliance + Wallets..... | 129 |
| Identity & Payments: Where we are and where to go. | 129 |
| DID Method Battle Royale | 131 |
| Writing Blue Checks that your profile can't cash - Authenticity Damage..... | 132 |
| X Licensing & Collaborative Creating for 'Mutual Benefit' using WEB V Tools! | 133 |
| CHAPI + FedCM: Wallet > selection | 133 |
| Educate Regulators Fix Misunderstandings on Identity: Wrong Words..... | 133 |
| Poly, the game of governance: A Tabletop game to help people create rules to support their goals..... | 136 |
| SSI Harms: Good, Bad + Ugly | 136 |
| Enabling Native Mobile UX for OAuth/OpenID Connect flows..... | 141 |
| eIDAS Revision: History and Updates including ISO mDL and ICAO DTC | 143 |
| People are Lazy – how do we make it easier for them to do the right thing? | 144 |
| SESSION #9 | 146 |
| From Twitter to the Data Palace - product brainstorming | 146 |
| Digital Identity for A Nation: How Singapore implemented National Digital Identity using OAuth 2.0 & OIDC | 146 |
| Hyperledger ICAM Solution for a Data Centric INDOPACOM Training Environment | 148 |
| Identity & IoT | 149 |
| Co-ops: A Business Model of our Future for our Future | 153 |
| Introduction to The Trust Over IP Foundation | 161 |
| Wet/Naturally Formed Systems (People) and Interaction with Dry/Human Structured Systems (Digital Landscape) | 161 |
| How to use FIDO for everything – As alternative to SAML, as an alternative to OpenID Connect, for privacy-enhanced identification, and for user-centric identity | 163 |

| | |
|--|-----|
| What do government's need to do to unlock transformation in digital identity? | 164 |
| IIW 35 Trust Registries - A Meta Network Approach | 167 |
| Show Me The Money (Business Models of Identity) | 169 |
| Can SBT (soul bound token) be a practical tool for identification | 175 |
| Ask A Federation Operator | 176 |
| Issuing to Orgs for fun and profit: Watch us do Multisig KERI, GLEIF, ACDCs, and all that Jazz | 177 |
| SESSION #10 | 178 |
| DID Comm/OpenID & VC Comparison | 178 |
| "Don't cherry pick your favorite privacy characteristics and say "PRIVACY" | 181 |
| Privacy Enhancing Mobile Credentials = Continued | 185 |
| ID Scheme Landscape: What are the leading Identity schemes/Frameworks/Models being worked on in UK, EU, US,China | 186 |
| Roger & We: Collective Action for Collective Action..... | 186 |
| GODIDDY.com | 201 |
| What is the Perfect Key Recovery? | 202 |
| What We Can Learn from Sports Brackets, Tinder, Netflix - Ranking | 203 |
| Trade-offs for SSI Adoption | 206 |
| IF CA DMV offers VC/mDL what would you do with it?..... | 207 |
| Introduction of the new EthrRevocationRegistry2022 method w/ Delegation, Owner Change, Meta Transactions, | 208 |
| Signing XBRL Document with vLEI..... | 210 |
| I understand identity...Do you really? Let's find out. It is so much better than the movies. | 210 |
| 2 - Edged Sword: the wallet metaphor in SSI | 211 |
| Thoughtful Biometrics Workshop - Prep Idea's Questions Issues | 212 |
| Notes Day 3 / Thursday Nov 17 / Sessions 11 - 15..... | 215 |
| SESSION #11 | 215 |
| CESR for first year wizards..... | 215 |
| OpenID Connect Federation - What is it and what's new?..... | 217 |
| VC for access to a bar? Risks, benefits, privacy-perserving ways | 219 |
| Passkeys are great until they're not..... | 220 |
| SB786: California law signed in Sept by Gov to allow vital records to be issued in the VC format by county recorders. Learn what we did :-). | 220 |
| Improving the UX for Digital Wallets + Brainstorming about User Experience | 222 |
| DIDComm-terop - Veramo, Aviary Tech, roots.id..... | 233 |
| Standard Wallet Backup Container | 234 |
| Bundle Contents..... | 236 |
| your agent, given a pico..... | 236 |
| SESSION #12 | 237 |
| What the hell is holder binding? In W3C VCDM/VCs | 237 |
| Dear Web5/SSI Founder... (mistakes founders make in this space)..... | 237 |
| Healing Authority Wounds..... | 238 |
| Rebooting did:ethr | 240 |
| Self-sovereign human-based identity for the next billion. 800K users today. | 242 |
| YOUR greatest standardization regret! | 242 |
| Dazzle Office Hours | 243 |
| Practical applications and considerations of programmable VCs..... | 243 |
| Can DAO / NFT be used for Open Source Ecosystem | 244 |
| SESSION #13 | 245 |
| Can Digital Identity Platforms be Regulated? | 245 |

| | |
|---|-----|
| Self-Sovereign Dapps..... | 246 |
| Bank On It! Identity in Financial Services..... | 247 |
| Modular Blockchain Designs + ZK Rollups (Why blockchain will play important role in the future of SSI) | 249 |
| Let's talk about the byway. (Not the information highway) | 250 |
| Don't Use DIDs use DID URLs..... | 251 |
| Further Exploration of DID and VC Data Architecture with Category Theory..... | 254 |
| DID Don't explain it. Have users experience it! | 254 |
| did:dns - Current version and ideas for improvements | 255 |
| SESSION #14 | 256 |
| Authentic Web++ | 256 |
| What's the DIF(F)? Decentralized Identity Foundation Explained | 259 |
| Trans Identity | 260 |
| Verifiable Voting: Using VCs, VPs, + ZAPs to solve cryptographic voting | 260 |
| What did we learn from NSTIC + What does government need to know to re-establish/re-charge identity ecosystem. | 262 |
| Designing a 1st Year General Studies Curriculum for "Introduction to Digital Identity | 264 |
| Let's Plan a Hackathon | 266 |
| DACH lunch..... | 266 |
| Ideas for Community Building in the SSI space. / ?..... | 266 |
| SESSION #15 | 267 |
| Trust Over IP Interoperability Framework | 267 |
| DIDs as first-class citizens in the blockchain world. A showcase. | 269 |
| BBS+ + Predicate Proofs | 269 |
| Verifiable Credential Rendering (Hints)..... | 271 |
| End Surveillance Capitalism | 271 |
| Trust Alliance New Zealand..... | 272 |
| Anoncreds 2.0..... | 274 |
| DID : Keri A DID method resolver reference implementation that probably sucks. | 275 |
| The State of Hyperledger Aries and how to make a wallet in 4 hours..... | 277 |
| Does Web5/SSI have an adoption problem? | 277 |
| Speed Demo Hour / Wednesday Nov 15 / Danube TECH..... | 279 |
| Diversity and Inclusion Scholarships / SpruceID | 283 |
| Women's Breakfast / Thank You to Sponsors Randa & JFF..... | 284 |
| IIWXXXV #35 Photo Albums by Doc Searls..... | 285 |
| Stay Connected with the Community Over Time - Blog Posts from Community Members | 285 |
| Hope to See you April 18, 19, 10, 2023 | 286 |



Heidi Nobantu Saul 🐝🦋 @nobantu · Nov 14

...

It took all day ~ but we're ready for [#IIW 35](#) with 300 seats in our Opening Circle!

See you tomorrow for Opening Circle and agenda creation ~

[@idworkshop](#) the place to be this week :-)



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. IIWXXXVI (#36) will be **April 18 - 20, 2023**



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

May 16

Allowing groups to self-organize, set their own agendas, and decide without central guidance or planning requires being vulnerable and trusting. But the results are worth the risk. »

Decentralizing Agendas and Decisions [#IIW](#) <https://shar.es/afmrSE>



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

Thank You to our Sponsors!



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

Upcoming IIW Events
IIWXXXVI #36
April 18 - 20, 2023
In Person in Mountainview, CA
<https://internetidentityworkshop.com/>

IIWXXXV Daily Schedule

| TUESDAY, November 15 / Doors Open at 8:00 Doors Open at 8:00 AM for Registration Barista! - Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme - Fruit - String Cheese etc. | | | |
|--|---------------|----------------|-------------|
| Barista! And Continental Breakfast | 8:00 - 9:00 | Lunch | 1:00 - 2:00 |
| Welcome Introduction | 9:00 -10:00 | Session 3 | 2:00 - 3:00 |
| Opening Circle / Agenda Creation | 10:00 - 11:00 | Session 4 | 3:00 - 4:00 |
| Session 1 | 11:00 - 12:00 | Session 5 | 4:00 - 5:00 |
| Session 2 | 12:00 - 1:00 | Closing Circle | 5:00 - 5:45 |
| Welcome Reception & Dinner 6:00 Off the Rails Brewery 111 S Murphy Avenue Sunnyvale, CA 94086 (408) 773-9500 | | | |

| WEDNESDAY , November 16 / Doors Open at 8:00 Barista! - Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme - 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 Back A Yard Caribbean BBQ (w/V&V options) - Here at CHM! | | | |

| THURSDAY, November 17 / Doors Open at 8:00 | | | |
|---|---------------|-------------------------------|--------------|
| Barista! - Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme - Fruit - String Cheese etc. | | | |
| Opening Circle / Agenda Creation (SHARP) | 9:00 -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 | IIWXXXV Nov 15, 16 & 17, 2022 | |
| Drinks/Dinner 5ish No Host @ Das Bierhauz 135 Castro Mountain View https://dasbierhauz.com/ | | | |



Phil Windley @windley · Nov 18

...

Geographic report for #IIW 35. Map shows which countries attendees came from. Of the 343 attendees, 248 were from the US. Almost 100 from outside US. Canada: 20, Germany: 14, Switzerland: 7, UK: 6, 4 each from Sweden, France, & Austria. 3 from Sri Lanka & Japan. 6 continents.



IIW35 Agenda Creation = Schedule & Workshop Sessions



Martin Riedel @rado0x54 · Nov 15

Day 1 of #IIW at the Computer History Museum. Decision fatigue is real! 😊
(Unless you are coming to my session at 2. That's an easy choice! 😊)



171 distinct sessions were called and held over 3 Days.

We received notes, slide decks, links to presentations and photos of whiteboard work for 146 of these sessions.

Tuesday Nov 15, 2022 ~ Day 1

Session 1

- 1A/ OpenID for Verifiable Credentials 101 / Torsten, Kristina, Tobias, Oliver
- 1B/ OAuth 101 / Vittorio
- 1C/ Guardian Agent vs Expert Agent / Adrian G
- 1D/ NO SESSION
- 1E/ Unlocking Capabilities of Ethereum Keys / Sam G
- 1F/ Making Digital Creds That Last for Decades / Ankur Banerjee
- 1G/ Intro to Dazzle - All Your Data in One Place / Johannes
- 1H/ Avatar ID / Michael Llang
- 1I/ Practical Examples (Use Cases) of SSI, My Data / Bryan Jin
- 1J/ Mastadon to Protocols / Dmitri Z, @bengo
- 1K/ CESR-OX Journey of Becoming a KERI Contributor / Kent Bull
- 1L/ NO SESSION
- 1M/ Brand Impersonation and the VLEI / Timothy Ruff, Karla McKenna
- 1N/ Digitized vs Digital / Heather F
- 1O/ NO SESSION

Session 2

- 2A/ The T.oIP Reference Architecture for Universal Interoperability / Wenjing Chu
- 2B/ Intro to OpenID Connect / IIW 101 Session / Mike Jones

2C/ FEDCOM 101 / Sam G , Heather F
2D/ Putting the Fun into Functional Authorization Models / Charles Cunningham
2E/ Securely Store Secrets / Kyle Peacock
2F/ Linking DID's - LEIs / Markus, Andre, Sebastian
2G/ WEB5 - Platform - Development - Open Q&A / Daniel @ Block
2H/ DIDCOM V2 - Featuring announcement about open source from SICPA / D Hardman, S Curren, D Reid
2I/ NO SESSION
2J/ Altruism - Capitalism: Where does sustainability lie? / Marty Reed
2K/ Business Models of IDtech / Zack
2L/ HELLO - WordPress / Dick + Marius
2M/ vLEI Update and Progress / Karla McKenna
2N/ Identity & Reputation for A.I. Models and Agents / Doug King
2O/ NO SESSION

Session 3

3A/ Selective disclosure - SD-JWT / Kristina Y
3B/ UMA 101 / an IIW 101 Session / Alec
3C/ 'On the Internet nobody knows you're a dog.' On the Internet with Trust....? / Wenjing Chu
3D/ NO SESSION
3E/ Blockchain is Poison for the SSI Brand with The Downfall of FTX / J Coffen(?) and M Riedel
3F/ An Analysis of Global DID Data / Zaida Rivai
3G/ Trust Anchor - Trusted Registration with Privacy Preserving account recovery / Dr. Tina P. Srivastava, Dr. Abbie Boubir
3H/ EDU-VC & Interop PlugFest / Simone
3I/ Roger + We - an open call to burn it all down - a continuation of the VRM discussion / Chris Heyer
3J/ NO SESSION
3K/ NO SESSION
3L/ User-Centric Identity for Voting & Election Systems / Matt Vogel
3M/ Passkeys - what, why, how? / Tim Cappalli
3N/ Beyond VCs Data XCHG + Trust Triangle / Neil Thomson
3O/NO SESSION

Session 4

4A/ Open Wallet Foundation / ?, Harl, Torsl ? (hard to read names)
4B/ FIDO 101 / An IIW 101 Session / Chris Streeks
4C/ An Introduction to Content Authenticity: an open standard for understanding content on the internet / Eric Scouten
4D/ Biometrics is Only the Beginning to Your Identity / ID Guy - Ken G
4E/ NO SESSION
4F/ NO SESSION
4G/ Verifiable Issuer Lists aka: Trust Registries, is the VC legit? / Manu Sporny
4H/ The BEST DID Method (sidetree v2) / Gabe, Daniel @Block
4I/ SSI in Web3 using Magic Link Wallet Self S Identity /
4J/ NO SESSION
4K/ Enterprise Identity and Interoperability / Kyle Robinson
4L/ Privacy Enhancing Mobile Credentials ?? / @PrivacyCDN
4M/ Hyperledger AnonCreds - AnonCreds From A to W3C to ZKP / Stephen Curran BC Gov
4N/ Federated ID & IDP Discovery / Heather F
4O/ NO SESSION

Session 5

5A/ The TAO of the Trust Spanning Layer KERI/ACDC/CESR/PAC WebofTrust / Zero Trust / Sam Smith
5B/ Intro to SSI 101 / An IIW 101 Session / Limari N, Kerri L
5C/ Zk - SPARQL / Dan Yamamoto
5D/ NO SESSION
5E/ NFT's & VCs in iOS & Android with Full Verification / Haydar
5F/ SSI in (US) Healthcare ?! / Deb Bucci, Stephan Baur
5G/ Signing in the Rain - HTTP messages signatures / Justin R
5H/ Credential Profile Comparison *started at last IIW! / Torsten, Paul, Andre
5I/ Trust Establishment - DIF & ToIP / Mike Ebert
5J/ OIDC Web to APP flow challenges in Solutions / Leon Tian
5J/ NO SESSION
5K/ Privacy Enhancing Credentials / @PrivacyCDN
5L/ Can a FIDO Authenticator be used for Payment confirmation? / Francisco Corella - Pomcore
5M/ NO SESSION
5O/ NO SESSION

Wednesday Nov 16, 2022 - Day 2

Session 6

6A/ Hello - Fasten Health, hello.coop / Dick & Jason
6B/ NO/Web3 - NO/SSI - YES WEB5 / Timothy Ruff
6C/ Concepts for Wallet Security - Device Binding, Wallet Attestation / Paul B
6D/ Architecting Enterprise Cloud Agents to interact with Third-Party Policy Engines / Jacob Siebach
6E/ Why Aren't We at Afrotech? A convo on DEI + Identity / Morgan F
6F/ Where OID4VC fits in the ToIP Stack / Torsten L, Drummond R
6G/ Interop Status - 17 issuers + 8 wallets!!! / CHAPI + VC / Manu
6H/ NO SESSION
6I/ User agent, given a pico / Bruce Conrad w/Pico Labs
6J/ NO SESSION
6K/ NO SESSION
6L/NO SESSION
6M/ ONLINE ACCESS - Modern Session Management in OIDC / Vittorio & George
6N/ What's up @ W3C CCG Credentials Community Group / no name
6O/ NO SESSION

Session 7

7A/ The MEE Project Introduction - An opensource, free software agent that represents you and protects your interests online / Paul Trevithick
7B/ Mind The GNAP - Delegation beyond OAuth / Justin R
7C/ How to build demonstrably trustworthy products? / Johannes
7D/ VC - AMA (ask me anything) / Brent Zundel - Chair VCWG
7E/ NO SESSION
7F/ Secure SSI with QR Code. Why QR Code is not safe. / Abbie
7G/ MDL <> VC Can we all get along? Interview report and input request / Kaliya & Lucy
7H/ Inclusive Future Tech Bill of Rights / Jessica Tacka
7I/ It's not perfect, but at least it's a step forward? / Bryan
7J/ Trust Registries vs. Machine Readable Governance / @darrello + @telegramSam - Re-Match_LD

7K/ Open Chat Try a Self-Sovereign Chat App / Kyle Reachock
7L/ NO SESSION
7M/ Client Discovery - Automatic Registration in OAuth2 / Tobias, Mike, Kristina
7N/ Mapping FedCM to OIDC Capabilities / Heather F
7O/ NO SESSION

Session 8

8A/ Human Rights Protocol Considerations with IETF GNAP as the example / Justin R + Adrian G
8B/ FIDO Alliance + Wallets / Tim Capalli
8C/ Identity & Payments: Discussion of where we are and where to go in the future. / Tony L
8D/ DID Method Battle Royale ~ you think your DID method is cool? Then bring it!! / Nick R
8E/ Writing Blue Checks that your profile can't cash - Authenticity Damage / Chris Kelly
8F/ X Licensing & Collaborative Creating for 'Mutual Benefit' using WEB V Tools! / Jonny S
8G/ CHAPI + FedCM: Wallet > selection / Dmitri Z, Manu S, Sam Goto
8H/ WRONG WORDS & Educare Regulators to fix misunderstanding on digital identity@ BGIN / Chris (MITRE) & @ Shin'ichiro, Nat
8I/ Poly, the game of governance: A Tabletop game to help people create rules to support their goals. / Joyce & Doc
8J/ SSI Harms: Good, Bad + Ugly / Darrell O'Donnell + Neil T
8K/ NO SESSION
8L/ Enabling Native Mobile UX for OAuth/OpenID Connect flows / George Fletcher
8M/ eIDAS REVISION - EU Digital ID Wallet MDL, DTC, SSI / Dan Bachenheimer
8N/ People are LAZY - So how can we make it easier for them to do the right thing? (for privacy) / Scott Phillips
8O/ NO SESSIONS

Session 9

9A/ From Twitter to the Data Palace - product brainstorming / Johaness
9B/ Digital Identity for A Nation: How Singapore implemented National Digital Identity using OAuth 2.0 & 9C/ OIDC / Wei Lai & Tze Yuan (Asurity)
9D/ Hyperledger ICAM Solution for a Data Centric INDOPACOM Training Environment / Paul Watkins
9E/ Identity & IoT / Phil Windley & Andre Priebe
9F/ Co-Ops the business model for our future / Chris Heller
9G/ Intro to the Trust Over IP Foundation: Come learn about ToIP and how YOU can get involved. / Judith Fleenor
9H/ People vs Technology - Wet vs. Dry - Environments/Systems - Naturally Formed vs Structured Systems / Jeff O
9H/ FIDO for Everything / Francisco Corella
9I/ What do Government Officials need to do to unlock transformation in digital identity? / Gail Hodges
9J/ Trust Registry "Meta Network" Approach / John Walker
9K/ Show me the MONEY biz models cont'd / James + Zack
9L/ Can SBT (Soul Bound Token) be a practical tool for identification? / Kara Paek
9M/ Ask a Federation Operator + Demos! / Nicole Roy
9N/ Issuing to Orgs for fun and profit: Watch us do Multisig KERI, GLEF, ACDCs, and all that Jazz / Faniel Hardman
9O/ NO SESSION

Session 10

10A/DID Comm/OpenID & VC Comparison / Sam, Torsten
10B/ Don't Cherry Pick your favorite privacy characteristics and say "PRIVACY" / @_nat Nat S

10C/ Privacy Enhancing Mobile Credentials = Continued / @PrivacyCDN
 10D/ ID Scheme Landscape: What are the leading Identity schemes/Frameworks/Models being worked on in UK, EU, US,China / Michael Becker
 10E/ Roger + We II : Collective action 4 collective action / Chris Heuer
 10F/ GODIDDY.com / MarkusS
 10G/ What is the Perfect Key Recovery? / Matt Vogel
 10H/ What we can learn fromTinder, Netflix, & Sports Bracket TS to build a trusted DID Reputation System / Ankur Banerjee
 10I/ Trade-Offs for SSI Adoption / Elina Cadouri
 10J/ IF California DMV offers a Gov Credential in VC/MDL what would you do with it? / Oliver T, Wayne Chang, Gail Hodges
 10K/ Introducing Ethr Revocation Registry w/Delegation, Owner change Meta Transactions ... / Phillip B, Dennis V, Lauritz L
 10L/ Signing XBRL with a VLEI / Phil F
 10M/ I understand Identity... Do I really? Let's Find Out + This Real Identity Stuff...Is so much better than movies! / Ken G "ID Guy"
 10N/ 2 - Edged Sword: the wallet metaphor in SSI / Daniel H
 10O/ Thoughtful Biometrics Workshop - Prep Idea's Questions Issues / Kaliya

Wednesday Nov 17, 2022 - Day 3

Session 11

11A/ CESR for First Years - Composable Streaming Event Representation / Drummond Reed, Sam Smith
 11B/ OpenID Connect Federation - What is it and what's new? / Mike Jones and John Bradley
 11C/ NO SESSION
 11D/ NO SESSION
 11E/ NO SESSION
 11F/ VC for age verification to access a bar? Risks Benefits Biometrics Privacy-Preserving / Micha K.
 11G/ Passkeys are great until they're not... / Dean
 11H/ SB786: California law signed in Sept by Gov to allow vital records to be issued in the VC format by county recorders. Learn what we did :-) / Kaliya
 11I/ Designing for our Users - Improving the UX for Digital Wallets + Brainstorming about User Experience / Sukhi Chuhan and Francisco Corella
 11J/ DIDComm - terop / Varamo, Aviary Tech Roostid and... You? / Nick R
 11K/ NO SESSION
 11L/ NO SESSION
 11M/ Universal Wallet Backup Containers / Sam C + L
 11N/ Your Agent, given a Pico / Bruce Conrad
 11O/ NO SESSION

Session 12

12A/ What the hell is holder binding? In W3C VCDM/VCS / Paul B.
 12B/ Dear Web5/SSI Founder...(mistakes founders make in this space). / Timothy R.
 12C/ Healing Authority Wounds: experience taste + looking ahead workshop /Surya and Kaliya
 12D/ Rebooting DID: ethr / Phillipp B. Lauritz L. Dennis V.
 12E/ Self-sovereign human-based identity for the next billion. 800K users today. / Remco + Paolo
 12F/ NO SESSION

12G/ Your greatest standardization regret! / Andrew H.
12H/ Dazzle Office Hours (get your data back) / Johannes E.
12I/ NO SESSION
12J/ Proof of possession methods for OAuth 2.0 tokens. When to use what (open discussion) / Janak
12K/ NO SESSION
12L/ Practical applications and considerations of programmable VCs / Howard
12M/ Can we use a DAO/NFT Ecosystem to govern an Open Source Project? / Mike S. + Prof. Matsuo
12N/ NO SESSION
12O/ NO SESSION

Session 13

13A/ Can Digital Identity Platforms be Regulated? / Ken G. Adrian G.
13B/ Self Sovereign D apps / Sam G.
13C/ Web5 Ontology work group. Let's discuss authentic data, relationships and disclosure levels. / Jim M. Timothy R. Bry B.
13D/ Bank On It! Identity in financial services. / Tony T.
13E/ NO SESSION
13F/ Modular Blockchain Designs + ZK Rollups. Why blockchain will play an important role in the future of SSI. / R??a
13G/ Let's talk about the byway. (Not the information highway). / Joyce + Doc
13H/ Don't Use DIDs. Use DID URLs. / Joe A.
13I/ Further Explorations of DID and UC Data Architecture with Category Theory. / Brett S.
13J/ DID Don't explain it. Have users experience it! / Bryan
13K/ NO SESSION
13L/ NO SESSION
13M/ DID:DNS. Current version and ideas for improvements. Tomislau + Markus
13N/ SESSION
13O/ NO SESSION

Session 14

14A/ The Authentic Web Manifested + Authentic Data / Sam S. Neil T.
14B/ What's the DIF (F) Decentralized Identity Foundation Explained / Chris K.
14C/ Trans Identity / Nicole R.
14D/ Verifiable Voting: Using VCs, VPs, + ZAPs to solve cryptographic voting / Sam G.
14E/ NO SESSION
14F/ What did we learn from NSTIC + What does government need to know to re-establish/re-charge identity exosystem. / Kaliya and Ken G.
14G/ Undergraduate 1st Year: Intro to Digital Identity / ? Privacy CDN
14H/ Iso Mobile Driving License - status update. / Andrew H.
14I/ VC + DID Hackathon? Let's plan one. / Brian R.
14J/ NO SESSION
14K/ DACH lunch. / Andre
14L/ NO SESSION
14M/ NO SESSION
14N/ Ideas for Community Building in the SSI space. / ?
14O/ NO SESSION

Session 15

15A/ToIP Interoperability Framework / Judith F.
15B/ DIDs as first-class citizens in the blockchain world. / Antonio

15C/ BBS + predicate proofs. / Dan Y.

15D/ NO SESSION

15E/ Verifiable Credential Rendering / Charles L. Ben G. Dmitri Z.

15F/ Ban Surveillance Capitalism / Chris H.

15G/ SSI tech stack for New Zealand Farming / Chris C.

15H/ New and improved Anoncreds V2! A practical demo using DID: CHEQD / Ankur B.

15I/ NO SESSION

15J/ NO SESSION

15K/ NO SESSION

15L/ DID : Keri A DID method resolver reference implementation that probably sucks. / Phil F.

15M/ The State of Hyperledger Aries and how to make a wallet in 4 hours. / Kyle R. Stephen C.

15N/ Does Web5/SSI have an adoption problem? / Timothy R.

15O/ NO SESSION





SimonE @psykoreactor · Nov 15

...

This is how Trust morphs from a (technical) Triangle to a (human) circle.

Verifiable only at [#IIW](#)



Mathieu Glaude @mathieu_glaude · Nov 15

Great start to Day 1 of the Internet Identity Workshop ([#IIW](#)). 300 people in the morning circle getting ready to rumble!



1



1



5



Notes Day 1 / Tuesday Nov 15 / Sessions 1 - 5

SESSION #1

OpenID for Verifiable Credentials

Session Convener: Kristina, Tobias, Torsten,
Notes-taker(s): John Walker

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

(get link to presentation)

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

Kristina - opens with a background on OpenID
OpenID - 4 New model from ISS -> Holder -> kVerifier

OpenID for VC issuance -> openID for Verifiable

Q: Daniel Buchner - How do you achieve a high assurance with OpenID for VC? How does this support eIDAS 2.0

Kristina - walkthrough of Credential issuance of via a simple OAuth authorized API - (reference slide)
Issuance is based on the strength of OAuth

Slide: OpenID for Verifiable Presentations

“OPENID4VCS ALLOWS A VARIETY OF CHOICES IN THE VC TECH STACK

HOW ARE ALL THE FORMATS AND PROTOCOLS SUPPORTED?

ANS: OPENID4VC IS A FRAMEWORK - POLYMORPHIC STRUCTURE

LATER SESSIONS ON TOOLS BUILT TO SELECT PROTOCOLS

SLIDE “WORKING GROUP UPDATES SINCE LAST !!W - MAY 2022

-renamed from OpenID Connect 4 SSI

Conformance test - 1st version

New sub page: <https://openid.net/openid4vc>

Slide: OpenID for VC Issuance

- Pre-authorized code flow
- Changed base protocol to OAuth 2.0
- Issuance of mDL (family) profile is in the appendix to this spec
- Protocol is being done in concert to ISO mDL spec
 - ISO 18013-5 - in person
 - ISO 18013-7

- ISO 23220-4 - presentation (draft)
- ISO 23220 -4 (draft)

Slide: OpenID 4 VP

Changed base protocol to OAuth 2.0

Slide: SIOP2

SIOP 'just' means 'iss'=='sub'

Subject_signed

attester_signed

id_token_token_types supported

SIOP now supports all OpenID Connect flows

Slide: Other standards bodies & non profits & governments

Slide: Working Group Issues to be Addressed

Tobias - Interop demo

OAuth 101 - an IIW 101 Session

Session Convener: Vittorio

Notes-taker(s):

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

- Goal — to help absolute beginners to learn about OAuth2.
- The session will discuss terminology, common scenarios, framework, etc.
- The session will not discuss Centralized/Decentralized Identity or SSI.
- Comments on SSI: SSI products are likely to be successful if they are built upon existing technologies.

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

NOTES FROM IIW #33 Session led by Vittorio

Scenario 1: Naive Approach

- A user signs in to LinkedIn
- LinkedIn asks a user to send invitations to all of users' contacts via their gmail.
- User sends their gmail login credential to LinkedIn so that LinkedIn can send emails on the user's behalf
- This naive approach is problematic as LinkedIn will get unlimited access to the user's account

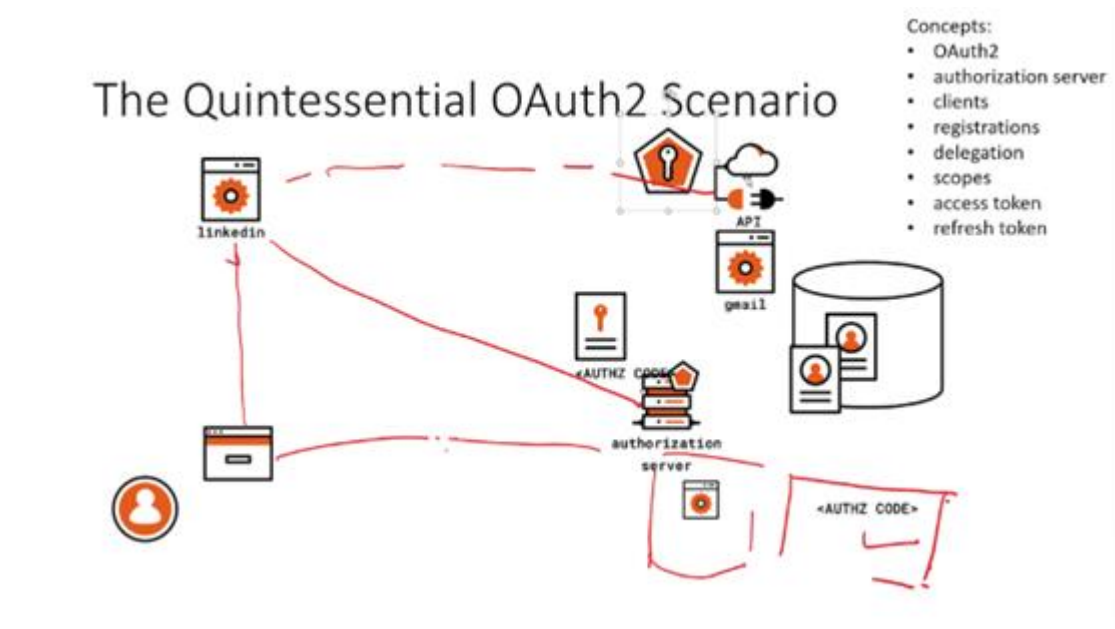
Accessing Resources Across Apps: Brute Force



Scenario 2: OAuth 2 Approach (Delegated Authorization)

- LinkedIn is registered to the Authorization Server
- LinkedIn writes an authorization message to the Authorization Server, asking to send emails for the user
- User's gmail login credential is sent (correctly) to the Gmail server (Resource Server)
- Authorization Server then send a Consent Dialogue to the user asking for the user's permission to perform the request
- If the user consent, the <authz code> will be sent to LinkedIn
- LinkedIn then sent <authz code> to the authorization server to obtain an access token
- LinkedIn sends the access token to Gmail. Gmail will only allow LinkedIn to perform the task as specified in the access token and nothing else. Hence, LinkedIn will be able to perform only the task that the user consented.

The Quintessential OAuth2 Scenario



Comments on standards

- Conventional standards arise from pre-existing technologies where lots of people use similar approaches to solve the same problem. Then, these people come together to write a standard.
- Nowadays, some standards arise from non-existing nice-to-have technologies.

Note

- OAuth is not a layer where identity federation occurs.
- Other applications/standards are built on top on OAuth to provide identity federation

Guardian Agent vs. Expert Agent

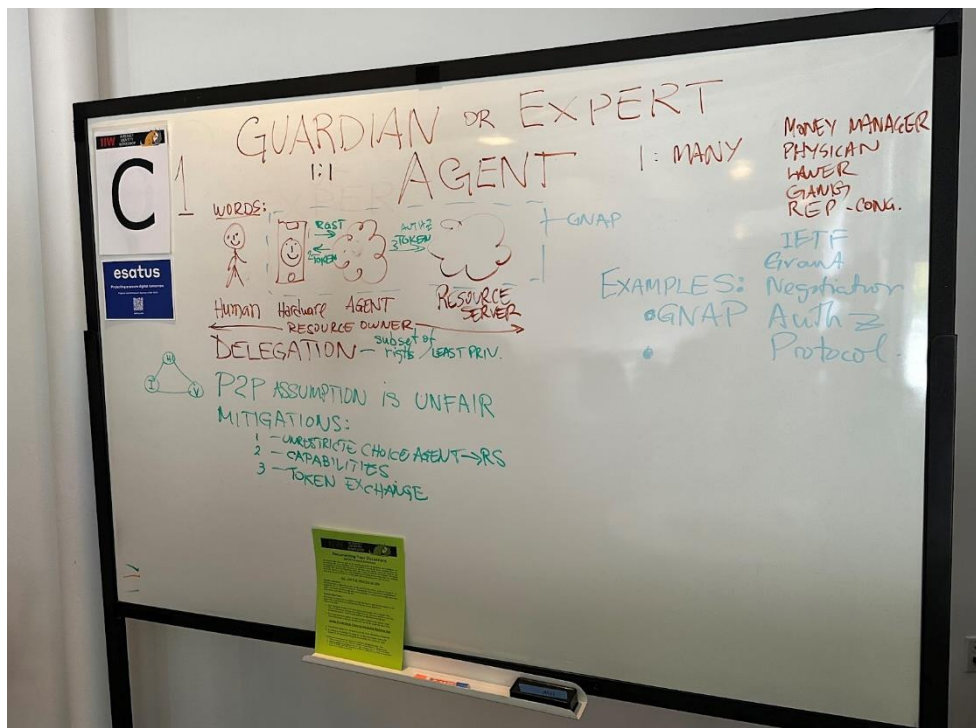
Session Convener: Adrian Gropper

Notes-taker(s): Christopher Kula

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

<https://datatracker.ietf.org/wg/gnap/documents/>
<http://bit.ly/HRPCinGNAP>

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



Previous work: definition wallets vs. agents

Open Wallet Foundation (Linux Foundation)

- new efforts such as driver's licences
- not a standards body: instead building a library of OS software

Discussion: interoperable protocols

Issue arises: what is a wallet vs. an agent?

Self-sovereignty can apply to an individual (as a right) --
it can also mean something that you empower with control.
Blockchains embody this principle.

Everything has to do with delegation.

Guardian

Somebody like the parent of a minor, or taking care of an elder. May or may not be a fiduciary.

A guardian is not assumed to be an expert.

1:1 relationship between a guardian and an identity. [Alan K. questions...]

Expert

1:many [Considered the term "aggregator"]

Examples:

Money manager

Physician

Lawyer

Gang

Representative (e.g. Congress)

Terms

Human

Accountable in the legal sense

Hardware

Has a biometric component

[Q: Is this required? A: pretty much yes]

Agent

Software in the cloud

Does not have a biometric link

[Can the agent be held responsible?]

Resource Server

Delegation:

Protocols that enable -

The ability to give a subset of one's rights to another [sth.]

Principle of Least Privilege

The IT community tries to apply the same solutions to id'ing people as to barcoding things. Bad things happen.

Q: example of misuse

A: Google Docs

The bus. model is built around: when you use you are forced to delegate your privileges for access.

All "hyperscale" platforms: Twitter, FB, etc.

Tortured attempts. to shoehorn SSI into OAuth.

Q: How do we make data interoperable? What is the objective of this session?

A: To speed up the process of interop.

Open identity auth was not enforced in design of backbone providers.

Q: Where do we want that interop to be?

A: Ex.: In the hardware layer there are (at least) two camps.

1) Link between biometrics and human is a human right. Hope that Apple, Google, etc. give it away.

2) Google and Apple etc should not be able/allowed to participate in that interaction.

Alan: Do you require wallet registration before you recognize a wallet, or do you have a protocol?

Example implementation: GNAP (Grant Negotiation and Authorization Protocol)

How can this (present) conversation help GNAP?

Nobody in that community talks about biometrics.

We should treat people differently than things.

Difference between GA and EA:

Pet peeve: asymmetry of power between individuals and the resource server.

To deal with that, you need to bring in an expert / union / gang / rep.

Orig. sin of SSI: implying that members of the trust triangle are equal peers. Assumption is unfair.

Q: Even if biometrics is assumed, the format (template) -- e.g. hash of facial features -- is not uniform.

A: Non-proprietary templates.

Alt term: to expert: specialist?

Mitigations to OAuth or GNAP:

1) Unrestricted choice of agent

2) Capabilities, i.e. choice in regards to delegation

3) Token exchange

Unlocking Capabilities of Ethereum Keys

Session Convener: Sam G

Notes-taker(s): Zack

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

[Tree LDR - Spruce](https://blog.spruceid.com/introducing-treeldr-a-canopy-across-your-data-schemas/) / <https://blog.spruceid.com/introducing-treeldr-a-canopy-across-your-data-schemas/>

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

Sam G from Spruce ID

[EIP 191](#) - Signed Data Standard

SIWE - sign in with Ethereum

- Standardized message format
- Additional capability to detect something like a phishing request

[Recaps Messages EIP 5573](#)

- “Read capability message” so users understand what they’re signing

Spruce is a part of “Chain agnostic standards alliance” - similar to EIPs but broader standards

Kepler node treats your wallet as a source of authority where you can delegate

Tracing that source of delegation, or the chain of delegation would require some amount of extension

[Spruce Rebase](#) - Witnessing Verifiable Claims

- Authenticating owners of social accounts and being able to provision access accordingly

Making digital creds that last for decades: Using DID URLs as permanent pointers to Schemas, Visual Design, Trusted Issuer Lists, Revocation Etc.

Session Convener: Ankur Banerjee (cheqd)

Notes-taker(s): Scott Phillips (Trinsic), Ajay Jadhav (AyanWorks)

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

- Presentation slides for discussion today given at [Decentralized Identity Foundation \(DIF\) on resources resolvable via DIDs](#)
- [DID-Linked Resources Specification](#) at Trust over IP Foundation wiki
- Blog post on [cheqd’s implementation of on-ledger resources](#) and [product documentation](#)

- Video of joint talk by cheqd and Animo Solutions on how resources [using DID URLs was used to support ledger-agnostic AnonCreds](#)

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

- What happens when the issuer no longer exists?
 - E.g., if there were KYC credentials issued by the FTX exchange?
 - Computer History Museum (IIW venue) is literally an archive of old technology - how hard is it to play 90s flash games, nintendo cartridges, etc?
- How do we make a statement about identity?
- Schemas are naturally used in traditional documents (lots of US drivers licenses have shared content)
 - They change visual format, but sometimes content/attributes are added
 - Systems need to understand and check associated schema *from the time the credential was issued*
 - We need to have version managed schema archives, so that we can find the old version of the schema
- We still have a single point of failure when storing schemas at a web URL - think about the Facebook outage of 2021-10-04
- The major cloud infrastructures are centralized and concentrated, 66% of the world's cloud infrastructure is AWS/GCP/Azure
- "Linkrot" breaks links on the web, all the time - columbia school of business - close to 60% of links from 1998 are dead, 40% from 2008 are dead
- We still have the question of visual representation of credentials
 - Allow the issuer to create a visual guidelines so that the owner can pick it out
 - Sometimes you get into different queues at the airport based upon the color of the loyalty card
- Canada has internationalization requirements about issuing every credential in French and english
- Keybase.io (owned by zoom) - allows people to show logos and favicons for claimed social media profiles

Crypto public/private key storage (and rotation) over the course of 10 years
 IETF Yang is a schema modeling language to define how schema can evolve over time RFC 6020
 Fundamental assertion that credentials can be extremely long-lived. We should practice credential hygiene
 We should have human readable and machine readable schema and governance files

- Think about liability in business, discovery as part of litigation
- Sometimes old credentials are valid for only certain activities (eg prove age with an old driver's license, but cannot drive)
- Create DIDDoc for Resource collection (eg for a schema)
 - Create a resource (and uid) tied to a resource collection (and uid)
 - Need diddoc controllers to update the credential as it evolves
 - Specify unique link to the resource (eg on cheqd mainnet)
 - You can have `previousVersionId` and `nextVersionId` that allows you to link to new or old versions of the did
 - This is the checksum of the did, different media types

- Discoverable resources: did method prefix, Resource Collection ID, module path, Specific Resource ID
- Took inspiration from from IPFS
- Query based syntax for a given resource collection id
- DID Core needs to have a standardized way to support resources
 - GIS did similar thing: They started with the basics, all the providers did similar things, then GIS standard adopted those things into the standard
- Max block size is 200KB, you can't put a video on the blockchain
 - There is nothing preventing `resourceUri` from have IPFS url or an https url
 - Multiple places availability for redundancy
- If you want to stop reusing schemas, maybe have copies in different locations
- DID Core is finalized, but DID Resolver is still open to modifications
- Maybe there is a schema that is published on `did:ion` or `did:polygon` you want to use - no problem. Everyone is doing did resolution already
- trustoverip confluence page: suggested optional vs required resource parameters
- Just because something might be a bad choice, doesn't mean we are going to prevent you from making that choice.
- Checksum should be a required, IPFS has it as hash-link/content ID of the file
- The whole point of did resolvers and did urls specs mean that you don't need to natively support every ledger/blockchain
- Goal is: W3C and DIF adoption for the did resolution spec that Cheqd wants to extend

What about blast pattern and DIDDoc overloading?

- * Was it deactivated because it was compromised, or because it was outdated
- * Have 1 or more did docs or did keys to publish schemas, another doc to publish resources, etc.
- * This helps reduce the blast pattern
- * You can traverse using DID URLs

Action items / next steps:

1. **Contribute or comment/feedback on [TOIP Wiki for DID-Linked Resources](#):** Working copy/draft of this spec is currently on TOIP Wiki but the objective is to turn this into a specification either as an extension of [W3C DID Resolution specification](#) or its own specification at W3C.

Dazzle

Session Convener: Johannes Ernst

Notes-taker(s): Paul Trevithick

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

Dazzle.town is the website <https://dazzle.town/>

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

Johannes Ernst (JE): we have a name and a logo. It's all about personal data.

Mission statement: we take back our personal data from the Web2 surveillance platforms to our own Web3 data place in the metaverse where we decide how our data is used and monetized.

JE: more and more people have the rights to get access to their data. E.g. taking your data from Twitter and putting into a place where people control. We call this place a data palace. <show the logo for the palace>. You own a data palace in the metaverse. It has all your data. What can you do with it.

From the user's PoV it is one place.

The project has 2 pillars: technology and governance.

Data Palace product

- My own place on the web/metaverse
- For ALL data that I've ever cared about
- With an open-ended set of software tools to interact with the data
- Controlled by me, entirely private
- Some rooms can be shared with others

Stakeholder-based governance

Doesn't work:

- Single dictator
- Wall Street pressure leading to user exploitation and manipulation
- "Give us all your data, it will be fine"

Goal:

- Product, platform and terms are governed and controlled by its users
- Individual and organization membership

Dazzle Covenant & Bylaws - the Dazzle DAO Covenant

Jurisdiction?

- JE: if you sign the VISA network you have to sign

Is this auditable for enforcement?

- ?
- JimF: JLINC could be used.

JohnW: when Dazzle is successful, people will say, oh we can do that, we have another covenant that covers our members better. So it's likely there will be multiple covenants?

- JE: the basic principles should be widely acceptable. The actual terms of a specific covenant would be specific to a specific relationships

WRT: Voting, we think this tool is interesting for people who are traditionally mistreated, so if you build vote based on reputation, doesn't that victimize those that don't participate (and have no reputation)?

- JE: we want to find some kind of governance that optimizes better than voting based on money invested

Anyone who signs the covenant is a market.

- Chris: I'm against user reputation. Brings up issues of participation and the right to be forgotten
- JohnW: reputation isn't necessarily the person who stands up and speaks at a community meeting, it could be a person who volunteers to drive people to meetings. There are issues with technocrats thinking about "do-ocracy" (people who actually do things)

Ecosystem

<showed a picture of sharing data between the palace and traditional businesses>

- Software on both sides signing a data sharing contract
- Data redistribution is not permitted

<entirely new apps (Lapps)>

<Share with Web3 businesses>

- It would be so nice to take our past friends and content and bring it in to some new place.

Questions:

Are palaces hosted together so apps can operate across a bunch of people?

- JE: as a user you have a choice of places to store your data. It's more like the WordPress model.

Jim: can I present different personas?

- JE: you share a room within it, never the entire palace

John: there are all kinds of scenarios where you'd want

We're building off data rights. This allows me to download my data AND an authorized agent.

Showed a Demo of a prototype of a web palace

Showed data pulled from Amazon, Facebook, Google.

Showed a query across data from all 3 sources. Showed searching FB data (FB has no search)

PT: how get past Captcha on the request to a website:

- JE: the situation is changing rapidly. The CA regulator started in June [2022]. Today there are many steps. But there is a lot of work in lots of places. E.g the latest EU laws say “continuous and real-time”

JohnW: there’s a nightmare use case where a parent is trying to get back her son (who died) data from FB.

<Demo of a webpage bot: builds a page of all URLs that I’ve ever shared>

Q: can you add tags? Is it editable?

- FE: if every case you can tag things and create new relationships between

Q: what id the db?

- FE: it is a graph database. The closed thing is Neo4J. Personal data tends to have a different structure than anything else.

Q: how handle shared login?

- ...

<Demo of address book>. A button that aggregates people. A unified address book. Showed typing in “Doc Searls”. Building a unified messaging history.

JimF: I’ve not seen anybody doing what you’re doing. Are you going to provide a hosted service?

- FE: the ½ dozen people that I’m hosting are hosted by dazzle

JE: hopefully there’s a business model where the commons gets funded. In DAO terminology, the community will tax the transactions.

- JohnW: your rate of taxation grows inversely to the size of the commons. A smaller and smaller fee per capita.
- JE: over time the platform over time will grow.
- JimF: you could have a multiplicity of palace providers

Chris (at MITRE). The government would love this. One place to serve a subpoena

<https://dazzle.town/>

- Telegram or Discord
- Or email johannes.ernst@DazzleLabs.net

Avatar ID

Session Convener: Michael Llang

Notes-taker(s): Andre Priebe

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

Avatar ID is the Identity in the Metaverse.

What is an Avatar, and what are its properties and features?

- Virtual, graphic representation of us in a digital world
- It can be photorealistic, but it does not have to show you. Rendering has to happen in real-time.
- Different Avatars for different personas are very likely and not completely different from our behavior in the real world.
- We can control the Avatar.

Are we in control of the Avatar or vice versa? Is there an Agency-Problem? And is the Avatar related to our Identity at all? Is the Avatar a part of us or vice versa?

Identity is about sameness in multiple interactions, but an avatar can be changed easily. But we have Avatars to be recognized easily - like our appearance in the real world.

People behave differently in digital worlds, not just in Metaverse but also in other purely digital, remote scenarios. The online disinhibition effect must be considered, even if the consequences may be in the real world.

Different avatars are "Spawn-points" for different personas of one person in the Metaverse. For good reasons we might want to have an Avatar which is significantly different than our physical representation.

The current experience of Metaverse, for instance, for meetings and workshops, is relatively weak. But we have to keep in mind that the current hardware has improved extremely during the last few years and is improving a lot.

A very important finding, we have to learn from the experiences of the past - the idea of Metaverse isn't completely new. Neohabitat was the first MMORPG released in 1985. Also, "Second life" from 2003 has several similarities with the Metaverse, but it had a couple of problems, like realistic geometry without teleporting. Therefore it ended up in 100.000s islands. Also, Metaverse won't be a 1:1 copy of the real world - why should we have photocopy machines in the Metaverse?

Our Avatar is separated from our physical body, but do we need a physical body? Recommendation to read about the "Bobiverse" - without the physical body, we are missing the ability to map the current experience to our experiences in the past.

We have to take care of the new attack vectors. A very intense experience has been shared - being in a Metaverse at a conference when one entity did very offensive and loud actions, but for the participants, there was no easy way out of that virtual room.

Practical Examples (Use Cases) of SSI, My Data

Session Convener: *Bryan Jin*

Notes-taker(s):

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

Bc-labs.net

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

We discussed about the examples of how SSI and DID were being used today. For example, a blockchain DID-based COVID vaccine passport was adopted in South Korea. It supports secure, privacy-ensuring presentation and verification of vaccination credentials for more than 43 million users. Lots of questions regarding the growth, adoption of how the government was receptive to the idea of user-centric credentials were asked and answered. Discussion on how the blockchain was used to build this verification system, and explained why it was necessary.

There were other examples of how DID based credentials were being used, such as a nursing license for travelling nurses.

Mastodon and Protocols

Session Convener: *@bengo*

Notes-taker(s):

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

<https://www.w3.org/TR/social-web-protocols/>

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

IIW Mastodon + Protocols

Dmitri: Intro. We met in SocialWG

Ben: Mastodon DMs aren't encrypted.

@bengo: I've given some talks about Mastodon and ActivityPub

* <https://www.youtube.com/watch?v=c17gjxEoyMQ>

* https://www.youtube.com/watch?v=BWfqV_adW54

Round of intros and 'why are you here'?

Mastodon

- * Lots of friction signing up and trying servers
- * Maybe hello could help people move from twitter to mastodon by just clicking through
- * e.g. some servers have approval processes
- * Link social accounts to proof you're not a bot
- * The people you follow, where are they on Mastodon?

- * Why there are so many points of friction is a byproduct of the standardization process being hard.
- * SocialWG made intentional (if unfortunate) decision to 'punt on' "Security" on ActivityPub
- * Ben: I wish the spec said 'you should use oidc' but the compromise was 'you may use oauth2'
- * We could talk about browser
- * Implement Webfinger
- * Mastodon has prepended '@bengo@mastodon.social' often. Web finger is `acct:bengo@mastodon.social` or `acct:bengoering@gmail.com`
- * Authentication often means login with password means there is a password hash in a database somewhere
- * dmitri: instances are needed for auth/authz. But also for moderation. On you instance you can see the 'local timeline' which are people on your instance.
- * What are the pinpoints that prevent people from leaving twitter?
 - * The cold start problem. Empty village problem.
 - * Cross domain user search is hard
 - * e.g. multiple beings across many domains
 - * At-mentioning your friends
 - * Which servers out there have the hash of this email address as my friends
- * In user land, everyone add to your twitter bio your activitypub actor id
- * Debirdify is a tool where you oauth into mastodon and twitter and it helps you find your twitter followees on the fediverse
- * What are the incentives for a twitter account to receive their twitter followers? (e.g. as they try to emigrate to fediverse)
- * People need to tweet or update their profile on twitter.com to point to their new activitypub actor
- * How do I find friends in general if they're not on twitter and never have?
- * Phone books have this problem too
- * What is private set intersection?
 - * Signal does this for contact discovery, but it could be even better by adding some more consent
 - * Secure multi party computing algorithms that can be used to help find the mutual friends you have with someone else, without disclosing to that friend all your other friends they don't know
 - * GitHub doesn't do this but does something kinda similar with bloom filters
- * Miskey calckey foundkey - use typescript
- * We need better protocols for what should happen when a mastodon instance needs to shut down (e.g. operator can't afford it anymore) e.g. mastodon.technology
- * joyce: It's really hard to get on mastodon. But once you're there you're with the people who care. Doc learned this sharing a post across mastodon as well as traditional social networks
- * We're still in hobbyist and bbs days of instance moderation. It's early in the fediverse.
- * We're still in the land of individual

CESR-OX - Journey of becoming a KERI contributor

Session Convener: Kent Bull

Notes-taker(s): Kent

Tags / links to resources / technology discussed, related resources

CESR

[https://github.com/SmithSamuelM/Papers/blob/master/presentations/CESR Overview.web.pdf](https://github.com/SmithSamuelM/Papers/blob/master/presentations/CESR%20Overview.web.pdf)

Recommended Reading

- Self-Sovereign Identity book from Manning specifically chapters 1-11

<https://www.manning.com/books/self-sovereign-identity>

- Keri White Paper

[https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI WP 2.x.web.pdf](https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI%20WP%202.x.web.pdf)

- Keri IETF draft Spec <https://github.com/WebOfTrust/ietf-keri>

- ACDC IETF Draft Spec <https://github.com/WebOfTrust/ietf-cedr>

- kentbull.com, Keri Start <https://kentbull.com/2022/06/05/keri-start/>

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

Why Keri?

- simple, unified identity protocol usable across multiple domains

Problem with other solutions

- The Balkanization of identity and crypto
- Hyperledger Indy applies a number of architecture assumptions
- need Interoperability between blockchains
- You don't need a distributed ledger that is globally ordered

CBDC use case

- Enables a multiplicity of payment channels

CESR

- C = Composable, 3 representations (binary, text with logging), in memory) with lossless conversion

It was more of a storytelling and information sharing session. We talked about voting and CBDC implementations of KERI, ACDC, as well as how to extend things through adding compatibility with CESR.

Brand Impersonation and the VLEI

Session Convener: Timothy Ruff & [Karla Mckenna](#)

Notes-taker(s): Karla Mckenna

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

IIW Session Brand Impersonation and the vLEI

Examples of Brand Impersonation (from the group):

- Fake website
- Telemarketer
- Fake tweet
- Fake texts
- Phishing
- Fake email
- Executive impersonation
- LinkedIn impersonation
- Fake invoices
- Fake apps
- DNS impersonation

Timothy proposed:

What two things do you need in assessing brand impersonal:

Uniquely identify the legal entity

Verify the authority of the person or thing representing the legal entity

Twitter Blue

Elon Musk – Twitter might need to become the arbiter of relationships among entities

Telecom protocol called StirShaken

FCC trying to enforce StirShaken in Robotexts – current consultation

Solution to Robocalls has not been so successful; actually is going up

Information about the LEI

Identifiers are different from authenticators.

Started with LEIs embedded in x509 certificates.

Still has limitations.

Started looking into SSI. Consulting effort. Was going to choose Sovrin.

Then GLEIF learned about KERI. Interoperability

Fraudster would not be able to prove authority to represent the entity. vLEI. Issue and hold credential.

Digitized vs Digital Credentials

Session Convener: Heather Flanagan

Notes-taker(s): Heather Flanagan

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

<https://sertifier.com/blog/the-future-of-digital-credentials-smart-certificates-badges/>

<https://openid.net/2022/10/13/fourth-implementers-draft-of-openid-connect-for-identity-assurance-specification-approved/>

<https://openwallet.foundation/>

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

Digitization is the process of transforming information from a physical format to a digital version.

Digital is something more native, more flexible.

Other thoughts in the room: these concepts are coming into the edu and employment space in a big way. As people grow skills and certifications (for example) are still paper based. The info isn't getting leveraged because they can't access it. When you talk about digitizing all that info, reading a JSON and turning it useful and turning it into a digital credential is going to take years.

What would the value be of a standalone, digitized credential without an anchor to a digital identity? Where is the original source?

Digitized credentials are (probably?) a relatively short-term concept between now, with so much paper history, and the future of 100% digital. Though much earlier history like WW2 records will always be digitized only (and only on request).

We're at an inflection point.

Looking from a content perspective that is digitized, digital is fluid content coming in, active while you're working on it, but digitized is solid, stable, fixed content. Digitized in photography would be to turn a digital photo into an NFT.

NFTs add a dimension into digital content of ownership.

Identifying yourself is the first step in digitizing your own content.

What would a bank account use case look like? Right now, it's an account number with a routing number, but there's no other metadata associated with it that makes it a solid credential. You could route money to an account, but it's much harder to get money out of an account. Third party transactions going through something like Venmo that requires verification would benefit by digital credentials, but every bank would have to agree.

The paper diploma isn't generally actually used; the verification happens regardless of the piece of paper. There has to be a trust anchor. The answer in the room is that driver's licenses are making that jump from digitized to digital credentials. It gets complicated as driver's licenses are being used for more purposes than just proof that you're legal to drive. When you digitize the credential, you can digitize part of it and spin off only the information relevant to a given transaction (e.g., age

verification). There is a pilot program in Virginia for that. It's about delivery, online purchases. It's in transition, so it's still very much built on the "paper" model still, but that's changing.

The meeting ground for digitized and digital is what we're calling eKYC. At the OI DF, they're trying to standardize how those two sets of credentials can be combined in globally interoperable ways to meet KYC requirements.

At google, looking at handling mDL in the google/android wallet. Digitized would be taking a photo of the credential and using OCR or something to verify the info. mDL is digital because the info comes straight from the DMV. The credential is issued and signed in a digital manner and directly issued by an authoritative source. With a digital wallet, we have something that hasn't happened in the identity ecosystem before: something everyone can relate to, from technical to entirely non-technical people. We also have something that all regulators can get behind, which is requiring more than two wallets. There is a new Open Wallet Foundation that is looking at how to develop wallet consortiums outside their ecosystems. We have a destination point for all things digital and digitized that everyone in the chain can relate to. We can create these wallets outside the two market players right now.

What's stronger, digital or digitized? What's more trustful? Hard to say at this point; we need a trust framework that allow people to make those judgements. (Some work here from the Privacy-Enhanced MOBILE Credential working group within the Kantara Initiative).

Just a straight photo isn't enough to be trusted; that's not really digitizing. It's more about digitalization. YOu can't compare digitized vs digital; you can't just digitize a credential.

Similar to biometric vs biographic. Realistically, we're talking about having a token, you validate it with state or local info that you get to have a drivers license. They've already taken a photo of your face, so realistically they could run your face. Are we after digitization so you're carrying a token, or are we talking digital where they can get all of that from taking your photo. The challenge is getting that info to the person on the front line.

Why get rid of tokens? Because you have so many of them. When you talk about digitization, you're taking your birth certificate, drivers license, marriage certificate, etc, and carrying all of them. YOu don't want to have all those aspects of documents. YOu want to have access to them, and you want them to be secure, but you need to worry what the security is going to look like and you need to worry about what people are going to do with it (Privacy).

Some of the branches that make up a digital identity will include digital info and digitized info.

Full digital systems suggest centralizing info, which goes counter to SSI principles. We have different levels of trust with our governments, and governments change over time, so you need to think about how to retain control of your digital identity.

To what end is all this work on digital identity happening? It's about quality of life, but how do you bring that all together?

Identification, verification, credential = that's the three areas that encompasses digital identity. Some concern that credential isn't defined well enough.

Are we getting close to a real digital identity via the work Apple is doing across the board with their wallets? It's got biometric, it's got something that you are, it's got a variety of credentials. Private industry is moving pretty quickly in this space, possibly faster than government.

Regulator in the room states that the public-private partnership is now working as well as we'd like.

SESSION #2

The T.OIP Reference Architecture for universal interoperability

Session Convener: Wenjing Chu

Notes-taker(s): Ajay Jadhav

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

<https://github.com/trustoverip/TechArch>

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

Wenjing presented:

- Stack vs. Reference Architecture
- What is the reference architecture? It is a generalization of various viable solutions
- It helps crystalize the most important architecture considerations while leave other details for substantiation
- A *Stack* is to view the decomposition *vertically* in functionality, where each higher layer incrementally adds functionality above the layer(s) below it.
- It is suitable within a domain of *locus of control* where dependencies are clearly ordered.
- But it is *not suitable* to capture relations between *loci of control*.
- The Reference Architecture is a prerequisite to to understand a Stack.
- An analogy for a Reference Architecture - a Building structure - layers vs. protocols between domains / locus of control
- For ex: Internet Architecture
 - OSI Stack - HTTP, TCP, IP, etc.
 - In reality -
 - Intra-domain routing e.g. OSPF
 - Ethernet devices, ARP, IP, ICMP, IGMP - inter-domain: e.g. BGP
- Another Example:
 - OIDC in the reference architecture view.
 - OpenID Connect Protocol - steps in abstract vs. a sequence diagram
- Most important considerations for TOIP - Design principles for TOIP

- Universal Connectivity
 - A.k.a Reachability, Interoperability, Hourglass, End-to-end
 - Decentralization
 - Authenticity
 - Verifiability
 - Confidentiality, Privacy

Reference Architecture: **Slide # 13-14-15-16**

- Subsystems are delineated by **locus of control** (domain)
- They interact through a **set of protocols**, not just one.
- Each type of subsystems has a shared stack*, but the stack is not identical across different types of **subsystems**** (e.g. Blockchain)
- Intermediary systems - message forwarding & other functions..
- E.g. a peer-to-peer **Trust Spanning Protocol** between Endpoint Systems
- Examples of **supporting systems**:
 - VDRs, Trust Registry, Witness, Watcher, Accounting/Auditing, Reputation, Discovery, etc.
- An Endpoint System
 - Locus of control composed of layers
 - Layer to layer communication, interfaces & protocols
 -

Slide #17

- Reference Architecture example two endpoint systems - A & B
- Example of how systems communicate

What Layer 2 needs - (Trust Spanning Layer)

- AID / DID + And end-to-end verifiable messaging protocol
- Properties:
 - A. authentication
 - B.
 - C.

An endpoint system example with **Indy-Aries**:

- Communicating with a Supporting system

Another example with **KERI**:

- Witness pool with Key Event Logs:
- KERI also uses other supporting systems (e.g. Watcher for confirmation) in addition to the Witness pool, as long as are required for functioning of AID or E2E
-

A Generalized Reference Architecture

- One system using Indy-Aries and another using KERI, will be able to talk to each other using the implementation reference architecture.

Intermediary Systems:

- E.g. DIDComm V2
- Works between the two end-systems

Another example - **WEB5**:

- DWN
- Can use the same Trust Spanning Layer for Universal Interoperability

An **Endpoint System's** Protocol Stack: **Slide # 24**

-

With this reference architecture, the details of each layer, interface and protocols can be specified one by one which, taken as a whole, completes the technical specification.

Introduction to OpenID Connect an IIW 101 Session

Session Convener: *Mike Jones*

Notes-taker(s): Mike Jones

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

The presentation is available at [http://self-issued.info/presentations/OpenID Connect Introduction 15-Nov-22.pptx](http://self-issued.info/presentations/OpenID%20Connect%20Introduction%2015-Nov-22.pptx) and [http://self-issued.info/presentations/OpenID Connect Introduction 15-Nov-22.pdf](http://self-issued.info/presentations/OpenID%20Connect%20Introduction%2015-Nov-22.pdf) and is posted at <https://self-issued.info/?p=2302>.

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

We discussed [OpenID Connect](#), including its design philosophy, original specifications, and subsequent specifications. We overviewed current work by the [OpenID Connect working g](#)

FedCM 101

Session Convener: Heather Flanagan, Sam Goto

Notes-taker(s): Heather Flanagan

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

<https://developer.chrome.com/blog/fedcm-shipping/>

<https://www.w3.org/community/fed-id/>

<https://privacysandbox.com/>

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

What is FedCM? A way browsers can help you exchange identity attributes between parties while maintaining a high privacy bar. At its core, it's a web platform high-level API (identity specific, but that comes with trade offs of more exclusivity vs less control). Trying to solve for the federation use case while preserving privacy.

Project has been underway for about 3 years (with various names). The initial focus was about the death of third-party cookies.

Safari and Firefox were ahead in many ways than Chrome in handling tracking prevention. The web is constructed in a fashion that has allowed tracking, and advertising networks are using the same mechanisms that the OIDF was using for some components of the protocol. Particularly impacted: front-channel logout. If the iFrame is cross-domain, those cookies count as third-party cookies.

How does FedCM know that there is a relationship between the RP and the IdP. The browser constructs that information from the UX by creating something that looks like an account chooser mediated by the browser. (Note this is actually a session chooser not an account chooser.) By establishing this relationship, things like front-channel logout will look. Since this is entirely mediated by the browser, the Googles and Facebooks won't see it.

Any sophisticated of IdP will have multiple levels of sign-in which may make this complicated (e.g., step up authentication).

Is the granularity at the IdP at the IdP level or the account level? This is a different dialogue than WebAuthn provides, which is very much at the account level.

Browser checks in with IdP on what sessions are active to construct the UX. Browsers remove the ability for the IdP to know where you're logging into until you consent.

The higher education use case brings complications because of the sheer number of IdP/RP relationships. Could the user bring their own preferred list? Or could there be a higher order of abstraction that says "we accept anything from this identity federation"? Bringing your own identity is a worthy goal.

The bootstrap component is going to be the hardest part - getting that first relationship recorded is critical.

There will be other areas where changes to prevent tracking will impact federation, particularly navigation-based tracking (aka, link decoration) and bounce tracking (aka, redirects).

If we can make FedCM compelling to solve some of the current pain points of federation, then both SAML and OIDC issues may be on the path to resolution sooner rather than later.

For consumers, Google expects that when Google exposes itself as a FedCM participant, that will encourage others to use FedCM as well, and then services like Dick Hardt's Hello can take advantage of Google's trailblazing.

Use case to explore: Tripit. They want to login with Google, but they need to be calling Tripit APIs. The site AS may have restrictions on what authentication methods are appropriate for a given client, which may in turn restrict what FedCM can show.

We haven't talked about when the list isn't sufficient for the identity the user wants to use (it shows one, but you want to switch to another identity). If you have three accounts, google, facebook, and yahoo, but are only logged into two, then the UX will say "there's this other account you're not logged into. Do you want to log into this other account?" This takes them to the account to log in, but that third IdP doesn't know yet who the RP is. This doesn't scale to the edu use case, but it's what's possible right now in the code. This then tells the browser the user is logged in and it will refresh the account list. After the user consents, the browser makes a post request to the IdP to the id-insertion endpoint. This is where the browser tells the IdP what the RP is. It has to prefill for the IdP. This is different from today's NASCAR communication.

Where does the authorization screen get presented to the user? We're separating authN from authZ; authZ is a secondary request. The consent the browser gathers is just to allow the authN. After the user consents, everything is game.

May be using consent in two different ways: an authorization server that says a client is acting a certain way, whereas FedCM is talking about the user saying "I consent for these actions to happen".

Sometime authentication flows also call fraud detection.

Timeframe: Chrome will block them in 2024, Safari and Firefox already do.

Putting the Fun into Functional Authorization Models

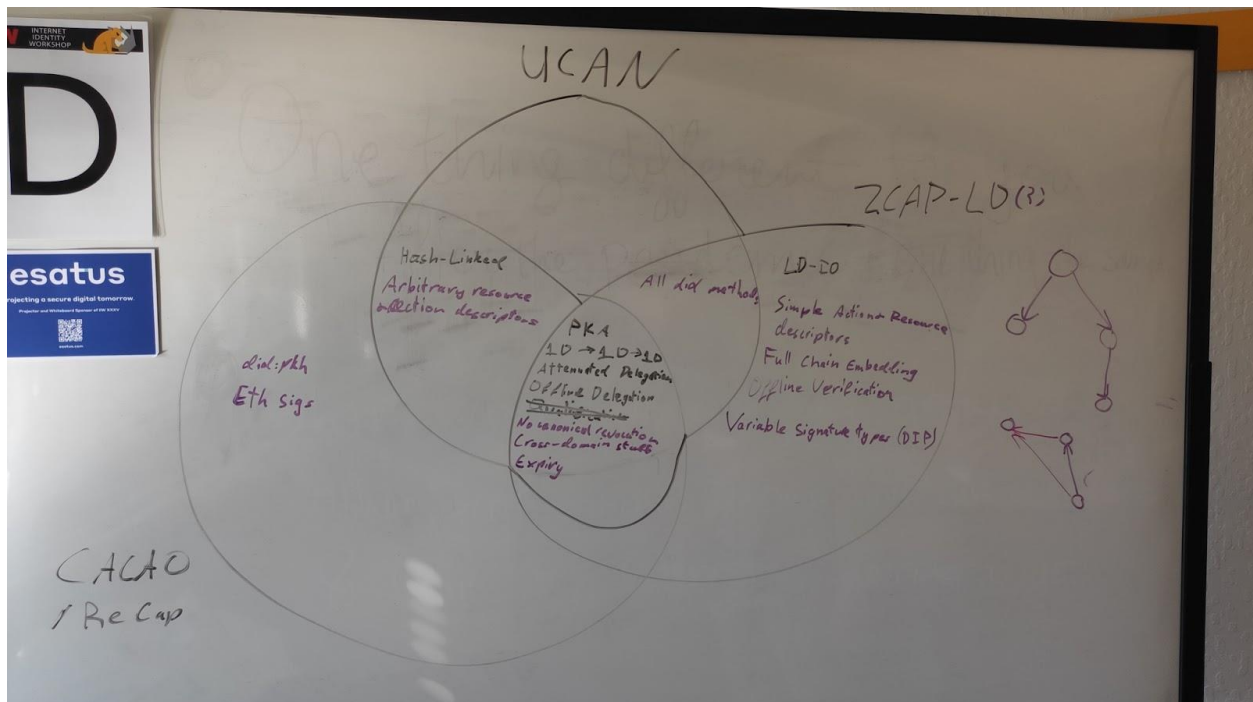
Session Convener: Charles Cunningham

Notes-taker(s):

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

Authorization Capabilities, OCaps, [UCAN](#), [ZCAP-LD](#), [CACAO](#), ReCap

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



Focusing on capability models which have emerged from the SSI space, and which specifically allow attenuated and offline delegation (delegation without communication with the resource owner/controller). We did a simple comparative analysis of features and characteristics with the aim of determining if (and to what degree) they can be used together within the same delegation chain.

Major distinctions include:

- fully-embedded parent delegations (zcap-lid and others) vs. hash-linked parent delegations (ucan and cacao), is a major complicating factor in interleaving different formats within the same chain
- All formats share a substantial amount of characteristics, due to their mutual aim of fulfilling the concepts of authorisation capabilities in a PKI backed manner
- ZCAP-LD has the most flexible format and signing possibilities
- UCAN and CACAO are specific to ecosystems based on IPLD

Additionally, several good suggestions were made for best practices

- Encryption of the parent chain to the verifier, when delegation happens, to prevent a delegatee from knowing the permissions of parent delegators

- Minimizing the number of network calls to improve performance and reduce attack surface (implicitly advocates for fully embedded delegations)
- Online delegation (where delegation requires token exchange with the resource controller) has certain characteristics which can be desirable in specific situations (gives resource owner full knowledge of delegations, makes tokens opaque to delegates to reduce information leakage, allows for hiding implementation details of the verification process, allows for secret-key (e.g. HMAC) based verification)

Secure Secret Storage

Session Convener: Kyle Peacock

Notes-taker(s): Kyle Peacock

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

Rich Authorization Request / Gnap - oauth standards

Secure EcmaScript - <https://github.com/tc39/proposal-ses>

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

The discussion is how to protect and store resources against cross-site scripting attacks, possibly requiring user interaction to access.

Outcomes -

- Cookies aren't ideal
- There may be some potential with Fido
- Secure EcmaScript is the most likely standard that will be able to help
- No definite answer today

Linking DID - LEIs DID - GLEIF Registry

Session Convener: Danube Tech - Markus

Notes-taker(s): John Walker

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

Slides: <https://drive.google.com/file/d/1Wuw76D4O3WNoJtEF8S6yecI01uib-rRI/>

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

Background on what is a DID

Background on LEI

Demo - Danube tech universal verifier

VC issued by - Danube Tech VC

Universal verifier can also check DID-LEI -> this did-lei combo is unique

Use case - wallet looks up legal entity that is behind the did

slide/ demo DID-LEI Link proof using JWT/JWS

(reference slide used by Markus)

Left side - signed by DID key

Right side - signed by vLEI key (oobi)

Slide DID-LEI Verification service - (show slide) POC process - 5 step process

At the core a DID-LEI Verification Service

Last step of the process is to Register the DID in the LEI record

What is the reality of using the VLEI to link the the DID - LEI ?

vLEI is a 'heavy' authentication -

Questions:

This solution is driven by the financial sector.

A lot of similarity to the 'well known' DID directory

Question is this demo leading to the solution being a library used in corporate 'wallet'?

Discussion point - Is the additional step of using GLEIF really worth it?

WEB5 - Platform - Development - Open Q&A / Daniel @ Block

Session Convener: Daniel @ Block

Notes-taker(s):

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

NO NOTES SUBMITTED

DIDComm V2 and SICPA Announcement

Session Conveners: Drummond Reed, Daniel Hardman, Sam Curren, Vlad Vujovic

Notes-taker(s): Drummond Reed

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

- [DIDComm V2 Specification](#)
- [Decentralized Identity Foundation Announcement of DIDComm V2 completion](#)
- [DIDComm.org](#)
- [DIDComm V2 Guidebook](#)

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

This session had two purposes:

1. Explain and give an update on DIDComm V2
2. Make an announcement about DIDComm V2 libraries from SICPA

Update on DIDComm V2

For a summary of the new features of DIDComm V2 that we covered in the session, see:

- [Decentralized Identity Foundation Announcement of DIDComm V2 completion](#)

Announcement from SICPA about DIDComm V2 Open Source Libraries

Vlad Vujovic and Victor Martinez Jurado from SICPA made the announcement that SICPA is contributing open source libraries it has developed in five different languages to both the Hyperledger Aries project and the OpenWallet Foundation for their use in open source, open standard digital wallets and agents.

VICTOR AND VLAD - PLEASE ADD EITHER A LINK TO YOUR SLIDES OR A COPY OF YOUR SLIDES OR SCREENSHOTS OF YOUR SLIDES HERE.

Altruism - Capitalism: Where does sustainability lie?

Session Convener: Marty Reed

Notes-taker(s): Charles Lehner

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

<https://www.nytimes.com/2018/02/16/opinion/sunday/tyranny-convenience.html>

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

~12 participants [12:15pm] No Cost Services vs. Cost Services

how to intersect world of making money with making
should be able to do things for free
to sustain economic opportunity
other people want to know that it makes money
how can an ecosystem sustain itself
have enough capital in the space
net positive, but sustainable?
can altruism be an on-ramp?

Mutual-benefit society

Any identity system requires force-ranking of many different components
privacy security, accessibility
different entities will rank differently
Purely-altruistic entities: NGOs
Governments: promote economic development

Look for opportunities to accelerate interactions in an ecosystem
financial incentive without cost to consumer
Per-transaction
Volume problem

How to create an ecosystem of credential exchange?

Open Source? SSI?

FLOSS developers contributing to public goods - that get co-opted by companies?

Where do you build a company in this space? What revenue does it generate - how?

Ongoing conversation how to make business about what we're passionate about

Biometrics
How to determine public consent?
Giving people choice doesn't always up-end the business model
Privacy: a loud minority (sad but true)
China going mobile-first: skipped all ideas of privacy

Privacy: user-control, safety
Tyranny of convenience. benevolent tyrant?
Security is not convenient
But have to operate in existing market?
Code at night for free?

If not able to find business model satisfying competing needs, falls back to government
centralized, not protecting privacy
absent a constituency standing up for those components, we get what we always had, traditional
centralized models that happen to have a digital component
Incentives?
Lack of choice

Who can least afford costs are impacted most

Problem of coders creating tech altruistically without profit motive
Government working with Open Source communities
Airport: government creating safety model
Partnership model?

Wrong question: how to do privacy-preserving digital health passes for international travel. 170 page
blueprint
Governments asking: how to restore travel in time for summer tourism season
Everyone has incentives

LEAP: Legislative, executive, administrative, people
Path forward with my tribe - vs. masses

Solving the right problem? Simpler than what you are trying to do
How fast to get teacher/provider through program to teach
Friction

physician and nurse credentialing
A. Cost to institutions
B. Opportunity cost (for institution and practitioner)
people would be happy to reduce 6 month process to 20 minute process

Licensed professionals get value out of this.
But have to change behavior of population, maybe significantly, and they may not want to change

Does value exceed cost ...

Enterprise identity
Traveling nurse. Driver license. Onboard to company
Doctor - issuing VCs from company
Present certs to patient
Millions of dollars

Decentralized?
Pan-Canadian network - Hyperledger registry
First name last name, date of birth

Centralized registry - very few issuers can publish onto them (decentralized amongst those issuers)

Governments not going to decentralize

Systems using foundational identity in functional contexts?

Belgium: functional identity roots back to - firewall between the two

Identity as functional, foundational, momentary...

Focus on credentials

Exchange identity for value seems pretty dirty

Exchanging credentials for value seems okay

Life is global; living is local.

Reputation currency ledger

Hard to buy insulin for reputation

Leave value as-it-is, build node

Translatory element

We know how to make sense of value

Node can place orders

Transact without taking identity out of the local space

Incentives for no-cost folks and cost folks to participate

Mutual value exchange

User-centricity

Payment going back to user: problematic

e.g. hospital paying, bank paying for KYC

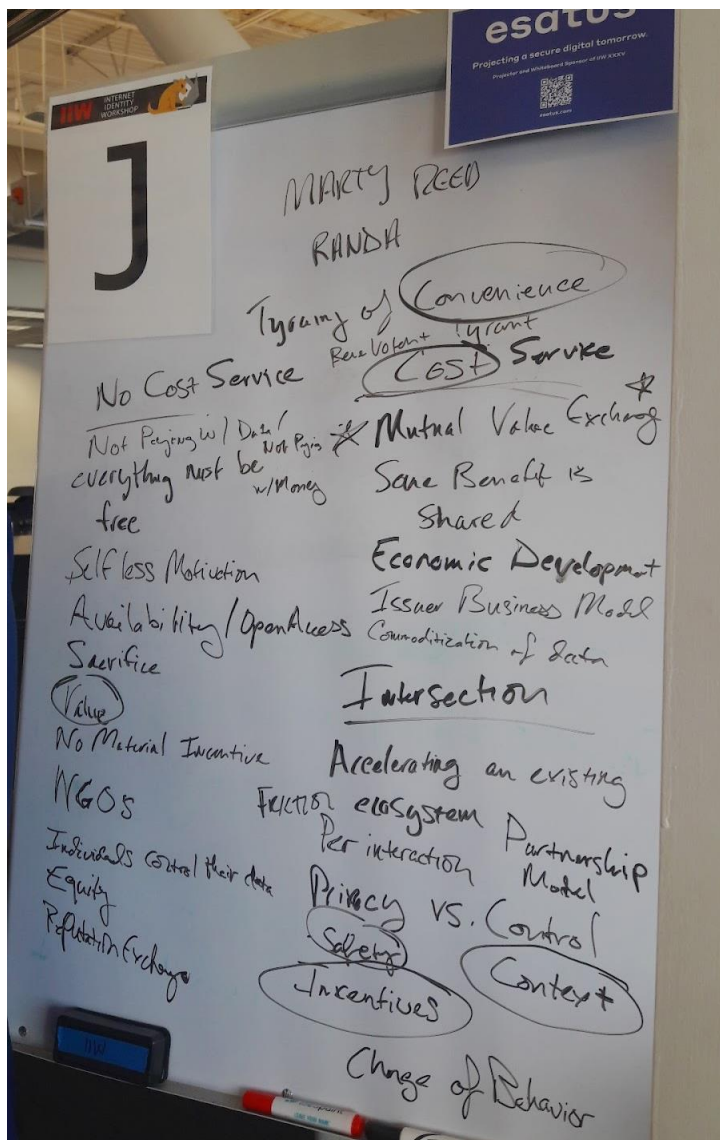
Community radio

to be commercial radio

No-cost except for electricity

Not-for-profit





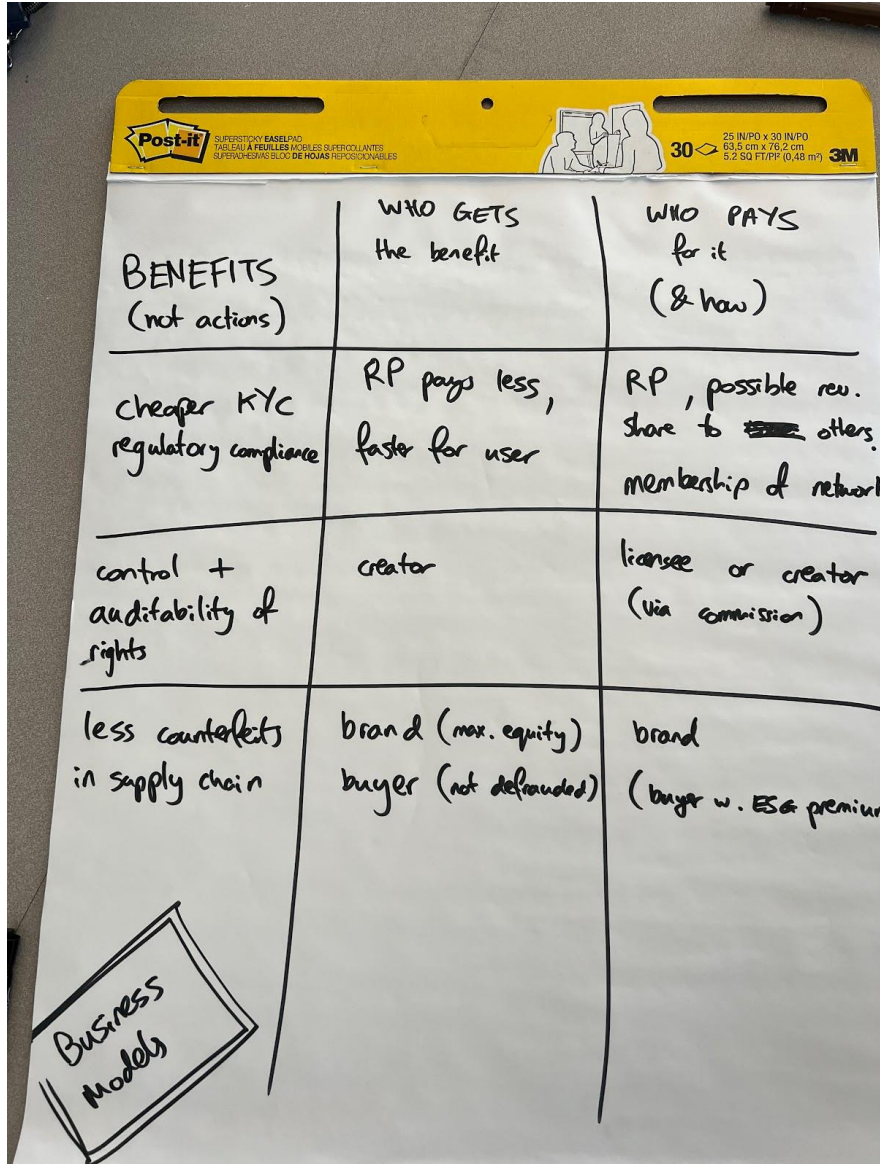
Business Models of IDtech

Session Convener: Zack Jones

Notes-taker(s): James Monaghan

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

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



The image shows a handwritten table on a yellow Post-it note. The table is titled 'Business Models' in a box at the bottom left. The table has three columns: 'BENEFITS (not actions)', 'WHO GETS the benefit', and 'WHO PAYS for it (& how)'. There are four rows of data. The first row discusses 'cheaper KYC regulatory compliance', 'RP pays less, faster for user', and 'RP, possible rev. share to ~~the~~ others. membership of network'. The second row discusses 'control + auditability of rights', 'creator', and 'licensee or creator (via commission)'. The third row discusses 'less counterfeits in supply chain', 'brand (max. equity) buyer (not defrauded)', and 'brand (buyer w. ESG premium)'. The Post-it note has a yellow header with the 'Post-it' logo and '3M' branding.

| BENEFITS (not actions) | WHO GETS the benefit | WHO PAYS for it (& how) |
|--|--|---|
| cheaper KYC regulatory compliance | RP pays less, faster for user | RP, possible rev. share to the others. membership of network |
| control + auditability of rights | creator | licensee or creator (via commission) |
| less counterfeits in supply chain | brand (max. equity) buyer (not defrauded) | brand (buyer w. ESG premium) |

Hello for WordPress

Session Convener: Dick Hardt at

Notes-taker(s):

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

[Hello.Coop](#) #Hello #Coop [The Wordpress Plugin](#)

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

Dick did a clean install of a Wordpress instance and installed the plugin in one click. Plugin is in subversion directory now, but more easily found by clicking directly to it...

<https://wordpress.org/plugins/hello-login/>.

The simplest easiest way to have Single Sign On from their centralized identity service, enabling developers and WP devs to easily have identity and authentication managed on their apps and sites.

Pulls in privacy policy of site to create a greater sense of trust.

The roles and access are still controlled from WP Admin

How does email verification work? Confirm with click on email string - Marius, please explain further

Demo of [Greenfield Demo](#), signing in with Gmail as a default, then logged out, and logged back into site with AppleID connected to the Hello id providing sign in to the app/site

“Hello is a cloud based wallet” - <https://wallet.hello.coop/>

- All your faves, plus everything else (as the co-op grows)
- Choose a preferred provider and 2 recovery accounts in case you lose access to your preferred
- It contains your profile photos from all connected accounts, and allows you to choose which pic to share with the site/app
-

BUSINESS MODEL: Charge fees on transactions that include making/sharing claims. No core access fees, so free plugin, free service until we deploy claims.

We do the interchange in the middle, serving individuals, and corporations - they do not compete with their corporate members.

Focus now is on developers, issuer's charge for claims and can make money on it, Hello takes a small percentage of that.

Will you support next ver of OpenID? Yes, as it shakes out and is finalized.

The onboarding process is pretty easy, simplifies login primarily, and then the wallet

You don't need to pick one particular sign on as a developer, with Hello, you can enable them all (well a lot today, more every month)

Reduces time to deployment by hours or perhaps longer. The devs don't need to deal with the fragmented identities that exist all over the place, empowering users to choose how to represent themselves on dev's site/app. "Harvest all your connected account profiles"

Expands the user options, instead of just seeing the 'sign in with Google' button.

Will user's be able to offer/store additional information/claims about themselves, 'self verified' like my spouse is, my children are, etc...? They can and will be doing a lot more, such as bio for enabling a simpler migration to Mastodon. Also, "bring my network" in the future

Do you want to extend this to people who want to buy something or comment on the WP? OAuth as a service to the WP Blog.

Market fit case for steep authie for login to wordpress - possible increase in security by having someone login with 2 credentials instead of just one. Obvious next step is gating access for being able to edit to the site.

As an employee, the enterprise owns your identity. - The org vs individual will be a battler for years to come... can we do something to bridge that gap? If you get enterprise adoption, its a way to get user rights in under the covers so to speak. Concern mentioned of squashing this from the top down...

Hello not necessarily an enterprise solution, but WP straddles that fence.

So many wallets. Grandma is just not going to do it, hard learning curve. (Dick - add more thoughts here, I couldn't here you) Our approach is to use all the wallets as part of identity, to aggregate them. Won't use something that they have to download... This solves for the QR code on your mobile phone for signing in.

Open Wallet Foundation.

New Features in Que:

- Invite user to Hello from WPAdmin users screen
- Adding GitHub, Twitter and others soon
- "Bring my network" functionality broadly, specifically considering Mastodon implementation now
-

vLEI Update and Progress

Session Convener: Karla McKenna

Notes-taker(s): Karla McKenna

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:

Included plans to publish the 1.0 version of the vLEI Ecosystem Governance Framework, the addition of a new authorization vLEI credential type that organizations will use to authorize QVIs to issue and revoke vLEI Role Credentials, new and improved technical features used with and by the vLEI, the launch of the vLEI Issuer Qualification Program.

The topics of authority to act on behalf of an organization and governance were discussed. The scope of the governance what is covered by the vLEI was clarified and the governance that must be put in place and maintained by organizations, stakeholders and users of vLEIs was discussed in much detail.

A full deck of detailed slides from the session is posted with the notes.

Public Link:

https://td2ec2in4mv1euwest.teamdrive.net/bqpcsfcc/public/nm3xLQTt?k=V966x6ZZyybokRaA5nhkYtDA4MU30OGV4_06Y2-9fGE

Identity & Reputation for A.I. Models and Agents

Session Convener: *Doug King*

Notes-taker(s):

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

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

NO NOTES SUBMITTED

SESSION #3

SD-JWT (Selective Disclosure for JWTs)

Session Convener: Kristina Yasuda

Notes-taker(s): Kristina Yasuda

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

Selective Disclosure, JWTs, VCs, salted hashes

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

Slides can be found here:

<https://docs.google.com/presentation/d/18uChiQHSpXPoN7EYSRGkeYbWS39b3mbbWFJ3OkCqA88/edit?usp=sharing>

UMA (User Managed Access) IIW 101 Session

Session Convener: Alec Laws

Notes-taker(s):

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

[2022-11-15 IIW UMA 101.pdf](#)

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

Please find the slides presented above. Focused questions around the flexibility and optionality of UMA to support both narrow and wide ecosystems, and how the specification is open and requires profiling during implementation. Also highlighted how OAuth systems can extend to support UMA and its use cases.

‘On the Internet nobody knows you’re a dog.’ On the Internet with Trust....?

Session Convener: Wenjing Chu

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

Blockchain is Poison for the SSI Brand with The Downfall of FTX

Session Convener: Trinsic & Martin Riedel (Identity.com)

Notes-taker(s): Martin Riedel

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:

Unstructured Notes: (Not Final)

- Blockchain has done a lot for the private key ownership.
- Frontier / Growing Pains
- Community is not aligned
- Until 2015 no Blockchain at IIW
- Germany very Anti (Public) Blockchain for SSI - CCC Krawallmacher
- Make it as simple as possible
- Decentralized identity is generally accepted.
- People use their cars everyday, SSI / Decentralized Identity should be a similar
- Concentration of clearly abstractable resources
- Reddit NFT -> Adoption without a lot of people understanding the tech.
- Accessibility vs Privacy
- Decentralization.

An Analysis of Global DID Data

Session Convener: Zaïda Rivai

Notes-taker(s): Zaïda Rivai

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

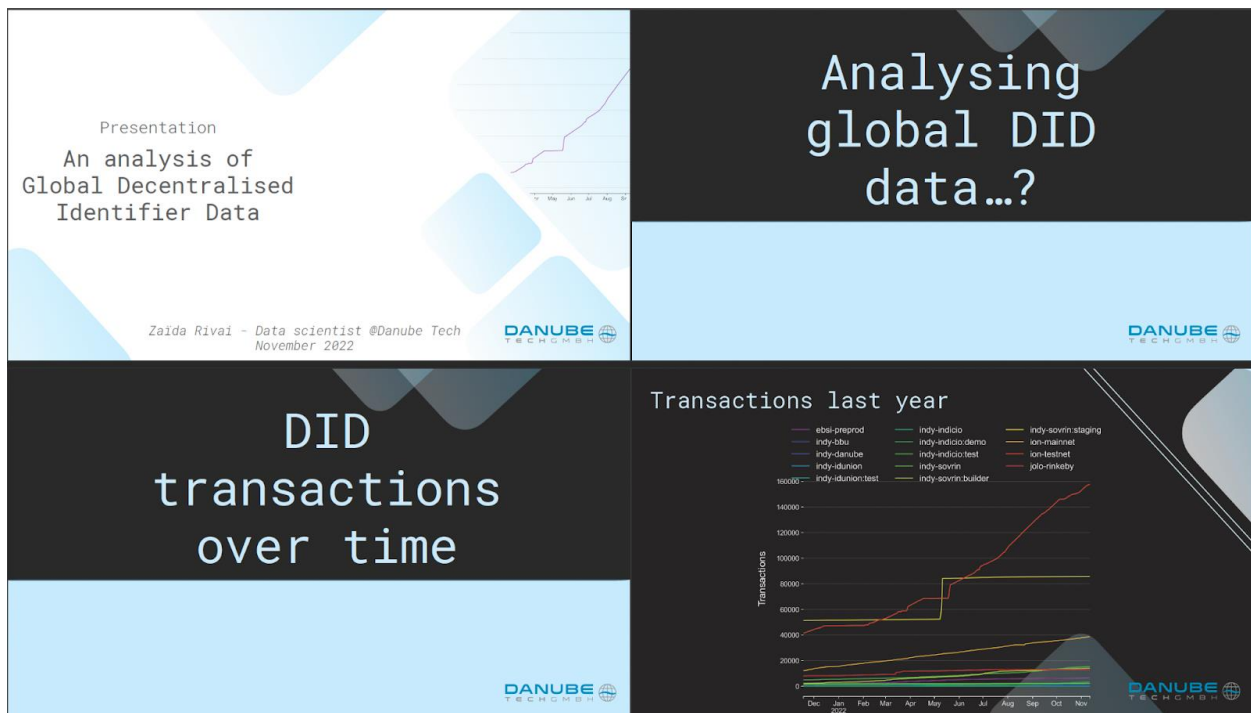
If you are interested in receiving in depth statistical analyses, contact contact@godiddy.com

Visit stats.godiddy.com to see some interesting stuff!!

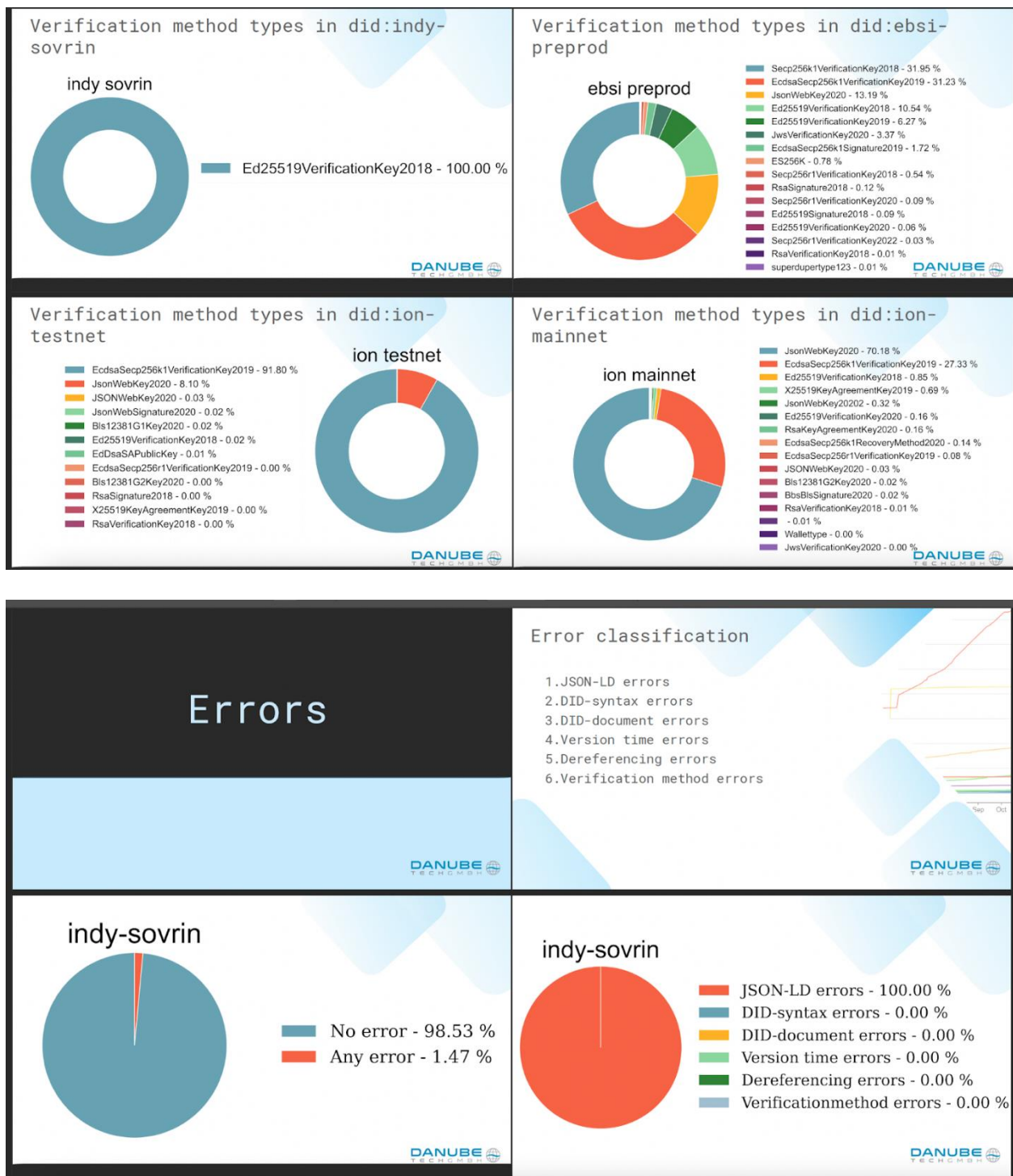
At Danube Tech GmbH we analyzed global DID data of several DID methods. Bear in mind this data shows global DID data so it is not a subset of the DIDs currently existing. We stratified based on DID method and network and showed the following:

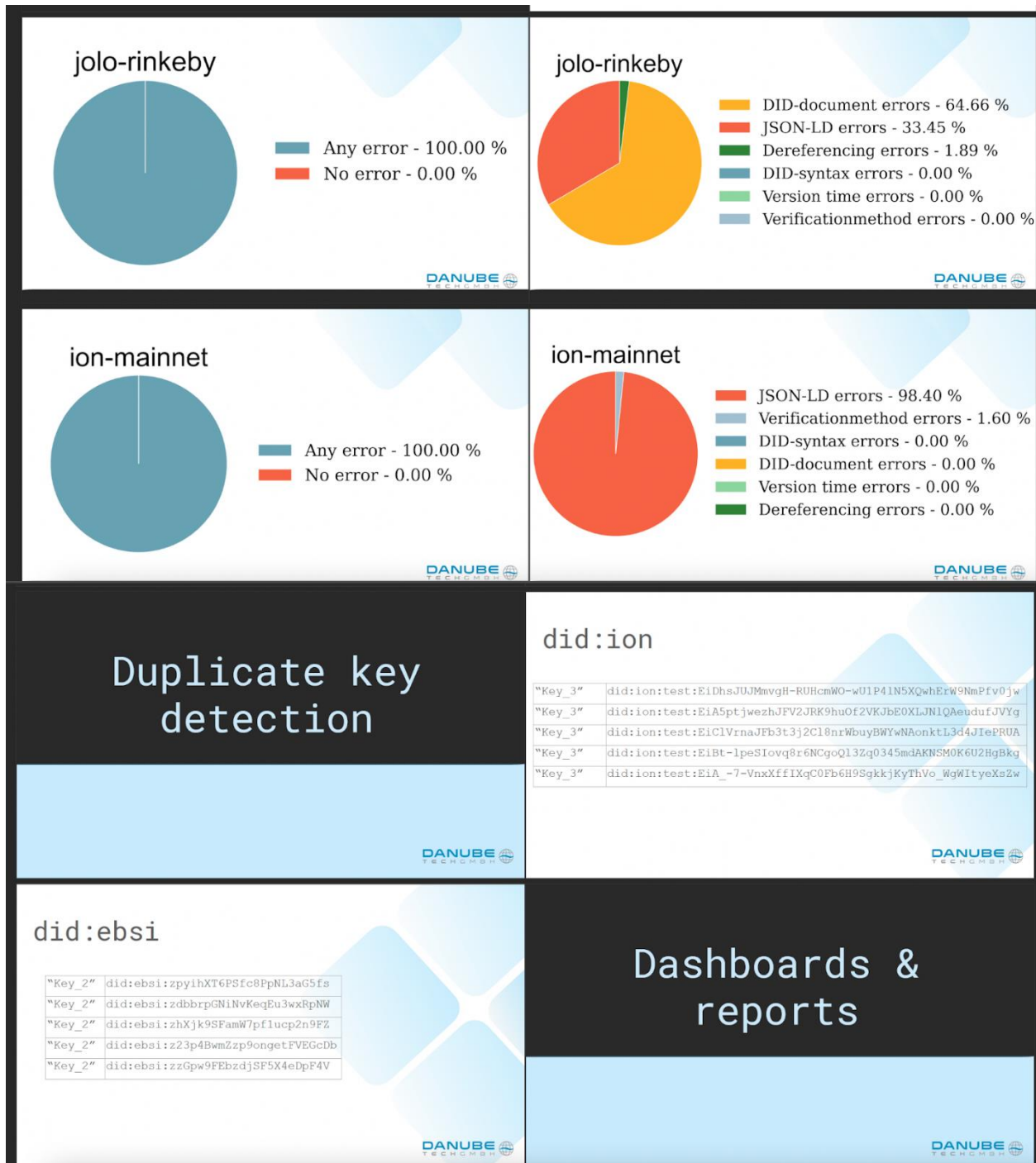
- DID transactions over time (cumulative counts)
- DID writes from the last year
- Distribution of verification method types in several DID methods
- Errors in DIDs
- Duplicate keys found in DIDs

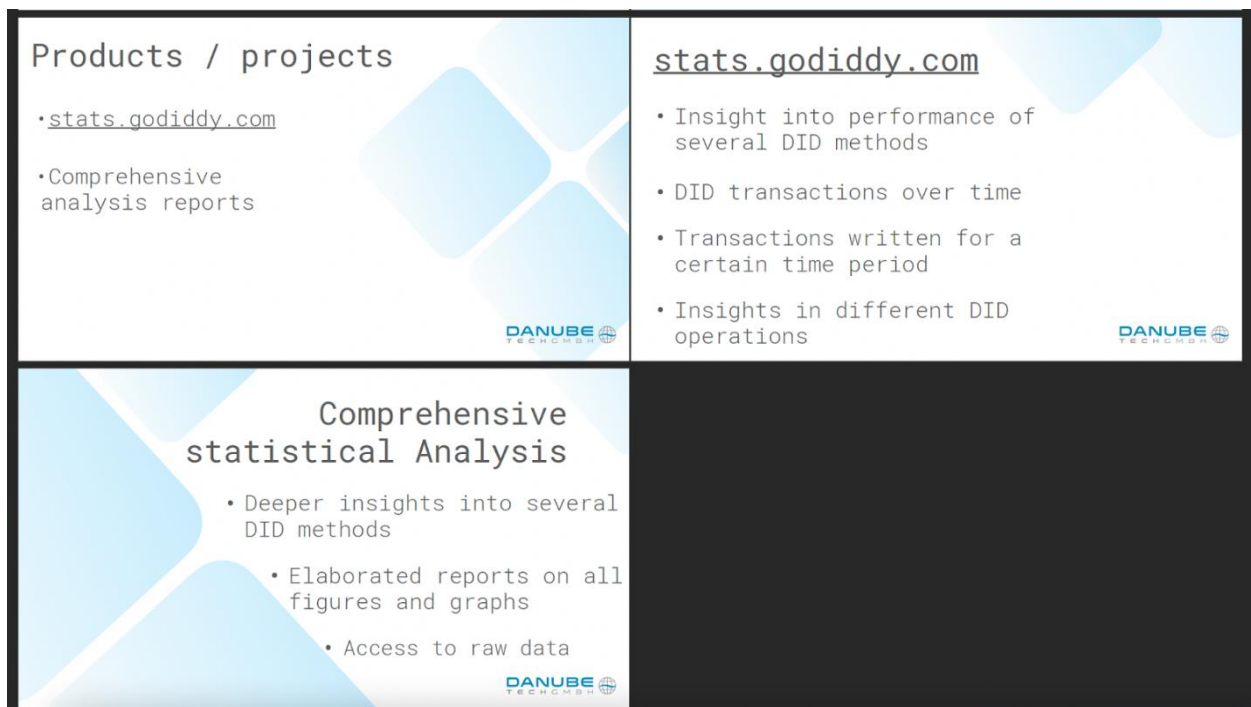
Please see the slides below:











Trust Anchor Trusted Registration with Privacy Preserving Account Recovery

Session Convener: Dr. Tina Srivastava - Dr. Abbie Barbir - Ramesh Kesanupalli - Jason Burnett

Notes-taker(s): Dr. Charles Herder

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

ADI Specification:

<https://adiassociation.github.io/ADIA-specification/ADIA-overview.html>

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

What interested you about this session? (Answers from attendees)

- These are the hardest, stickiest problems in identity
- Human experience problems
- Trust anchors are the hard problem with SSI
- Interested in learning how DIDs & SSI works
- Biggest problem is account recovery without centralization. Interested in how to do it in privacy-preserving way
- Interested in becoming a verifiable credential issuer
- User experience with user onboarding
- Recovery and registration are always the weak links in a system

- Government role in identity
- Financial sector, interested in contributing

Introduction, What is ADI Association?:

- Ecosystem of issuers, users, relying parties requires a governance framework - for example, establish assurance levels for issuers, verifiable credentials, etc. How to handle issues like an issuer issuing false credentials - by mistake or on purpose - establishing rules and processes to handle scenarios.
- Have completed Version 1 of Accountable Digital identity specification
- Includes flows for registration, account recovery, etc.
- Working with large companies who are going to be issuers and relying parties in this space.
- Starting in workforce, then to consumer
- Inviting contributions to next version

Accountability - required and should be honored by every party in the ecosystem

- from issuers, relying parties, individuals

Trust anchor is created and tied to human attributes

Network of networks

Identity registry is divided into regions (North America, Europe, Asia, etc.)

Different regions have different definitions of identity, different regulations

Get anchor in a specific region.

Biographically Based?

- Identity within a region

===

You have multiple places where there is trusted information about you

- Employer, Government, University, etc.
- First, Last, SSN, DOB, etc. is unique in this region
- Onboarded into the ecosystem by any one of the trusted issuers
- onboard with ID - confirmed with issuer, register credentials

Discussion:

- Credentials - used to confirm consent for transmission of VC from issuer to relying party
- Not re- inventing the wheel. Leveraging open standards where applicable.
- Open SPEC, not open SOURCE
- Not meant for anonymous user - meant for someone entering with an issuer (e.g., DMV)
- Lost or broken device is important problem. How user can maintain without centralized recovery or high friction IDV processes?
- Important for verified issuer to have mined credentials accurately. Analogous to CA issuers being untrustworthy
- Not storing PII is important
- Important to have a governance framework

Lots of interest in contributing to the specification.

Read specification and more information about ADI Association here:

<https://adiassociation.org/>

VC - EDU Updates & Plugfest

Session Convener: Simone Ravaioli & Kerri Lemoie

Notes-taker(s): Marty Reed

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

[vc-ed | Verifiable Credentials for Education Task Force \(w3c-ccg.github.io\)](#)

[JFF & VC-EDU | vc-ed \(w3c-ccg.github.io\)](#)

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

Roger and We

A deep dive into taking action in support of Roger McNamee's talk about reimagining the internet and putting the power back into the hands of the people.

Cheeky... an open call to burn it all down, and rebuild it with greater human centricity.

Session Convener: Chris Heuer on behalf of Customer Commons

Notes-taker(s): Chris Heuer

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

- 90 minutes of Roger's talk to VRM Salon at Computer History Museum on Monday November 14, 2022. [Audio and Transcript on Otter.ai](#)
- Roger McNamee https://en.wikipedia.org/wiki/Roger_McNamee
- His former VC firm <https://elevation.com/>
- **Audio and Transcript of our discussion** https://otter.ai/u/_yhpBT-DCKzczrNTAIw3RZ_G9-A
- The age of social Media is Ending - article https://www.theatlantic.com/technology/archive/2022/11/twitter-facebook-social-media-decline/672074/?utm_source=facebook&utm_medium=social&utm_campaign=share&fbclid=IwAR15whbXTImze-dAQ_63kVpZwT5EYMMQrC74asNefj-6uWWiaHzZ5W4gdr4

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

A deep dive into taking action in support of Roger McNamee's talk about reimagining the internet and putting the power back into the hands of the people.

Cheeky... an open call to burn it all down, and rebuild it with greater human centricity.

A few key items he mentioned:

- End surveillance capitalism
- No more billionaires (leg), turns out they aren't all that wise
- No commercial activity or applications to exploit human behavior
- Outlaw stock buybacks
- Technology isn't the solution - it's a human problem
-
- ??? What else did he say? Did you attend? Pls share to this list

Project VRM - Customer Commons -

- Profitable to harm others...
- Me to Me did list of harms

Secure personal data ownership, comms, storage, sharing - the antithesis of facebook with all the good human bits in tact.

Roger suggests we focus on a single use case to start, an activist toolkit.

- Tools for collective action
- Secure / Private
- Doesn't exist on big platforms where surveillance happens
- A space to organize, other than facebook events
 - Anonymously/Pseudonomously
 - Safely - psych safety

What is functionality?

- Distribution problem?

Why haven't existing orgs gotten more traction and impact?

Tools like CivicSpace

Roger as a unique asset, can get the message out there on CNBC

- What would he say differently next time?
- Analyze recent interviews, modernize questions and topics of interests
- Where did Facebook go wrong?
- Isn't China worse?

How are you being harmed by the internet / technology today? How to represent the voices? Build a collective directory? Same for activists?

- Fuckedprojects model
- Collect stories easily
- No IP collections, no surveillance, a model for doing it
- Conversation on how to mitigate harms
- Show how easy it is to exploit it...

Collect existing solutions and package them as a demo of key concepts

- What are key concepts/issues

Do an EARTH HOUR or SOPA...

Step 1

Get your data

Store it securely

Help us figure out what you need

Step 2

If you believe in your right to personal privacy, join us

Sign up for this substack, or this Mastodon - open source

Identity

Secure storage

Digime -

Directory for existing and emerging solutions] - join project

IIWorkshop.org

Internet Identity Now

Anti

Key Statements from his talk:

Transcript quality = 90ish%

So, I think we're in a really really, really special because a few things are really obviously true. And we're all pretending like they are so for at least a decade, everything in our economy, not necessarily bad, but literally everything has been based on the assumption that interest rates would be approximately zero. Inflation be approximately zero and that global peace would prevail. Allowing for arbitrarily long supply chains, so you can optimize labor costs all the time. Now, let's assess those three. Where would you say they are today? I would say that they're not just invalid. Today that we've moved to a different era that we are early in the multi generational re framing of the global economy in geopolitics. So just as in 1933, we abandoned unbridled capitalism in favor of collective action to fight the depression. Just as in

1981, we abandoned the New Deal, to re embrace. to re embrace unfettered capitalism. We are at a moment of decision now, I think our political leadership is conspicuously not plugged into this. Right? Very Hoover esque I would say. And I would observe that when I speak to groups, and this is very true, and I speak to college groups, people sit there and go, well, the government can't fix these problems. And I'm going really if you say that ahead of time, it becomes self fulfilling. But what we're supposed to remember is the government is that and, you know, if you're a young person today, you're being groomed to be a drone in a very large economic system, right? You go to school, you take out a huge amount of student loans into a job market where opportunities are limited. For entrepreneurs, it's almost impossible to get the biggest industries in the economy are dominated by monopolies. And you're set up for a life minutes and so I would point out that people under the age of 30 of the largest voting bloc in America and you flexed a little bit of muscle and point to the muscle and had a really big impact. If you voted 70% Rate It really changed everything our politics and everything. I'm encouraging Yes. Because I think that's the other thing I'll point out to you is that if we recognize where we are, which isn't the global economy has completely changed. We might sit there and go, gosh, are there any levers we could push that would make a difference? There's one really obvious one, which is that all of our Geopolitical Problems are the result of oil, Russia, Saudi Arabia, and as well take your pick. If I were in charge, my first rule would be I wouldn't make the value of the oil zero. I don't need to do it tomorrow. I just need to now save tension. That's the goal. And then we move the entire deal economy off of oil for two reasons. One, I'd like to save the environment so we can still breathe for the sort of children But secondly, that's the biggest economic opportunity since the early Industrial Revolution. Can you imagine how much economic value you're going to create? How much innovation you require? How many incredible startups are going to come out of sitting there and going okay, we're going off the oil completely. In fact, we're probably going to go off of individual vehicles, right? We're probably going to have to think about collective action again. Right, which means public transportation. But what happens if you do that? Have you ever looked at a map of LA and seeing how much of LA is parking lots? You know what that real estate is worth it? It stops being parking lots. Imagine highway 80. You want to have self driving trucks. You want a high speed rail across the country. Let's take Highway we'll take one direction and make it self driving trucks in two directions. So you can ship thing and the other one, we're gonna make high speed it'd be done in no time flat and you solve two problems at the same time. Right? You discourage people from driving cars and create really again, it's the Blacksburg I'm not leaving. Okay. I'm really pointing out to you. The future isn't as grim as it looks. Okay. I mean, there's a lot of bad stuff going on now. But the solution to it is actually really proceeding. So when I think about the internet when I think about the world wide web we talk about behind the web. The first thing to understand is, today's webinar is a core part of every problem we have to I mean, if you vaporize to completely we would be demonstrably better off yes, a lot of things would be inconvenient for a while. But think about how much easier it would be to solve the really big problems in society. If you didn't have a tool that was optimized for preventing you from doing anything that breaks the status quo. How much easier would it be to solve climate change, to solve gun violence to create a sense of community if you didn't have a tool that was literally optimized, prevent all those things from happening. I spent six years trying to persuade elected officials to regulate the World Wide Web for three in three different ways. First, but really for all of us, to require as a condition of market access. The demonstration sacred technology products are almost without exception today, unsafe. And I

mean, with web, it's really obvious but self driving cars, it's insane. I mean, we know how to do self driving vehicles, you put them in their own lane and you put a beacon or anything that you'd run into. That's not what we're doing. We're gonna go out there and run over 10s of 1000s of pedestrians before we figure it out. Right, because self driving cars are the Theranos of transportation. Right. Eventually, we will eventually be able to do a blood test from a drop of blood. But there's a lot of Moore's Law steps in between them. The same thing is true self driving car, doesn't mean we don't do it just which can be an honest crypto. I mean, I think we can today safely and not have facial recognition, artificial intelligence, because artificial intelligence would marriage behavioral economics is purely no social. And that is the primary economic use case of artificial intelligence that AI can provide all of these things can be valuable, but there currently no incentives to be valuable because there's no rule that says you have to protect people. You don't have to look out for the public good. And I kind of like the stocks that I like to get away from business models that exploit human weakness. Right. That's what surveillance capitalism is. It's not just in a platform for every company. They come to bracing because they all want little Facebook, Google poncho. Right? So you get a car today. To get in the door and all that other stuff and then you're an hour late with your lease payment, when are you going to use it, the faster you run, it stops these things are not serving your interests at net. So we need half rules, but I again, I'm at the point where my belief is just blow the whole thing up. Yeah, I mean, as you sit there, I totally agree with Google. I think the details matter so fucking details. What's just dropping again, blow the whole thing up and stuff. But this time, you know, because, I mean, if you sit and forget about today, all these entrepreneurs sit there and tell you but it's more economically efficient to do it our way and go, I grant you that I just don't value economic efficiency as much as I value democracy and the right to self determination. I value those things more highly. I would call with an economic inefficiency when it allows me to make a human choices or to have my you know, a politics that's based on all of us having a value in all of us being respected and all of us have been mean democracy is inherently inefficient because it requires deliberation. Same thing with self determination. I don't call it and again, that's not good or bad. thing. I don't think these people are evil, but they have a different values, which I disagree with. And as a country, we failed the public debate. And I think that's too bad. You know, because we have, but Elon Musk, he's giving us a chance to happen. Right? As you look at what's going on. I mean, anybody who thinks that billionaires are per se, wiser and smarter than the rest of us? Hard by French, especially in Indiana, you get the fucking kid I mean look up Dunning Kruger effect seriously, I mean, if I read a movie about this one guy's gonna be named Dunning. The other guys it's I mean, it's been obvious to me for more than a decade. That all you know, the secret to great entrepreneurship, is that you've got to be extraordinarily focused in a narrow area, and extraordinarily capable and completely resilient. The problem is if you start doing that in your teenage years, you go public in your early 20s By the time you're in your 30s you know, squat about anything else. Right? I mean, not anything else. And yet we sit there and assume wisdom and brilliance in all domains. And we have no safety and what if they're wrong? I mean, I have enormous admiration for people who run Silicon Valley. But I would not let them babysit children. I mean, that's not what they're good at. Okay. That's not asking people to do what they're not good at, is historically bad strategy.

So, I would like us to imagine a world in which we have ancients, in which the future is a result of conscious choices we make as opposed to passive acceptance of the status quo. I want you

to understand I do not expect to prevail in this. I spent six years at it, face to face with all of our elected officials from bottom to top. And power of the status quo is huge. But we got that number. And if young people would recognize that they have agency that nobody's gonna save right that is the choice of if you want a future. You gotta be the future you want to see. You know, so. I would like to think that the combination would happen on Election Day and the insanity going on in Silicon Valley right now will cause us all pause and start that conversation. And thank you all very much. Happy to take your questions.

That's really good. All right. So in the area, it seems like the internet has been a dystopia threat several times. dystopia is the software Catan cartel dystopia is the DRM mandate dystopia. So we've had a kind of building up of an organization or an internet freedom loving set of organizations. Today, we're kind of on the fourth level of dystopia, which is the surveillance capitalism. And this time, all the meetings are open to the public, whether it's IB for the CMA in the UK or the World Wide Web Consortium. All kinds of opportunities are available for people to come in and watch the dystopia being built in real time, whether it's on Zoom or GitHub, but we're not seeing that same activist energy that we got with the dystopia as the last time.

[Read/Listen to more at Otter.ai](#)

User-Centric Identity for Voting & Election Systems

Session Convener: *Matthew Vogel*

Notes-taker(s): Matthew Vogel

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

The USVoteFoundation.org
E2EVIV
Joe Kinery
Matt Blaze
David Wagner

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

Cryptographic voting systems have the problem where the voter would be able to sell their vote because of the verifiability of the vote.

Paper mail in ballot should be a backup to any the electronic system.

It is currently possible to have more votes for a party than there are registered voters for that party.

There are many different sources for government identifiers. This makes it difficult to ensure a cryptographic identity is truly unique.

Key management is challenge and there will need to be a practical memory based-solution to recovering a private. Center Identity proposed their visual memory based-solution for private key recovery.

Passkeys

Session Convener: Tim Cappalli

Notes-taker(s): Ajay Jadhav

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

[Passkeys.dev](https://passkeys.dev/) <https://passkeys.dev/>

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

Tim Presents:

- Intro to FIDO, WebAuthN, CTAP 1/2
- FIDO auth process explained

- Biometrics auth - external auth - using FIDO - CTAP1 and/or CTAP2
-

FIDO Properties:

Phishing Resistance

- Proximity
- Origin binding
 - time@mymail.com - login.capptoso.com
 - Works for login.capptoso.com

Challenges:

- FIDO 2 adoption has been slow
- **Roaming authenticators**
 - ... have a cost - and you generally need at least two
 - Are needed to securely bootstrap a platform authenticator
- **Consumers:**
 - Are not really interested in buying them
 - Not interested in putting them on an empty keychain
 - WebAuthN and “security key”
 - means nothing to the users

The Vision:

- As easy to use as password
- Easy to recognize and understand
- Leverages existing investments
- Needs to be durable across
- Works at scale
-

What is passkeys?:

- Not a protocol
- Noun - a password replacement
- Just like a credential certificate
- It's just **passkeys**

- Friends & Family edition
 - Use your biometric to login to the website instead of a password
- Tech savvy edition
 -
- Technologist edition
 - a FIDO2 discoverable credential which requires user verification and is backed up to survive device loss
- What gives us the passkey experience?
 - New Behavior
 - FIDO credentials can be backed up for persistence across device loss
 - Cross-device Auth

- A credential on one device can be used to sign-in on another device (e.g. Android to Windows)
- Autofill UI
 - The browser and platform can provide autofill entries for passkeys

Example: on **kayak.com** website:

- Familiar experience for users
- Dynamic
- Privacy preserving
- Simple change for RPs

Beyond VCs Data XCHG + Trust Triangle

Session Convener: Neil Thomson

Notes-taker(s): Neil Thomson

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

The presentation provides the material as presented. Other than a few minor clarification questions, there were not additional notes to add:

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

Trust “Triangle” + Data

A general approach to Data Interaction

IIW 35

Neil Thomson - QueryVision

The point of this presentation is to show an extended and expanded approach to doing data exchange between SSI Entities. This approach can be used for a wide variety of types of data exchanges in a manner that allows for establishing one or more data channels between data sources controlled by one Party/Entity with another, with only having to go through the base inter-Entity trust each time a data exchange takes place.

It does this by establishing base trust between the parties, then building a data exchange agreement/contract which creates and executes a data pipe from a data producer (source) to one or more data consumers.

SESSION #4

Open Wallet Foundation

Session Convener: Dr Torsten Lodderstedt, Hart Montgomery, Juliana Cafik
Notes-taker(s):

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

Presentation Can be found here:

https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.google.com%2Fpresentation%2Fd%2F1JW8_Wal5lPu3jWWBfzch4yhf25bOpb41%2Fedit%3Fusp%3Dsharing%26oid%3D103818431535491306994%26rtfpof%3Dtrue%26sd%3Dtrue&data=05%7C01%7Cjulianacafik%40microsoft.com%7C83ed0f85d37f429ebca908dac7f35aa7%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C638042145264550779%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTiI6IjEhaWwiLCJXVCi6Mn0%3D%7C3000%7C%7C%7C&sdata=aeL4FXyCMg%2F6CpH2%2FAklg0rHd8kBNxKxIjZAIInpoGd8%3D&reserved=0

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

101 session on the Open Wallet Foundation:

- Presentation: See link!
- Discussion Points:
 - The OWF is not building a wallet. It is an umbrella project for building core, or building blocks for wallets that are standards based;
 - ■ **Do**-ocracy: Fundamental proposal for the OWF to **do** the projects that members are willing to contribute the resources necessary to complete a project;
 - ■ Self-Organization: members self-organize “Code Projects” and associated working groups (where necessary) to propose a Code Project;
 - ■ Members have expressed interest already to contribute resources for these initial building blocks/credential types (based on the EUDI wallet as reference point) - [OWF Use Case Interest - Google Sheets](#):
 - 1.Payment Tokenisation ([EMV Payment Tokenisation Specification](#))
 - 2.ISO mDL ([ISO/IEC 18013-5:2021 - Mobile Driving Licence \(mDL\)](#))
 - 3.W3C Verifiable Credentials ([W3C Verifiable Credentials Data Model v1.1](#))
 - 4.Anonymous Credentials ([AnonCreds Specification v1.0 Draft](#))
 - ■ Code Project proposals will be required to follow (to be agreed) principles/requirements (e.g. security, privacy, interoperability), detail the requirements, the standards on which they are based, and what functions they plan to share with other projects
 - ■ Code Projects will go through a defined lifecycle.
 - Foundations for Interoperability to support different member-proposed standard credential types the OWF strives to lay a foundation for interoperability and inclusivity;

- The OWF has created an Associate Membership Group as it recognizes that the experience and expertise of Non-Profit organizations such as Open ID Foundation, OIX, DIACC, Trust Over IP can help guide the Open Wallet Foundation, and its projects and can increase the opportunities in industry and Government;
- Lively discussion about layering in human rights along with security and privacy requirements;
- Great points raised about potential challenges with code contribution, but interest in participating - OWF welcomes all contributions to the effort and welcomes participation from the community at all levels.

FIDO 101 / An IIW 101 Session

Session Convener: Chris Streeks and John B

Notes-taker(s):

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

FIDO Alliance <https://fidoalliance.org/>

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

Fast ID Online

FIDO (**Fast ID Online**) is a set of technology-agnostic security specifications for strong authentication. FIDO is developed by the FIDO Alliance, a non-profit organization that seeks to standardize authentication at the client and protocol layers.

An Introduction to Content Authenticity: an open standard for understanding content on the internet

Session Convener: Eric Scouten

Notes-taker(s): Eric Scouten

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

<https://c2pa.org>

<https://contentauthenticity.org>

<https://github.com/contentauth>

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

I started with an introductory presentation on Content Authenticity, the use cases we're trying to solve, and the technology we used to build it. ([Slide deck.](#))

Discussion after my presentation centered around several suggestions for additions to the C2PA standards:

- Digital watermarks as an additional mechanism to tie manifests back to the original content.
- Using self-certifying identifiers to establish identity.
- Discussion about potential censorship implications of identity in signed media.
- Sign metadata separately from content? Or sign portions of content separately?

Biometrics is Only the Beginning to Your Identity

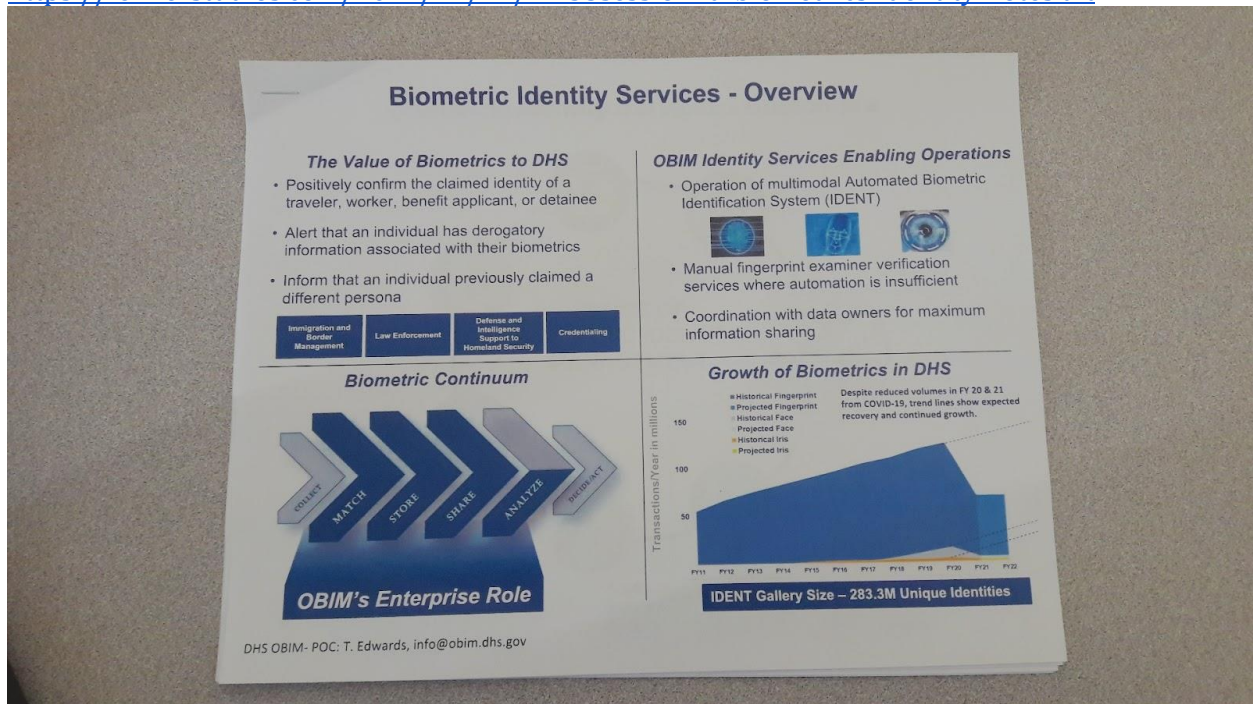
Session Convener: Ken G
Notes-taker(s): Charles L

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

Biometrics, identity, government

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

<https://lehnerstudios.com/2022/11/17/iw35session4d-biometrics-identity-notes.txt>



biometrics

10-2-1: 10 fingerprints, 2 irisis, 1 face

identity: who you are, what you have

...

[15:13pm]

lines at airports: first-world problem

defending our country - people are who they say they are

biometrics: security / convenience

adhar: largest biometrics system

for inclusion

supreme court case: supposed to be voluntary and free
but not so much; had to use to access benefits
not security. separate from national security; only for social benefits
24 hour SLA
OBIM different SLAs different?

adhar problem 2.5 years ago - looking into security
privacy, policy

US (TSA) tackling from the beginning
privacy act of 1974

identity beginning with biometrics
not just the biometric itself, but what you do with it
privacy folks asking why collect? what will you do with that information?

information sharing - certain things must follow

biographiccs - tomorrow

DoD, DHS, DoJ: 3 primary biometric systems in US government today
law enforcement, national security, immigration benefits
Department of State: primary customer, except for face - third party - outsourced
Face is a challenge

US citizen vs. others

trusted travels enrolled into OBIM
citizens

Department Homeland Security ...
Department of Justice, FBI - criminal enforcement
working for government, run you through FBI system
Department of Defence - national security - send back folks through their system and the other two

identity apparatus, sharing biometric aspects
each one has a biographical perspective
biometric is agnostic
associated data, passport

3 aspects
biometrics: identification, then verification
85% verification: "have we seen this person before?"
"derogatory information" - we don't tell them what
then they look elsewhere to find what they should know
identification: "we have nothing on that person"
credentialling: driver license, passport. getting something to use for access or identification purposes
e.g. working for port authority, use credential to get in

Q about naturalization

Identity utilizing biometric
Marriage - integration between biometric nad biographic information
biometric: common denominator

Human language technology
state department, immigration services: people have case working for some kind of benefit
phone call how to find out about your case. voice is really hard

biometrics - gait
laughs, earlobe
touches
Arnold S. walking
Standards: challenging. algorithm for matching
working with US attorneys. "how do you use those services in order to say that is the person?" not
about the biometric.
saying that about foreign nationals (not FBI)

standards allow ensuring match
policies, legal ramifications
identity of individual

direct link from biometrics leading to identity; biographics

rules for special protected classes
who is dealing with individuals sets rules
folks escaping countries where have been threatened
special protected classes in the US - can't provide data unless have nexus to criminal or national
security - even if match

policy and privacy folks. when info goes out or there is a challenge, can go back through rules on why
you provided info or identified that individual

Q about asylum seekers, for example

Who sets rules for how data/information is provided to others? Congress?
DHS: Service provider - we don't own the data. 40-50 stakeholders/customers. FBI: 3000+ (state end
local law enforcement)
The collector sets it Based on laws (Immigration act), congressional laws, presidential laws; a mix of
processes
Complex business process - may be shortcutted for simpler processes?

1856B (2004) 2 years for DHS to set up biometric entry/exit data to track all foreign nationals
entering and exiting US - congress
IIA immigration and nationalization preceede that. IMS entry/exit not biometric: paper-based I-94s,
cards to fill out; still active on land borders
biographics that hit the biometrics: come together
biometric portion, and flood of biographic information
Focus on biographics aspect; when bring together, need to have the human aspect

Chart of services provided

Inputs go into bucket, then say what should happen to person

Trying to determine identity of person in front of them, and then what should be their disposition

Red or green. going to secondary, have to answer many questions

Walking to go get bags, go through customs area with room with glass, see people sitting; waiting for stuff to come back saying let them go in; something has been presented that doesn't make sense (is questionable)

Identity having to begin with biometric. where to go from there?

Understanding of identity behind the scenes? People think they control it.

Look at the amount of paper and tokens in play

Most people doing trusted traveler program

If served, may have given up DNA

If gone to work for entity, may have taken your picture. Many places do comparison (challenging)

Facial recognition not yet "it"; gold standard still fingerprint

Paperwork... but there are self aspects going into it

What documents do you have out there, before death? A lot

Wallets getting smaller, things going into phone; phone becoming more of identity; how are sharing?

Become advocates

Identity - critical infrastructure?

Building infrastructure, get identity where it needs to be, holistically

"critical infrastructure" term of art?

aspects of government that if failed would be catastrophic to US, public safety, quality of life

banking industry (1930s), energy, water, transportation, health

National Infrastructure protection play 2013 (first 2006)

Emergency services, critical manufacturing, dams, commercial facilities

Logical and physical access control

People operating systems controlling these networks - don't have identity

Human aspect

17th sector should be identity

\$50-60B fraud (banking)

Identity: to be structured, disciplined?

How to network challenges, rank and strengthen?

Thesis statement for when you come back here in April? Action. Identity X

Digital Identity is huge. 40-60 sessions. to what goal/end?

EU: legislation supporting SSI

DHS S&P SVIP / CIS

Canada: DIACC (Digital ID & Authentication Council of Canada) - wallet specs

Driver License - Real ID - required to be unique - have to biographically check SSN to make sure have only one driver license

Foundational identity
Functional activity for other things
Federate
Do authentication without creating honeypot
Federated process
Federal advisory council

Wyden's bill to pass? Maybe? Senator from Oregon
Bill to create two-year process with stakeholders to make representatives on how to do identity in the US
Post-NSTIC
The National Strategy for Trusted Identities in Cyberspace (NSTIC)
Federated: still have middleman
Decentralized digital identity is peer-to-peer
Public side
Challenge how to
John Q public?
Policy and privacy guides
10 things need from policy and privacy guys - need to get 4 or 5, can work on the rest
federal advisory council important
only 2 entities that can create it: president, or a department head. DHS sec?
Depends on how and who they want to hand it off to
Solution set we're looking for: policy and privacy bars
Privacy Act is old (1974)
Estonia broke free from Soviet Union; said cryptographic keys are legally binding; then came out with citizen ID
estonia e-resident - for public and privacy interactions
decentralized (but centralized public key infrastructure)
2017 demo
Can sign and encrypt emails

Window of opportunity next 18-20 months opened by facial recognition
Aspect of identity
Need public-private thing
Quality of life: about all of us
Not just national security and public safety (law enforcement, etc)
How can I use who/what I am to open doors
ATM started with the rich
Then had to open it up to everybody, because
Demand signal for identity? every time you pick up a phone or do something

Q about Apple Wallet
Cyber/infrastructure security looking into it
Private industry doesn't have a true governance process
Biometrics identity approach by private industry - even without profit, grown at behest of the corporation wants to do
Support opt-in/opt-out process, doesn't always work

Verifiable Issuer Lists aka: Trust Registries, is the VC legit?

Session Convener: Manu Sborny

Notes-taker(s): Paul Trevithick

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

Manu is developing a new spec for a trust registry (lists issuers and verifiers). I didn't catch where this work is being done. Maybe W3C?

Manu presented a short deck. Link???

Manu started by presenting a survey of prior art:

- EBSI Trusted Issuer registry
- Biometric Passport Chip Protection
- Gaia-X Trust Registry
- eSSIF-UA tRIAN
- Spherity CARO
- ToIP Registry task force

Goals: create a data model that standardizes the common concepts across most of the prior art (80%):

- Assurance Community --> List of Verifiable Issuers or Verifiers <-- Interested Party
- List contains entries of issuers or verifiers

The BEST DID Method (sidetree v2)

Session Convener: Gabe Cohen, Daniel Buchner

Notes-taker(s): Gabe

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

<https://hackmd.io/@nAYABlJeTnuvBbRCb4GRBg/r1rj59Z8j/edit>

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

SSI in Web3 using Magic Link Wallet Self S Identity

Session Convener: no name on session card

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

Enterprise Identity and Interoperability

Session Convener: Kyle Robinson

Notes-taker(s): N/A

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

[\(112\) Greenhouse Gas Mining Pilot Demonstration - Energy & Mines Digital Trust | Government of B.C. - YouTube](#)

[Energy & Mines Digital Trust - Case Studies - Digital Government - Province of British Columbia](#)

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

[EMDT - IIW - Nov 2022.pptx](#)

[https://briartech-my.sharepoint.com/:p:/g/personal/kyle_robinson_briartech_ca/EYT51hXPjhtCijcKcf nawV0BS cCuy9Ccqp f716plAltzLw?rt ime=e06P7HbZ2kg](#)

Privacy Enhancing Mobile Credentials (Listening)

Session Convener: John Wunderlich @PrivacyCDN

Notes-taker(s):

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

Kantara Privacy Enhancing Mobile Credential Work Group

<https://kantara.atlassian.net/wiki/spaces/PEMCP/overview>

PEMC Draft Early Implementors Report (WIP Commenter Access)

<https://docs.google.com/document/d/18gNx9wcE6-8o9K9usv085KCPpWLuPOQjGTekpIICA/edit?usp=sharing>

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

Hyperledger AnonCreds - AnonCreds From A to W3C to ZKP

Session Convener: Stephen Curran, Government of British Columbia

Notes-taker(s): Stephen Curran

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

- Presentation [Slides](#)
- Hyperledger AnonCreds [Project](#) / [Wiki](#)
- Hyperledger AnonCreds Project Announcement [Blog post](#)
- [AnonCreds Specification](#)

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

Topics covered:

- What are AnonCreds?
- Hyperledger AnonCreds
- Ledger-agnostic AnonCreds – using AnonCreds on Indy and any other ledger
- AnonCreds Specification
- AnonCreds in W3C VC Format - [Proof of Concept implementation](#)
- Crypto-Agility – signing a credential using both LD-Signature and AnonCreds signatures

[Hyperledger AnonCreds](#)—short for “Anonymous Credentials”—is a type of VC that adds important privacy-protecting ZKP (zero-knowledge proof) capabilities to the core VC assurances. A core element

of the Hyperledger Indy project for more than five years, AnonCreds is a mature, complete model and interactions set, with extensive support across Hyperledger Aries frameworks.

The creation of the Hyperledger AnonCreds project outside of Indy signifies the continued evolution of an open source software project that was once monolithic and is now a set of well-defined independent components. Hyperledger AnonCreds is ledger-agnostic and client-agnostic. It is not tied to Hyperledger Indy or Aries. This makes it usable with other verifiable data registries/ledgers and verifiable credential client stacks. As a result, important privacy-protecting capabilities become available to a much broader audience, and the underlying cryptography can evolve without affecting the features above it.

Additional benefits of using Hyperledger AnonCreds include:

- Avoidance of identifiers: No correlatable identifiers are required in presenting data to a verifier. Correlatable identifiers may be applied in a use case specific manner.
- Verifier assurances: Credentials are bound to the holder, so verifiers know that credentials presented together were all issued to the holder providing the presentation.
- Minimal data sharing: Data to be shared by a holder to a verifier is minimized through the use of selective disclosure and ZKP predicates
- Flexible formatting: Credentials and presentations can be formatted in the W3C VC Data Model standard format.

IdP Discovery and FedCM

Session Convener: Heather Flanagan

Notes-taker(s): Heather Flanagan

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

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf>

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

Discussion re: the edu use case with thousands of IdPs and tens of thousands of RPs and how they'll need to be considered with in FedCM's account/session chooser use case.

RP gets a list of IdPs from a third-party federation (in the US, that's InCommon). InCommon manages the metadata (a giant blob of XML from a well-known spot). File of metadata is signed by InCommon and is about 90MB. InCommon serves as the point of trust for IdPs and RPs. You identify an endpoint in SAML metadata that's usually formatted as a URI or URL (includes a domain; see "entityID")

Where does the 90MB file get processed? Used to be the RP would load the entire thing, but that doesn't work any more. It's up the RP middleware to parse the XML server-side and boil it down to a JSON file that would feed their own interface (see the Shibboleth Disco Feed). This hasn't been standardized. Right now, the "nicest" method to do IdP discovery is called SeamlessAccess, and it has

nice UI standards for how to find things. It is also protocol agnostic. IdPs have a scope associated with them that's a piece of policy, and InCommon as a cert authority does domain validation to prove control of the domain. If you don't have control of the domain, we aren't going to publish your metadata. The user could type in their email address, and then say chop off everything to the left from the @ sign, but in higher ed that doesn't always work. Colleges and universities may share physical location but have different IdPs, and it's hard for a user to actually guess which email address to use to get access to a specific journal institution tied to the subscription of any one of the schools they are affiliated with. Also, students are more likely to type in their gmail address when asked "type in your email address".

Is there an equivalent to this in OpenID? You can do the exact same thing in OIDC

What parts of this break with third-party cookies? Some discovery components.

There is a proposal to mean it won't 100% break, but the solution will be "crappy" - Third-party cookies will absolutely go away. That's not optional. If you passed 1000 IdPs to the FedCM API, it would pass 1000 http queries to the IdPs; of those 1000 requests, all would fail except the one you logged into. So, if you're logged into one of the universities, it would come back with your logged in institution. Pretty sure that wouldn't scale. If you send a session identifier to every single server, you'd knock the system over. What FedCM is proposing is an extension to the FedCM is that IdPs can push to browsers to say "I have a logged in user". Where does the API endpoint live? It's a browser API (JavaScript or HTTP header). This is a variation of isLoggedIn. This doesn't help the bootstrap problem of that first IdP discovery.

You can still do the IdP discovery without third-party cookies; it's the persistence found in things like SeamlessAccess that become problematic. FedCM adds a level of efficiency in a different area in that the IdP list, if the user has more than IdP then it would have a curated list of choices per user. Would the new login status be useful independent of FedCM, something that would be lighter weight, something that wouldn't require all IdPs to expose info to the IdP.

University of California system does have an extensive front-channel logout and requires force reauthentication. Action: Heather to get contacts in that system to talk and hopefully help test FedCM

The walled garden of policy is what makes academic federation work. The coherent policy framework makes a huge difference.

There are two UX formulations they offer to capture consents - one that has browser UI in the top right of the screen (URL bar); other is autocomplete.

Some consideration as to how to train people on correct behavior.

Much of what happens next comes from how much the higher ed community can help build and test prototypes.

SESSION #5

The TAO of the Trust Spanning Layer KERI/ACDC/CESR/PAC WebofTrust / Zero Trust

Session Convener: Sam Smith

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

Intro to SSI 101 / An IIW 101 Session

Session Convener: Limari N, Kerri L

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

zk-SPARQL

Session Convener: Dan Yamamoto

Notes-taker(s):

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

- Verifiable Credentials
- JSON-LD
- BBS+ signatures
- Zero-knowledge proofs
- SPARQL
- Privacy-preserving
- Slides: <https://speakerdeck.com/yamdan/zk-sparql>

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

- presents a prototype implementation of verifiable and anonymous personal datastore supporting
 - storing JSON-LD based VCs
 - SPARQL-query
 - verifiable and anonymous result (using selective disclosed VP with BBS+ signatures)
- possibly have relationships with DWNs, Solid Pods, ...
- Uses jsonld libraries from Digital Bazaar as well as RDF/JS and SPARQL libraries from RDF/JS communities

NFT's & VCs in iOS & Android with Full Verification

Session Convener: Haydar

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

SSI in (US) Healthcare ?!

Session Convener: Deb Bucci, Stephan Baur
Notes-taker(s): Martina Kolpondinos, Scott Phillips

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:

Definitions

HIE: Health Information Exchange (across networks/providers)

UPI: Universal Patient Identifier



SSI in (US) Healthcare ?!

How can Self-sovereign Identity help an entire sector?

Validating the hypothesis that SSI allows to overcome hard digital identity challenges: We will discuss the problem space and link it to the basic building blocks of SSI in the design space.

The goal: A unifying conceptual architecture that promotes a multi-stakeholder solution path and helps identifying inflection points to the existing course.

SSI poised to solve US Healthcare “Digital Identity Crisis”

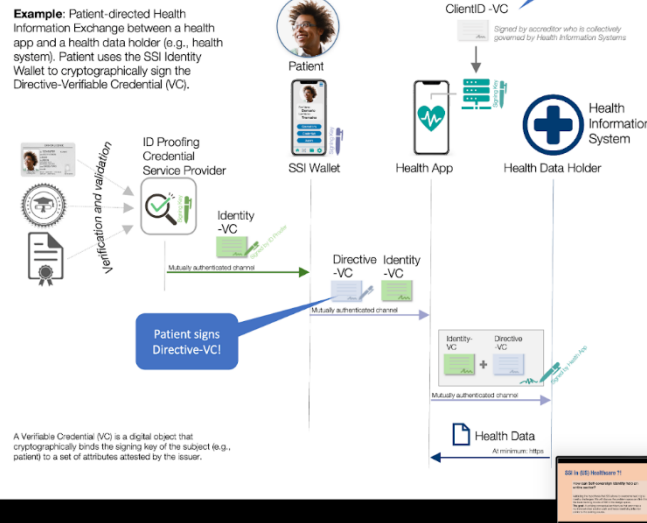
Self-sovereign Identity

SSI introduces a digital identity model in which consumers **own unique identifiers** used in passwordless authentication where identity attributes are conveyed through **verifiable, digital credentials**. With **cryptographic signatures** an individual or entity can let anyone authenticate them and verify their identity claims –privately and directly!

Why it matters: SSI increases digital security, significantly simplifies user experiences, and ensures confidential interactions. Patients can digitally sign directives or authorizations that can be transferred and verified without the need to re-login and click through forms. It creates the benefits of Single-Sign-On without the trackability of Federated Identity.

The big picture: SSI gives patients the needed sovereignty for true patient-centric digital healthcare. For health systems, it massively simplifies the securing of their Health Information exchanges. This form of digitalized counterparty trust accelerates time to value when proving and verifying of identities and their entitlements are required, e.g., in onboarding, credentialing, hiring, drug purchasing, referrals, health status, etc. Zero-Knowledge Cryptography offers a path to a unique patient identifier without the often-cited privacy concerns.

Bottom-line: These strong technology shifts indicate that many current approaches with digital identities for Digital Healthcare can be reimagined. In-progress programs based on centralized digital identities should be seen as short-lived bridges to the new era of Decentralized Digital Identity.



Solving for US Healthcare's Digital Identity Crisis (the same problem eIDAS v2 sets out to solve)

Problem Space

1. Support **patient-directed exchange**—i.e., a Health Information Systems (HIS) or health app requests patient data from a Data Holder (DH) as directed by the patient without patient interacting with DH. DH must have a way to validate directive.
2. **Find patients' data** that is scattered over a multitude of HISes, without a universal patient identifier.
3. Desire for **“Single-Sign-On” to the entire SECTOR** (system) without being trackable by 3rd parties:
 - a. A patient must be able to access every HIS **portal** with the same authenticator (username/password and/or passwordless).
 - b. A patient must be able to use a health app to **access FHIR APIs** using same authenticator as in 7.a.
 - c. The system must have a way to tell the patient **which FHIR APIs have data about them**
4. Offer patients **“Meaningful Choice”** (aka, fine-grained consent to Selective Disclosure of their individual PHI/PHI).

Vision → Design Space

- SSI building blocks:
1. DIDs, DID documents with listings of service endpoints
 2. ID Wallets, agents
 3. Verifiable Credentials binding subject-DID to identity claims attested by an issuer-DID, with anonymized proofs to prevent tracking
 4. DIDComm messaging and connections

SSI gaps:

1. Wallet interoper
2. Holder-issued VCs (or DIDComm message?)
 - a. Cannot be signed by pairwise DIDs
3. VC schema standards, availability, version control

Others:

- PODs, DWNs
- SIOPv2, OIDC4VP
- Smart contract based Registries, Directories, Indexes
- Trust Registries
- VDR

Summary

- A more precise problem statement should be provided to further discuss and lead to a clearer reasoning of proposals.
- A voice of the healthcare consumer has been cited which serves as a good way to describe the problem: *“one of my friends is immunocompromised. Friend hops among various specialists - the biggest blocker is getting different providers to share that data.”*
- Additional clarity should be provided why the lack of ecosystem-wide, coherent identity management is at the root for the challenges in health information exchange. This will make it easier to envision Self-sovereign IDENTITY as a strong path to a solution.
- It is important to understand that there will remain corner cases where it is inevitable to use “patient matching” based on demographic data.

- Source of verifiable credential for identity (as well as client-id for health apps) is critical. For consumers, this may come from the financial services industry to allow for portability of verifiable identity data (PII). For health apps, a form of an accreditor governed and trusted by health systems (the data holders –PHI). Root of trust should be further explored.
- Continuation of the topic is encouraged.

Notes

- Stefan objective: not another reference architecture, but how to grow the conversation outside of the SSI community circles
- Debbie will describe the US healthcare context:
 - Coordinator of clinical data at the NIH
 - Problem is - one patient may have many providers. How do you aggregate all that data?
 - We are trying to share that information across networks
 - A patient has the individual right to access their own data
- Stefan: the topic is about patient-centric data exchange. SSI in Healthcare also applies to other areas, such as clinician credentialing.
- Stefan slide *SSI poised to solve US Healthcare Digital Identity Crisis*
 - This is a proposed idea, not the implemented system.
 - What is the goal here? How do we make this HIPAA compliant?
 - Flow: Patient has SSI-wallet, gets identity VC from somewhere (only once), uses it to onboard to a health app, issues a directive VC (cryptographically verifiable statement by the patient about what data shall be shared from which provider to which receiving provider).
- You cannot just "have an app" that interacts with patient data, since you have to KYC your app user
- Patient-directed and patient-mediated data exchange differ: the latter moves data to an app used by the patient with the challenge how the app proves provenance of the health records.
- Network called "Avenir"? that shares the data
- Tony: one of my friends is immunocompromised. Friend hops among various specialists - the biggest blocker is getting different providers to share that data.
- Deb: there is a movement called "trusted exchange" where all members of a network share data.
 - The patient would be able to query the network to get all their data across providers
 - Is there a secure way that the patient can manage their data?
- Issue different SSI ids, one per provider, and make the patient manage it
 - What about universal patient identifier? HHS Department is not allowed to put one together.
- Deb has done work around patient-matching, and there is a real amount of false positives
- UK has a "kai number", which is supposed to be singular. If you are unconscious, they just assign you a new one.
 - You can't avoid the matching problem.
- Scott: What about designing for the less digitally native individuals? How do we make it inclusive for them?
- Ethan: Within this context, you need to have
 - Real clarity on what problem you are trying to solve?
 - As people who work in tech space, we find it easy to talk about tech. "We have a technology, we need a problem to solve". We should ask "what is the problem? Now how can we solve it?"
 - Technology moves *much* faster than public policy. Policy needs to move with, or perhaps ahead of technology in this space.
 - This has to come from

Goal proposals

1. No information flow (HIE) without patient consent
2. Control of HIE () is not with the hospital
3. Enable any licensed provider to access data without interference (hospital, bureaucracy, etc)

- We need to enable delegation, a fact that New York missed in their 2007 work.
 - Power of attorney, etc.
- Ethan: who is the issuer of the first credential? Do we have a root issuer registry? (Credential Service Provider, not an Identity Provider)
- Selective disclosure needs to be unpacked in this context - I will tell you the surgeries I have had, but not the medications I am on.
 - Public health, yes. Clinical Health, no.
- The token is a verifiable credential that authorizes me to access specific records.
- The identity is the ownership of the wallet, not the access to the records
- Think about authorization tokens instead of SSI
- Difference between HIPAA and non-HIPAA data isn't accessibility, it's *accountability*
- The problem of insurance is a uniquely American problem.
- The problem with patient-mediated is that all providers provide verifiable credentials. It's not in the provider's best interest to do so.

Signing In The Rain: HTTP Message Signatures

Session Convener: Justin Richer

Notes-taker(s): Justin Richer

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

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

We discussed the background and status of the HTTP Message Signatures draft specification in the IETF:

<https://datatracker.ietf.org/doc/draft-ietf-httpbis-message-signatures/>

<https://www.ietf.org/archive/id/draft-ietf-httpbis-message-signatures-14.html>

We also ran through live demonstrations in the HTTP Message Signature playground website:

<https://httpsig.org/>

Credential Profile Comparison *started at last IIW!

Session Convener: Dr. Andre Kudra, Dr. Torsten Lodderstedt, Paul Bastian

Notes-taker(s): Dr. Andre Kudra, Paul Bastian

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

Presentation

<https://docs.google.com/presentation/d/1odg79ZPSZfryTzlTP6R1oePN7jO4iU0the0UUViYfzk>

Credential Comparison Matrix:

<https://docs.google.com/spreadsheets/d/1Z4cYfjbbE-rABcfC-xab8miocKLomivYMUFIbOh9BVo/>

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

Credential Profile Comparison - A joint effort by the global community of experts

We looked into What, Why, How of the project of creating a Credential Profile Comparison Matrix and the accompanying Guiding Paper, milestones already achieved in 2022, insights gained, overview on 6 categories and 50 criteria derived to assess credential profiles, wrapping up with next steps to finalize the work by Q1/2023

Trust Establishment for Machine Readable Governance

Session Convener: Mike Ebert

Notes-taker(s): Mike Ebert

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

Slides: <https://docs.google.com/presentation/d/1hd-4uKEPv7cbf8kveOJAQtmH9H6m7dq7/edit?usp=sharing&oid=112759837137305414950&rtopof=true&sd=true>

DIF Working Group, Work Item:

https://github.com/decentralized-identity/claims-credentials/blob/main/work_items/trust_establishment.md

<https://github.com/decentralized-identity/trust-establishment/issues>

Calendar: [dif-calendar](#) (DIF Claims and Credentials Working Group meets weekly: Monday 10am PT)

Video Demo: <https://www.youtube.com/watch?v=8DUf7U4aKj4>

You can try the editor yourself:

- Visit <https://codesandbox.io/s/github/Indicio-tech/governance-editor> to create a governance file and save it to your hard drive.

- Visit <https://jsfiddle.net/eldersonar/flst0ekh/280/> to upload the governance file, customize the functions to ask new questions, and see the results.

For more information, go here:

<https://github.com/Indicio-tech/governance-editor>

<https://indicio.tech/governance-editor>

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

How do you know which issuers you can trust?

Build a list, sign it, and publish it!

Once you build a list of trusted issuers, what else can you do?

List schemas, create roles, and link schemas and DIDs to the roles (and thus to each other)

Are there future extensions of this functionality?

Beyond issuance, you could add other roles—verification roles, API roles, storage roles...

Indicio has done work with role-based workflows (so that the workflows or processes in written or human-readable governance can be followed and verified by the software as well). Hopefully we can add optional workflows to the governance file/trust list work that is being done.

Finally, DIF work will be merged with ToIP work in a joint effort soon. Waiting on a memorandum of understanding to be signed and then joint meetings to be scheduled.

OIDC Web to App Flow Challenges and Solutions

Session Convener: Leon Tian

Notes-taker(s):

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

Mobile web to mobile app flow:

Question: Is there a way to return to the same browser and same tab?

- If the user does not start from a default browser
 - Redirected to the default browser
 - Current solution: Detect browser type, and if not the same, message user to go back to the original browser
- If the user starts from the default browser
 - Redirected to a new tab
 - Current solution: Browser scope to be set “Browser wide” so that the new tab will have the session details.

- Alternatively, use the similar flow as “Desktop web to mobile app” flow(in the next page), ie. The popup(modal) page on top of the RP app will keep polling the status and return the control back to the RP app. On the IDP side, ask the user to click “Back” button to go back to the RP app.

Desktop web to mobile app

QR code is used to transition the user to mobile app

Current solution does provide flexibility for RP to decide on which device to continue UX afterwards

- Redirect to RP on both mobile and desktop
 - Auth code is passed to RP on the mobile device only - IDP does not need to differentiate “mobile web to app” and “desktop web to app” flows and always redirect the user back to RP on the mobile device
 - On the desktop, redirect back to RP web app on the same browser tab
 - RP can decide which device to continue the user flow
- Alternatively, the mobile IDP app does not redirect the user to the RP app, and the user will only use the desktop side redirect to continue the user journey with the RP app on the desktop side. This is more intuitive as all other mobile authenticators flow.

Privacy Enhancing Mobile Credentials (authoring)

Session Convener: John Wunderlich

Notes-taker(s): Heather Flanagan

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

<https://kantara.atlassian.net/wiki/spaces/PEMCP/overview>

PEMC Draft Early Implementors Report (WIP Commenter Access)

https://docs.google.com/document/d/18gNx9wcE6-8o9K9usv085KCPpWLuPOQjGTekpII_cA/edit?usp=sharing

<https://insights.som.yale.edu/insights/what-happens-when-billion-identities-are-digitized>

Consent receipts: <https://kantarainitiative.org/download/7902/>

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

“Acceptable/appropriate friction” not perhaps the right concept for a privacy paper. It is a design consideration, not a privacy consideration. The goal is meaningful consideration; friction is a side-effect. But there can’t be an over-dependence on consent either. But, consideration still might be better than friction. Friction makes you slow down and be thoughtful, but that might not be the only way to make you slow down and be thoughtful.

Reach out to marginalized communities to make sure that privacy-enhancing meets their needs as well.

Encouraging conscious decision making is another way to phrase what “friction” is doing.

Cognitive overload is another form of privacy abuse. That’s friction in the wrong direction.

The next order of how you solve the problem is the “reasonable friction” idea. But there are steps passed that. In the longer term, how do you do that at the protocol level? All RPs are registered, and there is vetting for all RPs on all use cases (see the Aadhaar system). That may not be achievable in all markets and in a cross-border interoperable way, but it’s an interesting model to consider as a gold standard. There is a proto-example of this with SAML entity categories that have the ability to structure attribute released based on the type of entity (e.g., research org) asking for the data.

What about data sharing receipts? If you get a receipt linked to the verifier, that could be evaluated by a court of law. Kantara published a consent receipt specification.

Can a FIDO Authenticator be used for Payment confirmation

Session Convener: Francisco Corella

Notes-taker(s): Charles E. Lehner

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

WebAuthN, Authentication, Secure payment confirmation, Web workers, Tracking, Merchants, FIDO, Signatures, PWAs

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

[notes below about discussion following the presentation]

Calling WebAuthN from web worker

...

WebAuthN signs hash of client data containing challenge

Relying party has to have entire/most of response to verify

Can't ask merchant to validate? Do they need to?

Sending FIDO response to merchant violating security - creating tracking vector across websites?

But credit card reuse...

Merchant knows who user is, credit card number

[16:36]

Q: Challenge signed by bank.com should only be processed by bank.com - core security property of FIDO - supercookie

SPC (secure payment confirmation): to try to get around restrictions

can use in other context then 3D secure

Is there a solution... can the merchant demonstrate in court that the account holder signed the confirmation?

Bank makes credential, stores transaction and large blob object - certificate of credential id, key - that merchant can trace back to bank
can extract large blob from key, including certificate... could validate

How can the merchant easily validate the response.

Not easy with WebAuthN?

Authenticator data: one element, JSON data: break up into several elements, one of which is the challenge

Take the elements other than the challenge, and say that these are part of the signature, together with the other ECDSA components

extended signature for FIDO use

Send to merchant challenge and signature these with (opaque) pieces

Give the merchant a function that verifies it

Merchant doesn't understand how it works...

Authenticate on merchant sid without phoning home to bank

Bank provides website, at least the webauthn component, as a website (PWA - progressive web app) - service worker - with single key - the user's FIDO key

Processing the FIDO response

page generated by service worker

Redirect

As bank, issue a PWA to do FIDO offline for user, serve as PWA that merchant can redirect to. Does that solve the problem?

Difficulty validating a FIDO signature

Windows only doing RSA

FIDO server, but not authenticator

Merchant to do validation

has to verify signature on confirmation of transaction

Progressive access...

Key in PWA not valuable?

Sharing FIDO response directly a problem. Platform would block as misuse

PWA can validate.

Merchant

Never going to happen - to change platform?

Proposal to take things as they are (not changing spec)

Software somebody provides takes existing response, breaks up, extract the challenge to replace with data transaction

together with "r" and "s" signature components

as extended signature

merchant takes that, (a, b, c, r, s) to verify

What is being validated?

Signature of concatenation of two hashes (authenticator data and client data)



Limari @Limarikal · Nov 16

...

It was a great opening day at my first ever Internet Identity Workshop where I also got a chance to present an Introduction to Self-Sovereign Identity alongside Kerri Lemoie, PhD. Looking forward to day two! [#iiw](#) [#decentralizedidentity](#) [#ssi](#)



Notes Day 2 / Wednesday Nov 16 / Sessions 6 - 10

SESSION #6

Hello - Fasten Health, hello.coop

Session Convener: Dick Hardt, [Hello.Coop](#) : [Jason Kulatunga](#), Fasten Health
Notes-taker(s): Chris Heuer

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

#Healthcare #MedicalRecords #HealthData #humancentric

Register your interest in getting involved with Jason here:

<https://docs.google.com/forms/d/e/1FAIpQLSd5EK-P0NqYqAazZaX0w2rUG2t7GIyNOw-I-cjKI4lC3pfcuw/viewform>

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

Jason Kulatunga, founder of Fasten Heath shared his personal journey through the medical system to resolve a simple issue, which was ridiculously complicated to solve. He had to interact with 7 health care providers to even get to understand he had a chronic issue.

Basically, the balkanization of the health data landscape.

HIPPA doesn't apply once you've shared your health data with a 3rd party! Did not know that.

Posted on Reddit "self-hosted". The post was very popular.

The post on Reddit is here

https://www.reddit.com/r/selfhosted/comments/xj9rx7/introducing_fasten_a_selfhosted_personal/

Dick Hardt demonstrated how Hello.coop can more easily manage the aggregation of that data in a secure method, for the different situations required in managing our health care records.

How is the encryption key managed?

- Dick explained this at the 12min mark of the recording/transcript

Jason did a demo in a sandbox of how the app/service works. (min mark 13ish)

- Demo accounts/data imported from Medicare.com, Epic, and Care Evolution
- Interesting approach to only decrypting and accessing the health data, only when the user is present - so will not automatically refresh and store their data without their express consent and action.
- Great discussion on underlying decisions in approach/architecture and how the medical records are handled securely.
- If there is a breach in his architecture, there is no real exposure for the user's data.
- "Break the glass" user story... ????

~~Web3, SSI, Web 5~~

Session Convener: Timothy Ruff

Notes-taker(s): Eric Scouten

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

Based on Timothy's Medium article <https://rufftimo.medium.com/zero-trust-web5-and-gleifs-vlei-63ffcb800028>

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

SSI is a second-class citizen / afterthought in Web3, behind cryptocurrency, smart contracts, defi, blockchain, NFTs, DAOs, etc.

Premise: SSI community should dissociate itself from Web3. Web3 is a dumpster fire and tainted in public perception. SSI is far more important and should stand alone.

<https://web3isgoinggreat.com>

TR: "I am not a believer in DAOs." (Hmmm. Why?)

Counterpoint / credit to Web3: Blockchain blew the doors off of status quo thinking. Got general public to stop being scared of deeply technical things. Wallets. Appreciation for open-source. Led to experiments in governance (DAOs).

TR: "VCs are going to impact every technical interaction. Your phone call will not ring unless the signature of the caller checks out."

TR: Re: Web3 things (see list at top of page). "My crystal ball says these things will not achieve ubiquity. They will not get much bigger than they are now."

TR: "What's the incentive of the Internet? There is no incentive." But the internet is huge anyway. Internet *enables* applications that provide value and thus have incentives.

New law in US: Financial Data Transparency Act. Every entity must have a globally unique non-proprietary identifier. Sounds very much like GLEIF.

Most in room (~80%) are at least somewhat persuaded by this argument.

Ooh, now Timothy moves on to challenge the term SSI.

~40% of people in the room have experienced "allergic reactions" to the term SSI. Why? Opinions around the room:

- Sounds libertarian
- It's a mouthful
- Sovereign implies nation-state imperialism

- Tax evasion
- Doesn't apply to enterprise
- Language is too fancy
- Implied association to blockchain

Sovereignty isn't total. Data could be lost. Identity could be revoked (by who?). Identity could expire.

KERI uses AIDs, not DIDs to avoid the idea that you're renting an identity. Your DID is typically tied to the lifetime of the ID resolving.

Read up on AIDs vs DIDs.

TR: "I am passionate about the *goals* of SSI, but I believe the *term* SSI is getting in our way." There are reasons why Microsoft, Salesforce, etc, are avoiding using the term SSI.

The term "self-sovereign" alienates big corps.

TR: Discusses and then dismisses the term "decentralized identity" as an alternative.

"Decentralized identity" is also conflated with Web3. Don't use it for that reason. Let Web3 have the terms SSI and decentralized identity.

Call it Web 5. Follow Jack Dorsey's lead. Why?

Dorsey's language intentionally distances from Web3. Use Web-something to create distance from Web3. (Some in audience dispute that it actually has that effect. Others says it's presumptive to say it's the new web.)

TR: There's no perfect term. Dorsey has already launched it. Web5 doesn't have built-in meaning, which is actually a benefit.

Audience asks so what IS Web5?

TR defines "web 5" as "autonomous control of authentic data and relationships."

TR: I see lots of problems with all of the potential names. I just see fewer problems with Web5 as compared to SSI and decentralized identity.

Holder Binding and Wallet Authentication

Session Convener: Paul Bastian

Notes-taker(s): Joshua Coffey

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

Link to the slides: <https://nextcloud.idunion.org/s/XB9LMWqbAamHx76>

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

- Lots of people focus on VDR and relationship between issuer and verifier
- Trust relationship to holder / wallet is mostly overlooked so far
- Verifier wants to ensure that credential has not been tampered with or transferred
- How can we ensure security of holder wallet?

- Found there wasn't much distinction between what credentials actually mean ("Evidence credentials" vs "Identity Credentials")\
- Evidence credentials don't need much security; identity credentials need a lot of security
 - Evidence credentials: gym membership, event tickets, etc
 - Identity Credentials: drivers license, diploma, etc.
- SSI ecosystems bring use cases from different domains together
- Attestations make statements about individuals, but can't make claims about who is showing the credential
 - You need an identity credential to bind attestations with the presenter

- To improve things, first think about your wallet security infrastructure
 - Extreme one: everything on your phone, all keys and crypto local, etc
 - Extreme two: Everything on cloud, phone is just window
 - Middle ground exists
 - We focus on mobile solution where everything happens locally
- Mobile device market is heavily fragmented
 - This makes it difficult to build solutions
- Tradeoff between market share and security
 - Secure Elements have low market share but high security
 - Software solutions have huge market share but lowest security
 - Apple Secure Enclave and Google Strongbox are good middle grounds
- Many hardware solutions cannot be directly interfaced with to use effectively
 - Secure Elements are very locked down and provide a minimal API
- Nobody has really jumped on Google Strongbox
 - We have to wait to see where it goes

- Three main pillars necessary for wallet security for mobile native apps:
 - Device Binding
 - Hardware-bound keys; you can make sure that your credential is not extracted from your wallet
 - Holder binding / auth of holder
 - PIN, Biometrics
 - Wallet authentication

- Ensure wallet software has not been tampered with by holder
 - Issuer and verifier need assurance that holder binding has occurred without holder (or others) messing with it
- Device Binding Solution
 - Love to use Zero Knowledge Proofs, but status quo is that there is no hardware support for these yet
 - Only real option ATM is elliptic curves
 - Well-understood, accepted by regulators
 - No backup / recovery strategy possible
 - Adds a unique, trackable attribute in the form of a device's public key
 - One key for each claim helps, but compared to BBS+ or ZKP is still trackable
 - Can maybe resolve this by having one-time credentials, but this has obvious drawbacks
- Holder binding solution
 - Pretty straightforward; two-factor of some kind, biometrics, PIN, etc.
 - NIST says biometrics on mobile phones is not yet sufficient for regulated use cases
 - Fingerprint sensors are easily hackable or spoofable
 - Not as resistant to presentation attacks as one would hope
 - Only thing that gets close to being accepted is Face ID, but issues still remain
 - Regulated use cases demand one stick to PINs and Passwords
 - Where is the PIN actually stored?
 - Must be in hardware, but this gets complicated because Google and Apple hide information about it, so you can't determine the strength of the PIN stored in hardware to attest to the strength of holder binding
 - Android SafetyNet and iOS Device Check help increase trust in holder binding
 - Key attestations prove keys actually came from trusted hardware
 - Only available in Android, but iOS ecosystem is more secure / safer so maybe this is okay
 - Question: Android safetynet already has key attestation, why use them separately?
 - Doesn't tell you anything about whether a specific public key is actually stored in hardware
 - Only attests general security of device(?)
 - Cannot reuse safetynet key for other purposes --different things are being attested
 - Key attestation says "Key X is indeed coming from real hardware"
 - SafetyNet attests that wallet app truly comes from developer; doesn't tell you about other kinds of keys
 - Safetynet tells you what developer signature of the app is + general security health
- Tested out solution in Germany in 2021
 - Implemented device binding and wallet auth
 - Issued 20k creds within 2 days
 - Halted due to massive overload and missing concepts for trusted verifiers
 - Mediators were unscalable; wallet security concepts weren't actually the problem
 - Used proprietary solutions, not standardized

- It only makes sense to do wallet authenticity checks at issuance
 - Doing it at verification brings too much load to SafetyNet; Apple and Google don't like it
- DIF Wallet
 - DIDComm flow
 - Verifies wallet is secure and holder is who they say they are
 - Holder attests security capability of wallet and issuer makes decision based on such
 - Wallet goes to attestation service to perform attestation
 - Helps hide complexity from issuer
 - Issuer must not check different attestation formats of different mechanisms we have as it's too complex
 - Attestation service issues attestation VC to holder; holder presents attestation VC to issuer to verify attestation
 - Issuer then issues actual VC to Holder, linking to attestation VC in some way
 - Verifier then asks for both VC and Attestation VC, and verifies they are both linked together
 - Question: who operates attestation service?
 - Can be backend service for wallet software
 - Could be an external regulated/qualified trust service
 - Vendor of wallet and attestation service don't have to be same entity
 - Wallet provider invokes attestation, they must have some level of control over process
 - SafetyNet is being deprecated but is being replaced with new service that works just the same
 - OID4CI flow
 - Very similar to DIDComm flow
 - In DIDComm flow, issuer asks for attestation; in OID4CI flow, wallet has to know to fetch attestation ahead of time
 - Open question as to who should trigger attestation
 - In issuance request, we place a Verifiable Presentation of wallet attestation
 - Speaker has no strong opinion on preference for which flow
- Trust Registry is necessary for ecosystem because we need a list of trusted Attestation Services and wallet providers
- Attestation Service could revoke device attestation VC if vulnerability is found in certain phones/hardware elements/etc
 - This is why it is valuable to have the attestation VC stored in the wallet alongside the identity VC, as opposed to just storing the attested public key from the attestation VC in the identity VC
 - Attestation Service could just inform issuer to revoke identity VC
- Issuer might want to know, from the attestation VC, what kind of biometry is used to protect wallet
 - This is another reason to have full Attestation VC in holder wallet
 - Wallet itself is going to have to do its own authentication because mobile app providers conceal too much about auth from apps
 - Minimum security bar must be met on device level AND app level
- Question: How do we verify the verifiers are trusted? Why are we only talking about trusting the holder?
 - This is where trust registries come in

- Apps have to be aware of and care about trust registries
 - If we have an authenticated wallet, issuers can ensure that they only issue to wallets which properly respect trust registries / trusted verifiers
- Question: Should Google and Apple come together to create a shared API to solve these problems?
 - Sure, that'd be great
 - Government is a skeptical of Google and Apple wallets; they want to build their own wallets
 - Many of these capabilities need to become OS-level, but we need to protect against vendor capture
 - If multiple wallets all meet the issuer requirements, they should be on the same playing field --even if not made by Apple or Google
- Regulators view biometry as less secure than PINs
 - We can't just do whatever we want; if we want to solve problems that governments are interested in, we need to work with them on this
 - Biometrics are not magic

Architecting Enterprise Cloud Agents to interact with Third-party Policy Engines

Session Convener: Jacob Siebach

Notes-taker(s): Jacob Siebach

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

Authorization

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

How does an enterprise organization utilize a third-party policy engine for it's authorization requests when, in an SSI ecosystem, it may not own all of the data necessary to evaluate the authorization policies?

The discussion involved lots of talk about existing infrastructure, and how it will be difficult many existing organization to transition infrastructure to use SSI components. Some things mentioned were Red Hat Key Cloak and constructing policies in such a way that an OAuth server can get the data requested.

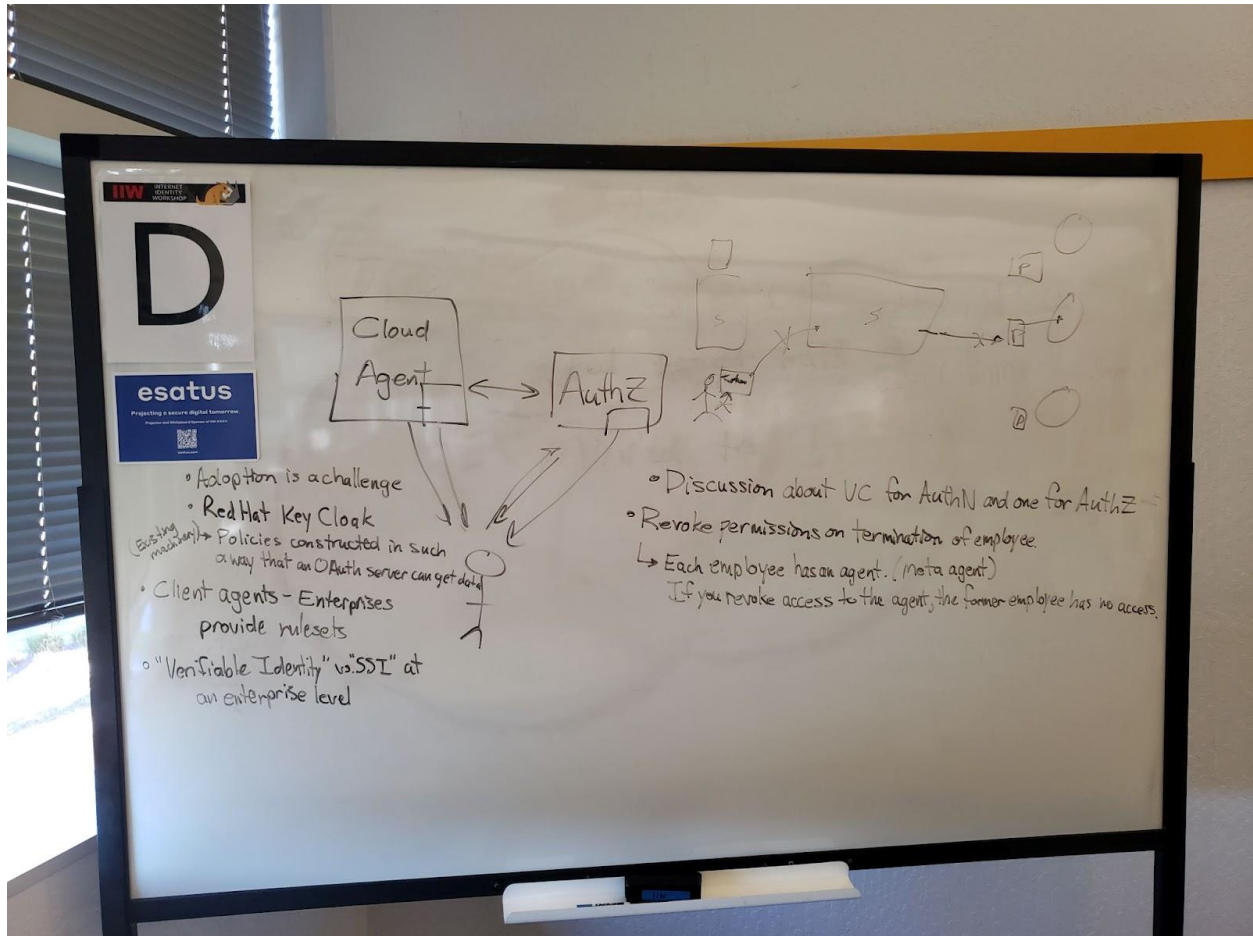
SSI-ENABLED SYSTEMS

For systems that can utilize SSI, one option is to provide separate VCs for AuthN and AuthZ purposes. Also, by giving the user an entry agent that then connects to another internal system, all that needs to happen for deprovisioning is to remove the authorization for the user at the entry agent and then they can't get into any other systems.

Additionally, instead of calling it “SSI” in an enterprise system (which implies that the user owns the data), we should call it “Verifiable Identity” (since the enterprise owns the employee data: employment status, administrative rights, etc.).

CLIENT AGENTS

Chris (from MITRE) suggested that in the future, organizations would provide policy rules as a selling point as users could download and install rulesets in their own agents.



"Why aren't we at Afrotech?" Identity and DEI

Session Convener: Morgan Fykes

Notes-taker(s): Jessica Tacka

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

Diversity Equity and Inclusion (DEI)

20,000+ people in Austin at Afrotech at the same time as IIW, and a lot of IIW attendees aren't aware of it. How do we bridge that gap?

Why we are interested in this session group intro:

Everyone is welcome vs "come join us" are two different statements

Diversity helps us build better - UX

Hard being a minority representative in working groups

Existing in a space as only white woman in a room, often all white people

Here to learn

FOMO for missing out on Afrotech - DEI advocate

If something isn't working, the people for whom it's meant to work should be involved

Made a promise to be part of any DEI session at tech conferences

Diversity of thought, role, and identity - need all the voices. Even a .01% failure is critical. Can't build systems for the best of us. They have to be for all of us.

Diverse teams produce better products. Only opportunity to avoid potential harms that are incredibly difficult to fix post-release.

Third culture kid speaks to diversity and the desire to be included. We're all kin. Authentic marketing and how we speak to the right people, their values, and what they care about.

Afrotech was created in 2016 and 20,000+ people are in Austin right now. Identity has a lot of layers, so if we're going to have a conversation about it, it goes even deeper than double-booking important conferences. It starts with a conversation.

How do we move this forward?

- having common tools - privacy tools, DAOs, standardization created by diverse teams. Counterpoint: where are the diverse people setting the standards?
- Conversely we don't know how many people at Afrotech know about this workshop
- What is mutual discover of groups?
- Onboarding and access - materials, platforms, timezones
- How do we make sure we're offering something they want to work on?
- WE TALK ABOUT THIS BADLY
- Definition of identity - an identity is how we recognize, remember, and respond to specific people and things
- Dark effects of identity - car won't start because you didn't pay your rent
- Infinite identities online and they might not be related to we we are and who our experience is
- Reinvention and forgiveness as identity

Is there already an topical overlap between IIW and Afrotech?

- There is a web3 section this year for Afrotech

- Suggest IIW sponsors Afrotech next year
- Wherever that conference is, pull up
- Some of the solutions IIW wants are at Afrotech and vice versa
- Even if we connect virtually

If Morgan were to be an ambassador for IIW to Afrotech next year, what would support look like?

- Money makes the world go round
- Take the right people to them

DEI in tech vs DEI in sub-categories

Three part series on identity called Planet work

@digitalsista

-Naming the harms of web2

-Mitigating the harms of web3

Start with a virtual event. Worries about cultural competency coming from historically privileged individuals. (Getting comfortable being uncomfortable)

Tip: person of privilege ask "what did I do wrong?" if they trigger

- Create a space where people can be wrong

A lot comes down to who the facilitator is.

Surveys for before and after assessing anticipated fears or worries and then what actually happened.

Afrotech was started by Blavity, a Black media company, as a holistic space for technology. Also as a response to the question "where are the Black people in tech?" At Afrotech there are more Black people talented people than you can imagine.

More appropriate approach is the "who" of showing up might fall more towards to the .orgs vs the IIW which is more of a trade association.

Groups will have a code of conduct for what kind of space this is. Is anyone welcome, etc.

Never ask a question if you're not able to accept no for an answer.

Can of worms - as we're writing specs, to be at the table you have to pay membership to be part of the group. (Understandably for IP, etc). Gatekeeping - how do we lower the gates?

- Charter includes seats that are open for particular voices.
- Seats for "diverse people" should instead be named for the problem. The specific folks who are historically excluded.
- Credentials community groups are a free way in.
- Decentralized Identity Foundation (DIF) memberships start at zero
- Time is a barrier to entry

Where OID4VC fits in the ToIP Stack

Session Convener: Torsten L, Drummond R

Notes-taker(s): Mathieu Glaude

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

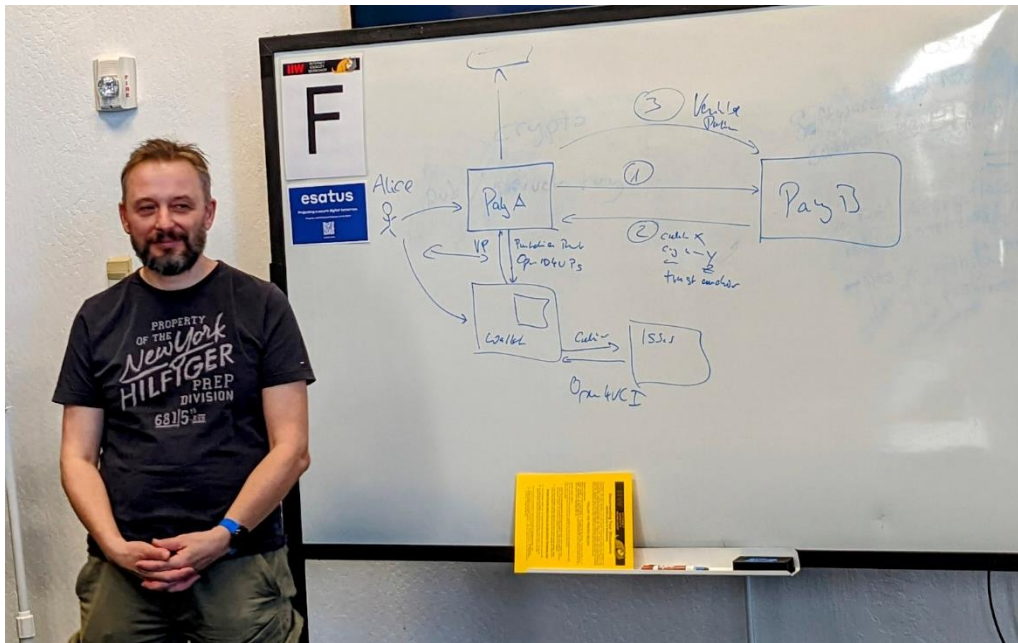
How would GAIN fit into the ToIP Architecture?

- In parallel to the reference architecture development, worked on instantiation on how GAIN and OPENID can benefits those building on ToIP architecture

About TOIP

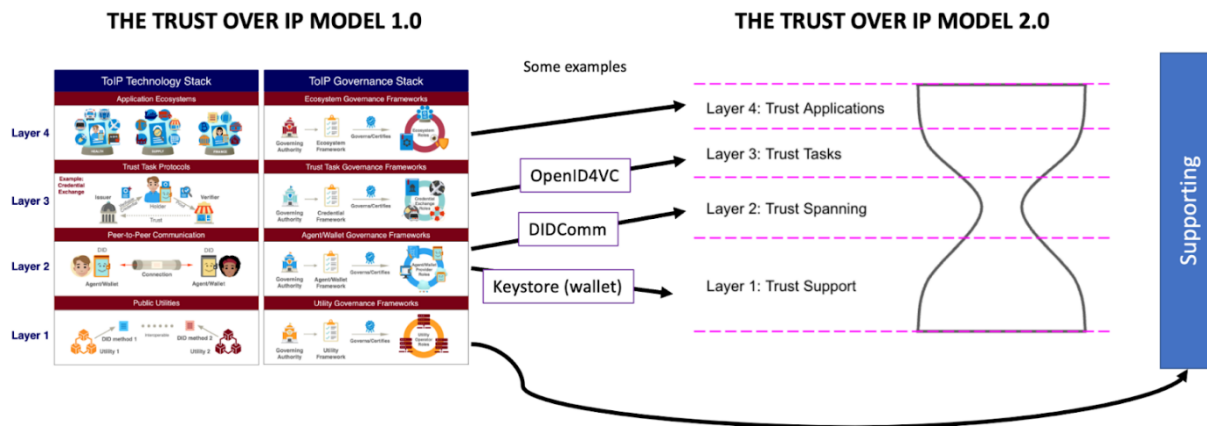
- Specifies architecture that allows entities to communicate with each other. Note: there is a new architecture proposed (ToIP-Technical-Architecture-Specification-V1.0-PR1-2022-11-14) which uses an hourglass model, similar to the hourglass model used on the Internet with IP
- They use the Trust Spanning Protocol to communicate (e.g., DIDComm is a strong candidate)
- There are 16 out of 30 requirements across the stack on Layer 2 (TSP)
- The TSP needs to be a general purpose protocol

Key question: How can Entity B trust Entity A?



- How can Party B authenticate or authorize Party A.
- To solve the problem, party A & B need **credentials** so that they can establish trust in that architecture
- The ToIP reference architecture has a support system on layer 3 that can help with the above
- When party A communicates with Party B, Party B asks for eligibility (challenge)
- Option: Party A (app running on behalf of user) could use OpenID4VP to obtain presentation of credential which is later used to authenticate and authorize cred

- Party Specifies that they want a credential of type x, crypto sig y, crypto format z
- If user has suitable cred/requirements in their wallet, the wallet creates presentation minted for Party B
- This is like HTTPS, when trying to access resource you get challenged
- This separates the wallet from agent/user where all credentials of user resides
- If user lacks credential required, in the same flow they can reach out to issuer using OpenID4VCI
- The new proposed ToIP architecture makes it clearer to see how something like OIDC4VC can fit in on layer 3



Interop Status - 17 issuers + 8 wallets!!! / CHAPI + VC

Session Convener: Manu
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

user agents, given a pico

Session Convener: Bruce Conrad

Notes-taker(s): Bruce Conrad

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

Slide deck at <https://bruceatbyu.com/s/IIWXXXV>

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

During the session, we gave control of four picos to each person. These picos are hosted by the Manifold application, run by Pico Labs. Each pico represents something: the owner (with contact information), their manifold, and their things.

Some questions asked and answered during this session:

- What is a pico?

A very tiny virtual computer. A personal computer in the cloud. They are insanely cheap (an EC2 instance costing less than \$10 per month could host tens of thousands of them).

- What is Manifold?

A web application which hosts picos for their *owners*. Once logged in to Manifold, you can add *things*, each of which is represented by a pico.

- What is “Safe and Mine”?

An application that is installed in every thing (as represented by a pico). It allows you to specify a message that you want someone who finds your thing to see. You also register a QR code, a tag, and then affix that tag to your thing. [thanks to Joyce Searls for the name]

- What is manifold_cloud_agent?

An application that can be installed in a thing. Once installed, your thing is now an Aries agent, capable of DIDComm v1 connections with other Aries agents.

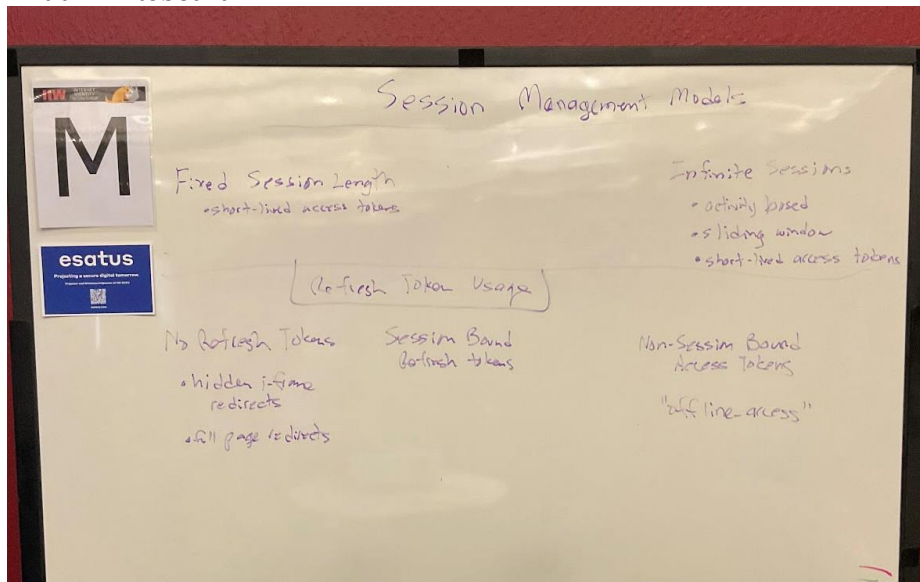
Session Management Models

Session Convener: Vittorio Bertocci, George Fletcher

Notes-taker(s): Heather Flanagan

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

Initial whiteboard



You have non-session bound refresh tokens, that allows “offline access”

You also have session-bound refresh tokens (no way to say this in the spec)

You also have no refresh tokens at all; can do session management this way with hidden iFrames and full-page redirects but it's ugly from a UX

Session bound refresh tokens need to be specified. It has been done at different companies, but it's ad hoc.

Suggestion is to add a scope to allow this behavior.

Diving into being super tactical:

- SPA allowed tokens via implicit flow, and refresh tokens with iFrames to hit back on the authZ server (but that required cookies). The outcome is that implicit flow was a bad security idea and cookies are going away, needed to move towards code flow in an SPA.
- Complication: the original OAuth spec does not provide an affordance of the client to ask for a refresh token. The authZ server decides whether to give a refresh token. OIDC introduced an affordance for refresh tokens (a refresh token that's independent of your session supporting offline access).
- When people are supporting an SPA and they want to use the flows, they ask for a refresh token to support offline access because it's the only way to get that token. That means the app is responsible for deleting that token and they have to make a call to disable that token. Everyone does that differently, and they may not do it at all.
- During the implicit flow, whenever we have an iFrame, they touch the IdP session, so if the IdP session has “sliding” cookies, we poked it and added new life to it.

- A refresh token endpoint has an entirely different threat model to the authorization endpoint.
- It would be good if there is an online-access scope that tells the authorization endpoint to create a token tied to the session. Step two would be if we find a way to tell the authZ server to allow the refresh token to extend the life of the IdP session.

The IdP would know the app logged out because the app sends a message to the IdP.

We're trying to preserve the ability for instant logout.

How often do you have to come back to get an access token? That should be configurable for your environment.

Is the session lifetime bound to the refresh token life time? Yes. The refresh token's time should be set to the IdPs session? Yes, but if you have a sliding/infinite session timeframe, you probably want to have a different lifetime for the refresh token. If the refresh token times out it may turn into an SSO moment where the RP will re-query the IdP and find out that the IdP still considers the session active, and then there will be a new refresh token.

There are times where, at hyper scale, keeping track of sessions is not ideal.

A single IdP session could be bound to multiple refresh tokens? The term session becomes overloaded in this scenario.

- [whiteboard image that won't make any sense; needed to be a video]

This could be a polling mechanism, but it doesn't have to be. All the infrastructure is here, and the application already needs to be able to use refresh tokens. So, if you decide you want this to be a mechanism to see if the session is still active, you can do that. But it also offers the freedom to only use it when you need it. If the UX requires you know in advance, then fixed frequency will help. But if you don't need that, you don't have to use that. Note that polling the IdP is actually terrible for the IdP itself.

For logout, Backchannel logout will still be an option, but it's not ideal. It's a best effort approach, often requires quite a few holes in a firewall, and may be dependent on memory.

If you only have one RP, then you can use CNAME tricks to make logout work (though Apple might block that move as well)

Why was this rejected a few years ago? Offline access was considered a bad idea that OIDC shouldn't have done, and doing an online access would just double down on that bad idea. Back then, there were options so this wasn't too big a deal, but today with browser changes and an increase of workforce IAM where distributed logout is even more critical, it might be worth pushing again. More specific reasons this was rejected:

- authorization server should decide if you get a refresh token; the client shouldn't ask for it
- Another thing to consider, within the scope of OIDC in general, access to an access token does not mean logged in, don't conflate the two. Mobile app and what logged in means is really fuzzy in other spaces, which complicates matters. The idea behind offline access meaning refresh token is partially the user is not logged in any more but I need access to that API (unrelated to authentication). Unclear if the session management needs to be tied to the refresh token.
 - Need to be more clear as to what it means to log in. This should reduce what actually happens today.

Different tokens that have their own timelines

- IdP session
- RP session
- IDT (ID Token) Lifetime
- AT (Access Token) Lifetime
- RT (Refresh Token) Lifetime - might outlive other tokens, is the longstanding artifact

Untangling the timelines of the above is complicated

CCG - What is it and what are we doing?

Session Convener: Harrison Tang - Kimberly Wilson Linson

Notes-taker(s): Kimberly Wilson Linson

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

[Mission | W3C Credentials Community Group \(w3c-ccg.github.io\)](https://w3c-ccg.github.io)

Email: public-credentials-request@w3.org [undefined:public-credentials-request@w3.org] to subscribe to the mailing list.

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

The CCG is a community organization made up of anyone interested in the credential and identity space. We welcome all members of this community to join in education, discussion and work items so that we can help to inform the work conducted by the W3C working groups.

We meet on Tuesdays at Noon Eastern

SESSION #7

Intro to the Mee Project

Session Convener: Paul Trevithick

Notes-taker(s):

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

Paul presented this deck:

https://docs.google.com/presentation/d/1xV9A3HT6zx5cQekseDs61_ZDndV0bT6stHdp8WkpqYs/edit#slide=id.g11fe743ad95_0_2

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

Lots of lively discussion about the Mee project.

Discussion included a philosophical aside about whoness, selfness and Hume's notion of structure vs. bundle.

Mind the GNAP

Session Convener: Justin Richer

Notes-taker(s): Dean Saxe

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

<https://www.ietf.org/archive/id/draft-ietf-gnap-core-protocol-11.html>

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

- delegation protocol similar to OAuth
 - built on similar mechanisms as oauth
- Justin and team looked at OAuth + OAuth like things + UMA + extensions to OAuth to drive thinking about GNAP
- There is no plan for wire compatibility with OAuth with GNAP
 - it is NOT OAuth 3
- What does the room want to hear?
 - What does "delegation" mean in GNAP? Is GNAP allowing a user to delegate access to another?

- GNAP allows delegation from a resource owner to a client instance
- In GNAP the end user is a separate entity
- The end user is the user using the client instance, they are usually the resource owner
- GNAP does NOT cover any way to connect the end user and resource owner together - there is no definition of how you set up that policy/mechanism
- talking about the RA and end user as separate entities gives flexibility in the protocol
- GNAP enables use cases where the right of authority comes from both the resource owner (RO) and End User
 - but the delegation is *outside* the scope of GNAP
 - OAuth2 covers a single user case
- In the cases where RO and end user collapse to a single person, it is supported directly by the protocol
- in GNAP every single request starts the same way
- Adrian Gropper - The lack of connection between the RO and end user is essential in our health use cases
- GNAP is not delegation between users - it's between person and software
- Section 1.6 of the spec - async authZ diagram on the screen
 - from a protocol perspective GNAP presents a menu of options
 - client says "this is what I can do, this is what I want"
 - authZ server says "this is what I can do and will allow"
 - there's a dynamic negotiation/conversation happening
 - Client requests access from the AS
 - AS responds with a wait message
 - the AS can map the client request to who can authorize the request
 - the client polls the AS until access is granted (or denied)
 - Note that the client is saying it has no idea how to contact the RO
 - the AS instead does this on behalf of the client while the client waits
 - the AS can decide what is the best approach for contacting the resource owner
- Can the client host the AS? Or is it typically hosted elsewhere?
 - Justin - these are roles in the system fulfilled by some software, so they can all run on the same service
- This is a protocol for effectively generating a limited scope API key in response to a request
- GNAP separates the AS, RO, RS, etc as roles
 - the AS knows about people, processes, policies and how to generate an access token
 - the RS has to know how to understand the access token and what is being communicated
 - GNAP does not specify how the AS and RS are tied together
 - there's another draft addressing this mechanism, it is not in the core doc
- CIBA Example
 - call center example
 - end user and RO are different
 - as a call center agent you need to access information about someone else in the system
 - client instance makes request to AS "this is my current user, client software, and user the client wants data about"

- the driving use case here is a user in a call center receives a call
 - user asks to view a set of info on the caller
 - caller gets a push notification on the app requesting access
 - caller approves
 - the interactive approval via a trusted channel allows the call center user to see the customer's data
- In the protocol the client asks for something at AS with a four part request in a JSON doc
 - First section: API Access
 - grant requests have a rich set of data that can be requested that is defined by the AS
 - second section: Info about the client
 - client send name, URI, and key information
 - Third section of the request says how the AS can interact with the client for starting and finishing the interactions
 - multiple starting mechanisms
 - one, and only one, finish mechanism
 - fourth section: subject info
- Response from the AS for a redirect flow
 - two part response in JSON
 - interact - tell the client to go to a URL with a nonce
 - continue - here's a URL and access token to call the URL
 - the token is presented signed by the client key
 - this ensures that only the client is able to call the AS as a part of this request
- in GNAP the client is stupid - all the intelligence in the system is within the AS
- message binding
 - in the grant request the client send a pub key to identify itself
 - that same key is used by the client to create an HTTP message signature
 - the sig headers are added to the top of the grant request
 - this allows the AS to pull out the key to verify the sig on the message
 - this ensures message integrity, the method and target URI have not been manipulated, etc.
 - the AS is then clear that the client made the request
 - HTTP Message sig is not the only mechanism, JOSE could be used as well
 - similar message binding is used for the RS, as well
 - unless you opt out and get a bearer token to talk to a RS
- finish message allows the client to tell the AS that the interactions have been completed

How can we build provably trusted products?

Session Convener: [Johannes Ernst](#), [Dazzle](#)

Notes-taker(s): Joshua Coffey,

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

- Speaker motivation:
 - Building something called Dazzle, which is...
 - Why don't we get *all* data about you and put it into one product, a "data palace"?
 - This is only going to happen if the user has extremely high confidence they won't get screwed by this product
 - If we say "we won't be evil", we won't inherently be trusted.
 - We want to do more than just SAY we're trustworthy; we want to demonstrate it provably.
 - Apple promises security but their phones are a black box.
 - The only "proof" is the strength of their brand.
 - We have no evidence Apple actually implemented things correctly
- Definition of a "Trustable Product"
 - A technology product that doesn't:
 - Do anything I'd disapprove of if I knew it did it
 - Do anything I'd disapprove of if I actually understood the consequences of what it did
 - This is really important – people don't understand enough about technology to even know what to approve or disapprove of
 - Counter-example: a weather app that sends location info to some extremist political faction that harasses people with whom they disagree
- Definition of a "Provably Trustable Product"
 - A product that I can be (quite) certain is trustable
 - Based on more than just promises
 - Evidence must be provided
 - Example: open-source software you compile yourself
 - You *can* review the source code yourself to determine if it is trustworthy
 - Even software you compile yourself can hide things from you that you can't find, but this is a step
 - Counter-example: multi-million dollar marketing spend on "Privacy is important to us"
 - This proves nothing
- Analysis
 - First question: does product work as intended by people who built it?
 - If it works as intended, it might do good or bad things
 - If it only intends to do good things, it's trustworthy
 - If it does some bad things, these things can be overtly or covertly done
 - If overtly done, the challenge is in communicating properly to the user what is done and the consequences
 - If covertly done, the challenge is in breaking into the product / reverse-engineering to determine what it does
 - If it doesn't work as intended,

- There could be any number of unknown issues – and it may or may not do bad things.
 - It may be trustworthy.
 - There could be known issues which may or may not be serious
 - Bold-faced font instead of italic isn't a big deal, doesn't impact trustworthiness
 - Privacy leaks are a big deal, make it untrustworthy
 - How do we reduce the ways a product can end up untrustworthy?
 - Open source code
 - External audits
 - etc.
- There are things beyond open-source that can prove trustworthiness
 - Proof of Storage
- Question: Why would you say that overtly-bad things (where users are fully aware) is untrusted? I trust it to do exactly what it says.
 - Because a trustworthy product wouldn't do something I'd disapprove of *if I understood the consequences fully*.
 - It's open in one sense, but the consequences might not be openly understood
- Platforms can assist products in proving certain things
 - Browsers can indicate that a product provably never communicates in certain ways
 - Best regime we have for this is in publicly-traded companies
 - Financial statements are reasonably reliable (barring Enron)
 - When you install apps, it's common to ask for permissions for camera, storage, etc.
 - Something that could be more useful for this problem is to make things more fine-grained
 - "I only talk on the internet at certain points in app lifecycle / only for X purposes" would be very useful assertions if provable and testable
 - Would prevent covert wrongdoing
 - Self Assertions + External Testability
 - Developer characterizes what app does, and someone externally tests this
 - We should try to move towards a culture of security where people can prove and be trusted what their *intentions* are.
 - This is really hard to do, and has to be done for every single app update
- Length of time that something is on the internet makes a big difference
 - Most domains (90%) only exist for a few hours
 - Long-lived domains have a vested interest in their reputation
 - It's very unlikely for someone to build up a positive reputation and then turn around and be suddenly malicious
- What if a developer could assert "my app never does X and alert me if it does"
 - Inversion of asking for permissions
 - Doesn't address the issue of fine-grained control
 - You can ask for permission to use a camera, but you can't ask for permission for a specific purpose
 - It's hard to control what a resource or permission is used *for*
 - Most apps need to access the internet. An "internet access" permission is useless. How do we provide finer-grained control?
- How do we build a culture / system / platform where people have observability into what is happening inside a product, *in a way they can understand the consequences of it?*

- The app store provides a certain level of trust – supposedly, Apple’s screening prevents malicious software
 - Only provides certain levels of protection.
 - Do I trust Apple? Should I have to?
 - What if a government demands that Apple rescind certain protections for certain apps?
 - Perfect security isn’t possible, but it’s a useful addition / marker.
- If there were a curated list of best practices in a particular field, apps could say they’re compliant with those best practices
 - Chat apps could get together and determine the best practices for chat apps
 - It’d narrow the scope of verification of assertions of trustworthiness
 - This could easily become subject to regulatory capture
 - What if all the chat apps agree that tracking location is a great, justified, fantastic thing that chat apps should do?
 - Group needs to be diverse to avoid any one interest group taking over
- How do we make it easier to figure out the implications of something an app does?
 - There’s a good reason for Zoom or a QR code scanner to use a camera
- What if we bring in experts to assess what an app does and determines if the things it’s doing are justified or not?
 - We’re kicking the trust can down the road
 - “We have a model for that; it’s the Underwriters Laboratory”
- What if the repercussions for breaking a pledge of trustworthiness are so huge that nobody would ever do it?
 - “If I break these rules, my company is liquidated”
 - Put up a bond
 - If you hire a plumber you don’t know and who doesn’t have a large customer review base, you trust them because they’ve essentially put up a bond when they got licensed.
 - What if we did a smart contract where the community could vote to punish a company somehow for violating a pledge?
 - Who gets how much voting power?
- What about an “Ethical Bug Bounty”?
 - Companies would incentivize people to submit “ethical bugs” for reward
- If we don’t publicly commit to the right trust model from the get-go, the market opportunity will be 1/10th of what it could be
- Is there a place for these discussions in the market? Can this make sense?
 - “The only reason we have best practices is because there’s no protocol”
 - Where would be a logical place to have this conversation?
 - Probably not a traditional standards committee or a non-profit
- Why not have this entire process be handled by the law?
 - This is an extremely difficult problem to define in the law
 - Convincing a government to adopt a policy or process which has not been proved out is near impossible
 - The law is concerned with punitive measures, but maybe the solution lies in alternative incentive structures which guide behavior outside of punishment
 - Law is an MVP of a sort
 - Companies which truly exceed and demonstrate excellence do so by meeting a standard which far exceeds the law
- We should define a term for this concept (“... Product/Software/Technology”)
 - Provable
 - Trustable
 - Certified
 - Audited

- Integrity
- Safe
- Worthy
- High-assurance
- Benevolent

Follow-up:

- Mailing list to continue discussion: <https://groups.io/g/trustworthy>.
If you are reading this as part of the IIW notes, even if you did not attend the session, feel free to sign up.
- Survey on what to call this:
<https://apps.dazzlelabs.net/nextcloud/index.php/apps/forms/FRAeJXNKgBWtiKIS>
Feel free to vote.

Verifiable Credentials - Ask Me Anything

Session Convener: Brent Zundel

Notes-taker(s): lol, lmao

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

<https://www.w3.org/groups/wg/vc>

<https://www.w3.org/2022/06/verifiable-credentials-wg-charter.html>

<https://w3c.github.io/vc-data-model/>

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

Good chat about the current state of the work at the VCWG on v2 of the VC Data Model.

Q&A session where technical responses to deep questions were explored, and all the dirt was dished.

Secure SSI with QR Code. Why QR Code is not safe.

Session Convener: Abbie

Notes-taker(s):

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

held a great session on how to secure QR code. OASIS ESAT secure QR code standard was reviewed. Uses cases discussed and reviewed. Excellent feedback from the audience and interest for future enhancement. OASIS IDTrust was also introduced and why it is a good place for doing you SSI work is explained



Real World Deployment



Trusona in 30 seconds

<https://www.trusona.com/videos/trusonas-no-passwords-experience-in-30-seconds>



Passwordless MFA for Roaming Users, Hot Desks and Kiosks

<https://vimeo.com/530933203>

Secure QR Code Authentication Version 1.0

OASIS Standard

04 October 2022

This stage:

<https://docs.oasis-open.org/esat/sqrap/v1.0/os/sqrap-v1.0-os.docx> (Authoritative)

<https://docs.oasis-open.org/esat/sqrap/v1.0/os/sqrap-v1.0-os.html>

<https://docs.oasis-open.org/esat/sqrap/v1.0/os/sqrap-v1.0-os.pdf>

Previous stage:

<https://docs.oasis-open.org/esat/sqrap/v1.0/cs01/sqrap-v1.0-cs01.docx> (Authoritative)

<https://docs.oasis-open.org/esat/sqrap/v1.0/cs01/sqrap-v1.0-cs01.html>

<https://docs.oasis-open.org/esat/sqrap/v1.0/cs01/sqrap-v1.0-cs01.pdf>

Latest stage:

<https://docs.oasis-open.org/esat/sqrap/v1.0/sqrap-v1.0.docx> (Authoritative)

<https://docs.oasis-open.org/esat/sqrap/v1.0/sqrap-v1.0.html>

<https://docs.oasis-open.org/esat/sqrap/v1.0/sqrap-v1.0.pdf>

Technical Committee:

OASIS Electronic Secure Authentication (ESAT) TC

--

mDL <> VC - Can we all get along?

Session Convener: Kaliya Young (in-person), Lucy Yang (virtually)

Notes-taker(s):

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

[VC <> mDL Community Project IIW Session](#)

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

Tech Bill of Rights

Session Convener: Jessica Tacka

Notes-taker(s): Nicole Roy

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

Substack for the Tech Bill of Rights: <https://techbillofrights.substack.com/>

Socio-authority as morality/criminality - Important tenet for a bill of rights.

Related to the right to be forgotten/forgiven: The right to be alone. What do you do when your information lives on someone else's cloud. The digital home that some can afford but some can't. Admission to people with consent versus being observed. Something to be self-sovereign of. Discussed this in yesterday's Mastodon protocols session.

US Bill of Rights - fourth amendment. People feeling that their fourth amendment rights have been violated due to the whole FISA stuff and web 1 and web 2. Unreasonable search and seizure.

Winning the narrative. Narratives of the founding fathers were from a specific space of privilege. We have adapted these principles to become compatible with modern life. Women can vote, non-land-owners can vote. We're not done fixing it.

Lack of cultural agency and cultural influence.

Notional first 1-10 demands in a bill of rights:

Postal service came out of a requirement to be able to communicate.

Is the context of this a US-centric thing or global thing? Want it to be global.

This stands on its own, it does not need government backing, it is self-evidentially the right thing to do.

UN Sustainable Development Goals - framework, but they're very weak on communication and privacy.

Clean slate laws

"We Demand The Right:"

- To privacy of our information
 - (Name the private attributes like location, etc.)
- To digital self-determination
- To freedom from prosecution on the basis of attributes of our humanity
- To universal access to an appropriate global baseline of technology necessary to participate in civic and social demands
- NEW WORDS and CONCEPTS for NEW WORLDS (fiduciary versus agent versus what???)
- To be here - to be visible and to have visibility into the human process of technological advancement
- To be respected as peers
- To have representation in decisionmaking that affects our existence in the world
- To repair the things we depend on in our lives
- To have technology which enables access across the full spectrum of abilities and capabilities

***Discussion with Carlos and Michael as the session excited - the right to have visibility of and access to all of your data.

It's not perfect, but at least it's a step forward?

Session Convener: Bryan Jin

Notes-taker(s):

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

Bridging the gap between the ideal technological advancement and how the technology can be made more tangible. Pursuing the perfect, ideological solution may not ever emerge, or it may be too distant for end users to agree with its value. What good does a great technological solution do, if the end users don't buy into it? From the engineering perspective, SSI & DID model of credential presentation and verification makes perfect sense; however, does it relate to end users and businesses to have them adopt it?

In order to switch over to the "Web 3.0", perhaps it should not be about presenting the greatness of the technology, but presenting the tangible, relatable benefits to the service providers and end users instead.

Super simplified example: So what if we aren't creating complete, perfect technological solutions to replace the existing (perhaps analogue) models? If using a mobile credential for ID verification results in still using a driver's license to manually match you to the mobile credential, is it a pointless solution? It could still be meaningful in a sense that you can significantly prevent the use of fake ID, offloading the verification load and risk (compared to using a central server-based digital verification), etc. Take smaller steps towards the goal, and bring meaningful results (however small they may be).

Trust Registries vs. Machine Readable Governance / @darrello + @telegramSam - Re-Match_LD

Session Convener: Darrell O'Donnel / Sam Curren

Notes-taker(s): Sam Curren

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

<https://wiki.trustoverip.org/display/HOME/ToIP+Trust+Registry+Protocol+Specification>
<https://identity.foundation/trust-establishment/>

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

Trust Over IP Trust Registry Task Force and the DIF Trust Establishment work item (of the Claims and Credentials Working Group) have decided to work together given the large overlap in concepts applied to ecosystem governance. An MOU is being pursued for this purpose, and regular calls will be scheduled between the orgs, with a joint work item as the goal of this combined group.

Everyone interested is encouraged to join this conversation as the meetings are scheduled.

The main goal is to help verifiers understand which issuers they should trust for which types of credentials, and which verifiers should be trustworthy for holders during presentations of credentials.

The main disagreement prior had been the requirement to have / not have an API present to answer queries, as opposed to the downloadable file for local processing approach.

The Trust L1st concepts presented in a different session yesterday also overlap. There have been conversations between these communities as well, but efforts will be first applied to the DIF/TOIP alignment with anticipated future involvement of the larger community.

Self Sovereign Chat with OpenChat

Session Convener: [Kyle Peacock](#)

Notes-taker(s): Kyle Peacock

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

[Open Chat](#) - chat app

[Open Chat Source Code](#)

[Internet Identity](#) - identity provider

[Internet Identity Specification](#)

Other social media

<https://dscvr.one/> - reddit-style forum

<https://distrikt.app/> - twitter-style microblog

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

We discussed how anonymous cryptographic identities can be generated and used to give users ownership of their own user data and content, and how that architecture works in practice with Open Chat.

We gave a live demo, and had several attendees sign up and join the IIW 2020 chat group



Client Discovery / Automatic Registration in OAuth2

Session Convener: Tobias Looker, Mike Jones and Kristina Yasuda

Notes-taker(s): -

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

Link to slides: [Client Discovery IIW](#)

https://docs.google.com/presentation/d/1Map6ff6itga23dZ7vcrsdnVSuUUuCpzZpdd9t0joDEM/edit#slide=id.g193a836c0b7_0_30

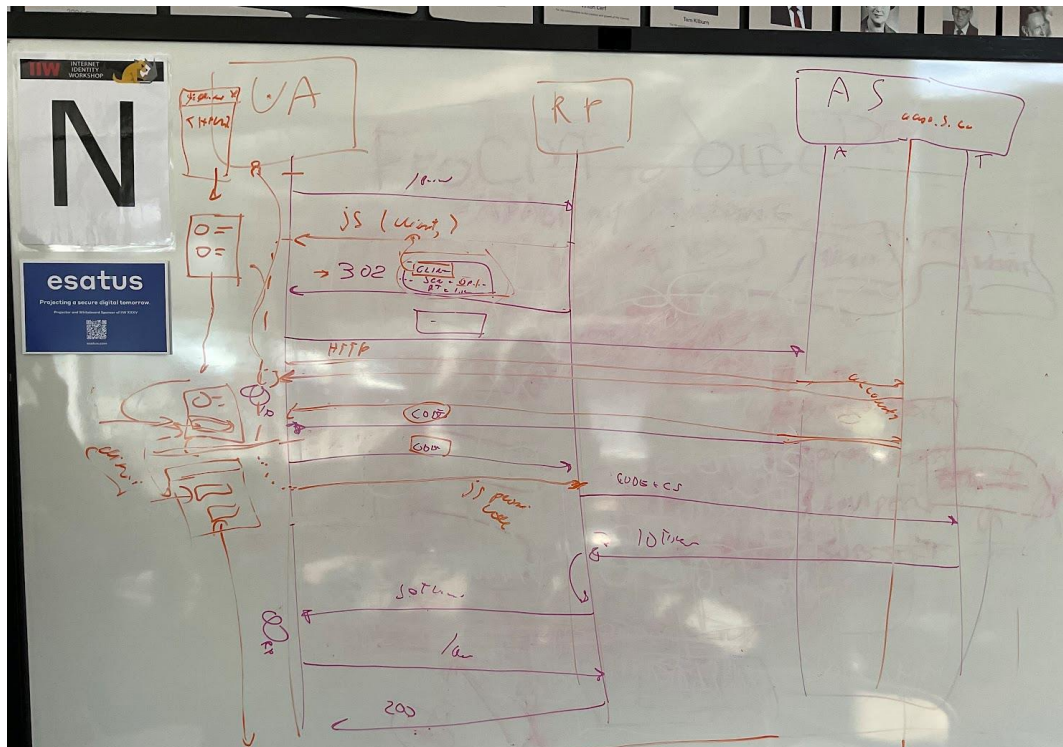
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Mapping FedCM to OIDC Capabilities

Session Convener: Heather Flanagan

Notes-taker(s): Heather Flanagan

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



Will create two sequence diagrams, showing OIDC login and then showing where FedCM overlaps

FedCM makes a trade off between exclusivity and control (there is less control). The login session described in the diagram is purely login; we need to be able to destroy the cookie in logout, and that might be where we're hoping FedCM might help or be called or something.

One concern is that since the user will want a consistent look and feel; while FedCM might not be needed in every scenario, we want the same UX.

FedCM: One option (considered less than ideal because all the RPs would have to change, and there are more RPs than IdPs) if you could change all the RPs so they use JavaScript instead of sending a 302 HTTP call and send a subset of current info. The JS constructs a permission prompt in the form of an account chooser. Right now, FedCM doesn't deal with scopes or selective disclosure.

If you are unable to provide scopes, the code won't actually be the same. The line to the authorization server requires the scope. If you get back a code from FedCM, it wouldn't represent the same thing that they currently get back from the authorization server. Scopes aren't just filters to attributes. They are messages to authorization servers that can have many outcomes.

As result of this exercise, there is an intersection only in the first part of the flow shown, and in the logout. FedCM will be less expressive. If you don't want to use top-level redirects, you should be able to use a JavaScript call instead.

Consent dialogues are going to double; the AS consent may have more detailed requirements as per regulation than the consent being asked by the browser.

The FedCM overlay does assume you're already authenticated and have active sessions. If there isn't an active session, there should be a URL to log into an IdP.

FedCM seems to be most concerned about the IdP and logging in, but the RPs are more interested in other things because what's most important is what happens after authentication; if the RPs have to change infrastructure just for authentication, that's a harder sell.

One gap is that depending on where you're going at the RP, there may be different security requirements (e.g., different authentication context). Maybe this can be handled by a code coming back from the Authorization Server that requires re-authentication. The first cookie let's you find out there's a session; after the browser collects all the authentication it needs, all shields are lowered. The entirety of what else is in the initial request gets added after the browser consent flow. FedCM is asking for consent before they actually have an active session. Think of it perhaps as registering the IdP session with the browser, setting up their account chooser.

There is an infrastructural sign in with an entity, regardless of where you want to go. User will have to register on every browser instance.

Concern about the enterprise scenario where the identity of the IdP is determined by the RP. Signing into Workday from Okta is an example of this. It's a significant number of RPs that are using OIDC, but not a significant number of global OIDC accounts.

The RP can provide a list of authorized Authorization Servers in the JS call. If the clientID changes from one session to the next for the same user (effectively a different IdP each time) this will result in a bootstrap problem every time.

FedCM isn't making OIDC requests; it will contain some of the information in an OIDC flow. What semantics is the IdP using if not OIDC?

We need a third endpoint in the Authorization Server side (e.g., account.google.com)

The code that's listed might not be the same between OIDC and the JavaScript. In order to get the code needed for the Authorization Server, might need a new ceremony.

There will be enough infrastructure work on the Authorization side that we may need to consider incentives. It's also not a great UX because of the multiple prompts. But it will allow for things like front-channel logout, and is a ceremony-based account user that will future-proof you against further bounce tracking mitigations.

Some concern that this will look to a user like a phishing attack.

SESSION #8

Human Rights Protocol Considerations in IETF GNAP

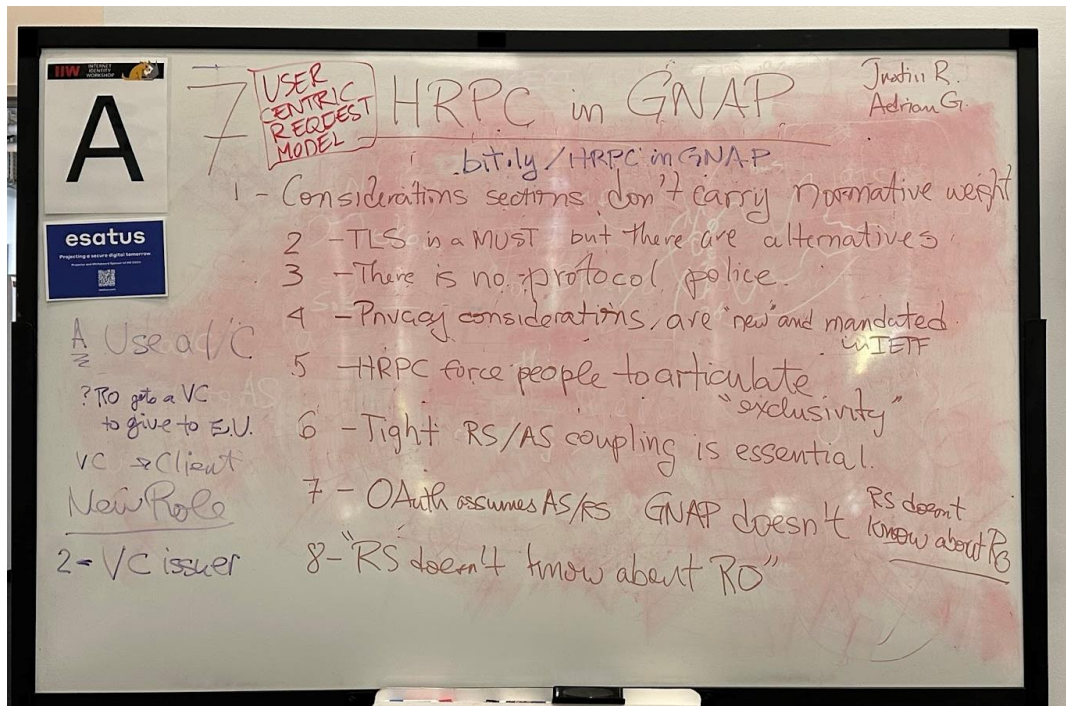
Session Convener: Adrian Gropper and Justin Richer

Notes-taker(s):

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

<https://bit.ly/IETFinGNAP>

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



Outcome:

- AK and JR came to an understanding of the solution
- AK will work with AG to improve the User-Centric Request Model accordingly
 - https://docs.google.com/document/d/1gH1HVvOpJqLkg8BBbDCWh9SclDnJnztvd7x_YVVhtsw/edit
 - <https://hackmd.io/zjYaHjMFRTGtIEIUdzCLnA?view>
- JR will help AG rewrite the GNAP [Human Rights Protocol Considerations PR](#)
- The discussion will continue on the IETF HRPC hrpc@irtf.org and IETF GNAP txauth@ietf.org lists

FIDO Alliance + Wallets

Session Convener: Tim Capalli

Notes-taker(s):

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

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

NO NOTES SUBMITTED

Identity & Payments: Where we are and where to go.

Session Convener: Tony Lopreiato

Notes-taker(s): Leon Tian

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

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion:

Mastercard is working on creating an interoperable ID network, which separate from payment network.

We'd like to have a general solution for ID network - not a Mastercard priority solution

Current challenge: Linking Identity to Payment across the payments Ecosystem

Card payment (tokenized or not) 5-7 seconds

Issuer check identity during (KYC). At the time of payment transaction, there's no link to the original KYC'd card holder. This could result in fraudulent transactions - friendly fraud included. No good way to tie identity to the person.

What's been done today to overcome the challenges:

Proximity (in -person) payment

Chip & Pin

Biometric Authentication in device wallet (emulated chip)

Address Verification (Zip code)

Online payment

Merchant authentication

CVC/CVV

Address Verification

Question about tokenization:

Tony explains how tokenization works.

Card on file token can be domain specific (merchant)

Wallet token can change, no difference for in store and e-commerce uses, except that there's a channel type.

Certain token can only be used in In-app payment

Discussion: where to integrate identity & Payments

Get identity information added to payments message

ISO : Currently limited fields, could be long haul to add new ones

EMV Co

Proximity Payments

ID card Program

Chip integration

Adding identity onto the card

Biometric Payments, Tencent in China. Amazon One Wholefoods

QR code Payments

Online Payments

Merchant - based solution

Wallet-based Payments. mDL and payment put together? Tying together identity and payment

Age restricted Purchase : online alcohol purchase. How to check identity

Buy Online Pick up in Store

Buy Now Pay Later

Linkage to payments service (e.g. Disputes, Click to Pay 3DS, AVS, tokenization)

Question about possible business model changes to digital payment companies, e.g. Block after identity and payment integrate.

Answer:

This will evolve. These digital payment companies do identity protection today. But they'll look to integration with digital identity (e.g. mDL)

Between Acquiring bank and merchant lies the opportunity to link ID to payment. Block has a lot of expertise having terminal, email etc.

ID Network is analogous but separate from payment network. Different identity products. Tony explained ID Network e.g. working with Optus - 2nd biggest MNO to create reusable identity and use at other RPs.

Question about Finicity Open banking

Answer: IDV - income verification offered by Finicity.

DID Method Battle Royale

Session Convener: [Nick Reynolds](#)

Notes-taker(s): [Italo Borssatto](#), [Ankur Banerjee](#)

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

1. [DID Method Rubric from W3C](https://www.w3.org/TR/did-rubric/) <https://www.w3.org/TR/did-rubric/>

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

| DID Method | CRUD operation cost | Implicit | Permanence | History | Programmability of DID controllers (out of 1.0) | Pros/Cons | Persistence |
|---------------|---------------------|----------|------------|---------|---|---|--|
| web | Free | No | No | No | 0.8 | Human Readable, Discoverable, base tech is widely used | DNS |
| key | No support | Yes | Yes | - | 0 | Versatile, Simple, Constrained | Trustless |
| pkh | No support | Yes | Yes | - | 0 | User base, Simple, Constrained | Trustless |
| ethr | \$1 - \$.04 | Yes | Yes | Yes | .5? - 1 | Upgradable, Versioning, Complex-resolver, Meta transactions | Ethereum, API services like Infura / Alchemy |
| Ion / element | \$0.0001 (batch) | Maybe | Maybe | Yes | .2* | Discoverable, Pre-rotation | Ethereum, Bitcoin, IPFS (Sidetree) |

| | | | | | | | |
|--------------|-------------|---------------|-------|-----|----------------------------|---|---------------------------------|
| 3 | Free-ish | Deterministic | Maybe | Yes | .5* | Ceramic Ecosystem | IPFS |
| ens | \$4 / \$100 | No | No | Yes | 1 | Human Readable, Discoverable | Ethereum / ENS |
| iden3 | \$.001 | No | Yes | ? | .5* | Selective and private disclosure (zkp) | ZKP + EVM |
| keri | Free-ish | Yes | Yes | Yes | .8 (M of N threshold, ...) | Not globally discoverable, pre-rotation | Trustless / Watchers, Witnesses |
| cheqd | \$0.0005 | No | Yes | Yes | .8 (M of N threshold, ...) | On-ledger DID resources, AnonCreds without Indy | Cosmos SDK |
| ipid | Free? | No | No | - | .8 | | IPFS |
| peer | ? | Yes | Yes | - | 0 | Implicit service endpoint | Trustless |

Writing Blue Checks that your profile can't cash - Authenticity Damage

Session Convener: Chris Kelly

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

X Licensing & Collaborative Creating for ‘Mutual Benefit’ using WEB V Tools!

Session Convener: Jonny S

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

CHAPI + FedCM: Wallet > selection

Session Convener: DMitri Z, Manu S, Sam Goto

Notes-taker(s):

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

Write up created here: <https://github.com/fedidcg/FedCM/issues/374>

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

Educate Regulators Fix Misunderstandings on Identity: Wrong Words

Session Convener: Chris MITRE, Nat OpenID, Shin'ichiro Matsuo

Notes-taker(s): Reuben Bailon

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

List of words abused and proper translations:

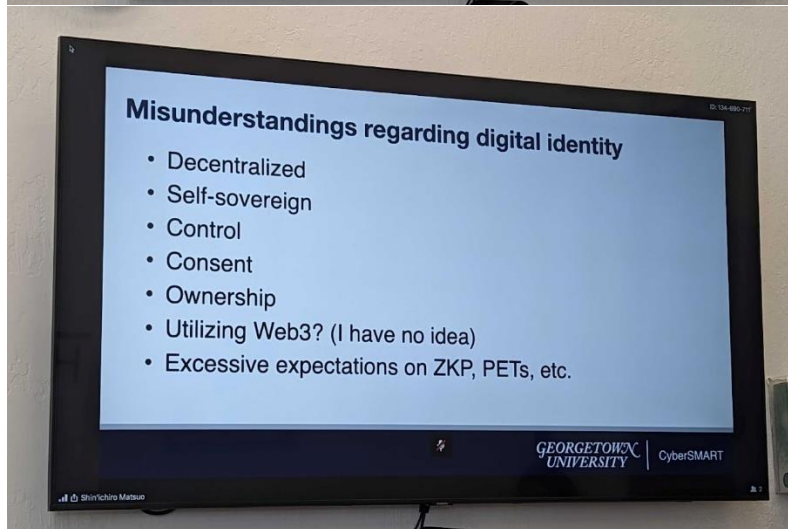
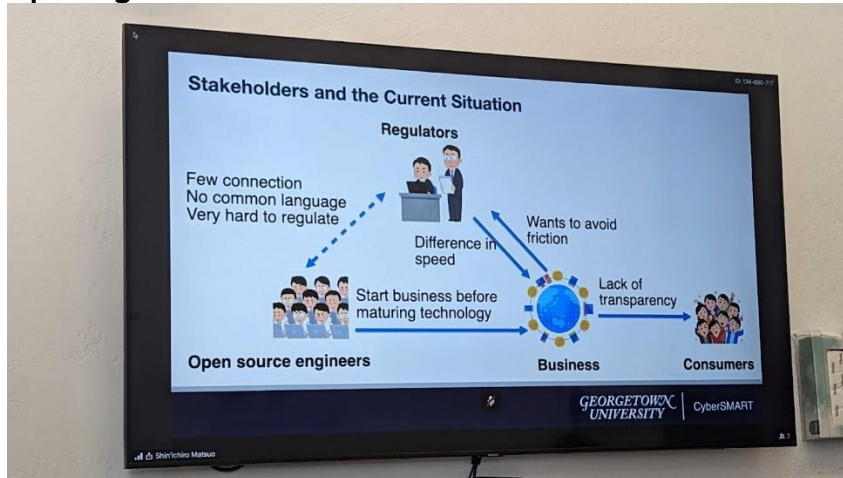
https://docs.google.com/spreadsheets/d/1KD_dxNvolRHGIjwvc8TCxYVbrDu56EEXmgNAqf2g7FU/edit?usp=sharing

Link to the slide deck:

https://drive.google.com/file/d/1D24uoirVEwTh6olTzAMNr6eKuWKUifj_/view?usp=sharing

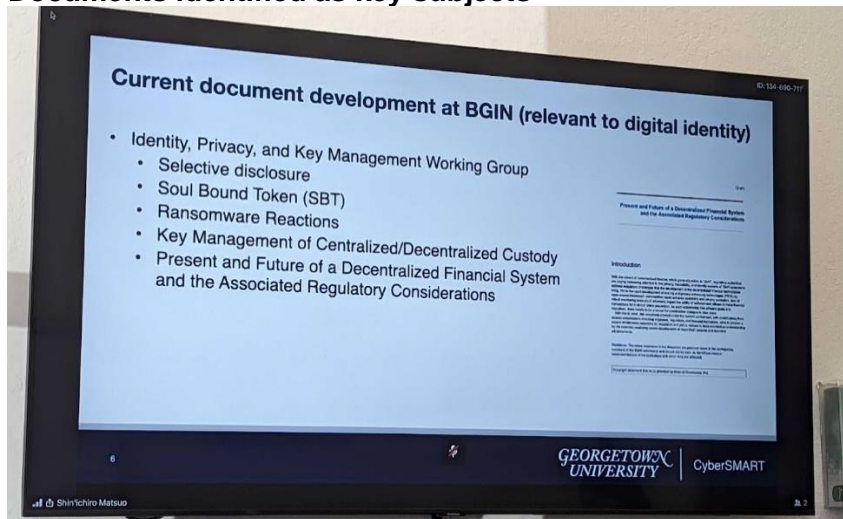
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Opening Slide - Stakeholders and the Current Situation

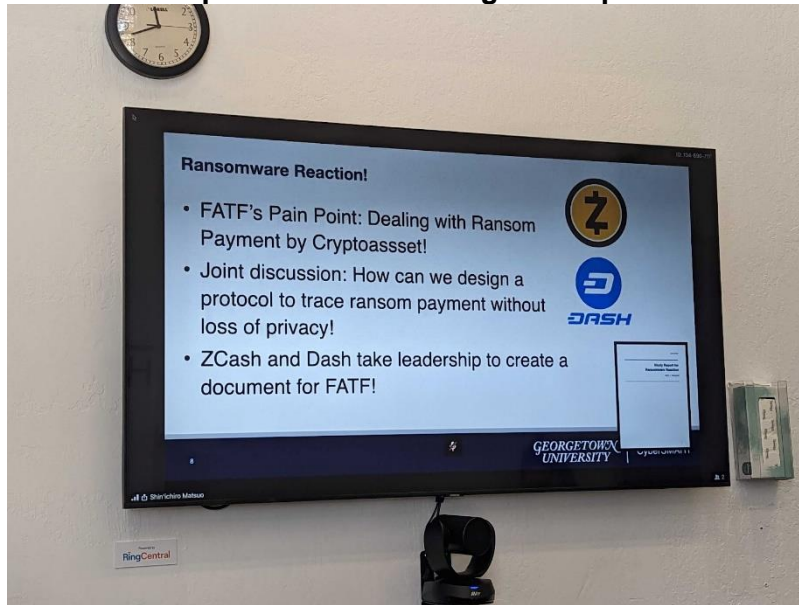


FAFT Organization formed by police to fight money laundering. But technology is not their expertise.

Documents identified as key subjects



Collaborative process of technologist and police



Discussion

- Suggestion for a focus group that includes a wide variety of backgrounds to align on words and phrases used
- Working session: develop a list of words/phrases that need clarifying definitions
 - Link provided at the top of the page
- Next Step
 - Chris to engage the community to continue the activity to ensure language has accurate representation: reachout to Chris cjb@mitre.org and Shin'ichiro for more information or to get involved
 - BGIN will continue working on creating common documents relevant to digital identity, at the IKP working group chaired by Nat Sakimura.
 - BGIN will hold the next general meeting from November 30 to December 2nd. The session of IKP-WG will be held on November 30th. It is held at the University of British Columbia in Vancouver, but it is a hybrid meeting. See the meeting website: <https://blockchain.ubc.ca/events/blockchain-governance-initiative-network-bgin-block-7-vancouver-hybrid>
BGIN website: <https://bgin-global.org/>

Poly, the game of governance: A Tabletop game to help people create rules to support their goals.

Session Convener: Joyce & Doc

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

SSI Harms: Good, Bad + Ugly

Session Convener: Darrell O'Donnell, Neil Thomson

Notes-taker(s): Neil Thomson

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

The initial draft of the paper: [Overcoming-Human-Harm-Challenges-in-Digital-Identity-Ecosystems-V1.0-2022-11-16.pdf](#) is available for viewing. This will continue to be updated.

- [Permanent Link to Harms Paper](#)

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

First draft of the paper **Overcoming Human Harm Challenges in Digital Identity Ecosystems.pdf** is available for viewing. If there are comments - send them to neil.thomson@queryvision.com (for now) and a ToIP specific feedback channel/email, etc. will be set up for public comments for later drafts.

The ToIP Harms Task Force is looking any and all feedback:

- What's missing
- What needs modification and/or a different perspective

Comment within ToIP, there are many Technical perspectives on Harms, but the principle author: Nicky Hickman, provides a human perspective that many of us in the tech community frequently miss, or are not aware of.

One key perspective is that SSI/ToIP cannot just look at issues from the tech side, but also from the human and governance (which is the other half of the ToIP Governance Stack)

The paper lays out a framework to determine what harms that digital identity and other SSI principles can or could cause and what can be done to mitigate or eliminate those harms.

The paper also acknowledges the political and other factors (PESTEL - Political, Economic, Social, Technological, Legal and Environmental) which both assist in identifying harms, their sources and potential solutions.

An example in the paper is of persecution (and conviction) of a woman previously convicted of a crime for illegally voting, where she was entirely unaware (and was not informed or checked at the time of voting by the election process) that as a convict it was illegal for her to vote.

A key consideration is what is the influence of SSI/Digital Identity, which can cause social division or partitioning of those who cannot (\$\$, skills) or do not want to participate.

Another question is whether the implementation of SSI/DI lends itself to users casually releasing all types of personal and behavioral data (e.g., transaction and location information) if they are not aware of what a web site/service does with their data or finds it simpler to just state “Yes” to any consent for use of data, etc.

Observation: online it is currently too easy violate privacy (or have your privacy violated) and it is too hard to enforce (your) privacy.

A question that came up frequently in discussions about existing and potential (online, digital) harms:

- Is this a general online problem vs. an SSI specific problem?
- What does or could SSI do to limit, mitigate or eliminate causing harms?
- What are non-technical (legislation, regulation, society norms) aspects

Discussion:

Why do Governments need a single (government-issued) single identity for government services?

Answer; even in full democracies, governments, and particularly bureaucrats, are biased towards control, plus simplification of their tasks (vs. the public)

There is a tendency for the development community to grab stated problems and start solving them without understanding the requirements and impact.

There is a great deal of complacency about sharing data due to the “seduction of convenience”. Many users don’t believe that they could come to significant harm online (due to their behavior, including consenting to everything).

Education and notification (hey, this website sells your data to XXX, YYY) on harm could/should be a default for online systems and perhaps browsers.

In many cases, it is unclear if online authorities are doing their job (on harms) or if they are concerned about harms at all (in an effective manner).

There is a need to rebalance in favor of users through incentives and regulation/legislation.

Why do we need SSI, and what issues does it address?

- Companies make money using personal data. Using SSI features can be part of the solution.
- How do we get users to see SSI as in their interest and what it does for them -> Education
- Reality is that businesses using the surveillance capital business model will push back

SSI Harms vs. Anti-Harms

- Is SSI bringing new or “enhanced” harms to the digital/online space?
 - No.
 - SSI does bring new tools to address to mitigate or block harms, but they need incentives & regulation (through legislation), including a shift in general business behavior to make them reality
- Apple is an example (albeit in a proprietary manner) in pushing back against the model with their recent anti-tracking features - which have impacted Facebook enough for Facebook to push back, hard.

Bad identity/data privacy vs. SSI?

- What has to be fixed about identity/data privacy in general vs. SSI specific?

Even with the assumption of higher requirements for consent and more sophisticated choices, users won’t understand those choices and will most likely not be willing to put in the effort to protect themselves.

Potential solutions:

- Standardized base set of consent “expressions” and machine/human readable “language” so that consents work across websites/services.
- 3rd party services to create consent “packages” which users could subscribe to as a service for general (default) consent
- Authentic data/data provenance chains and trust anchors (traceability of data)

Need a harms model of online governance (identity, data, privacy,)

Bad example of identity system arms: Indian Aadhaar identity system, a mandated single identity system by the Indian Government. This was very easy to use and was widely adopted. However, the implementation meant that the government got notice of every transaction - whether personal or purchase.

Problem for online data - it can be very difficult to correct incorrect data (e.g., date of birth, name, height, ...)

Role of regulation - implement limits (which is part of SSI) to limit what “Verifiers” can ask for. There are multiple examples of bars and other businesses scanning and keeping driver license and other information, which they have no legitimate reason to do so for proving legal drinking age, etc.. This is a legislation/regulation problem.

Problem being seen in some countries is compulsory government issued identifiers and unavoidable surveillance. An example of this is mainland China, which, during COVID had green and red status for individuals. Red status blocks travel and access to many services. This was reported as being done routinely to individuals out of favor or seen as treats by the government, including dissenters. This was a result of China’s Social Register, where social activities and behavior of all citizens is subject to recording and use in “prosecution”.

Another example is creating a list of approved journalists (those favorable to the local government), restricting access to news events and “pressers” with politicians.

Other aspects are general digital/online functionality that is independent of SSI tech. This includes businesses using personal data for correlation out of band with SSI workflow.

There is also the risk of over-disclosure, which SSI cannot address, as it is every user’s right to consent to any request by a verifier.

This is also true of digital wallets, that through interaction on behalf of the could gather a great deal of information, including behavior.

The phrase “with great power comes great responsibility” was mentioned in this context.

These are all examples of policy/political problems requiring legislation vs technology (or strictly technology) and outside of SSI.

Additional aspects - those who entirely opt out of leveraging identity technology, such as religious (or similar groups) who do not believe in having photos taken (or any other biometric). This creates a tiered (and potentially fragmented) society.

Alternatives that need to be accommodated, including:

- Passive physical card, resilient paper, token or fob
- Electronic card with independently stored data (for offline)
 - Potentially executable (smart) agent, which could be transferred to local compute engine

Part of the problem for future harms, is while they may be a recognized potential problem, the most damaging are going to be unanticipated. As is true with some aircraft accidents, the really damaging ones are only obvious in hindsight, so any assumptions on SSI systems cannot be that technology is of the “sealed box, can’t be updated” variety.

Does SSI:

- Actively provide mechanisms to mitigate prevent known harms?
- Introduce new harms (level of investigation unknown, but nothing obvious so far)?
- Have mechanisms to capture audit trails to determine root problems once harms have been identified

A goal for SSI (and related tech) is that as a “brand name” that safety is built in, or updatable to react to unexpected harms.

A complicating factor is what regulations are invoked in each jurisdiction. Recent and ongoing evidence is political decisions about digital identity and privacy are clearly causing harms as outlined in this paper.

False trust:

- Being dependent on implementation
- Assuming cyber-secure
- No bad actors
- No bad developers (poor implementation)

To address harms requires joint efforts and monitoring by jurisdictions (governments), profit and non-profit business/organizations, in addition to tech.

Some known harms:

- False representation
- Overly complex consent or assumptions of expertise by users to self-avoid harms

Recommended viewing - the Coinbase documentary on the history of the introduction of the credit card

An unproven assertion - that digital tech in general, and SSI and proposed digital privacy and related tech in particular makes freedom greater in highly democratic, personal freedom and privacy protecting societies, but also provide mechanisms to make subjugation worse in repressive regimes.

Positive regimes:

- Health Care - control of Health Care data. Ability to request and present by the individual, authorization by the individual
- Much easier to demand your own data
- Problem with much of the freedoms is the “gun to the head problem” where a bad actor can force someone to act in a self-harming manner under threat using same tools that provide advantages.

Conclusion

- Without good laws and a moralistic society, you’re screwed. New! Improved Oppression!

Tech makes it easier to be good or ba

Risk - you are carrying “everything” on your device, which is now a single point of failure. Even backup doesn’t help in the “gun to the head” problem.

Aside from smartphone as single point of failure, there is nothing new.

Witness - gun fights in Miami over identity theft information (thumb drives or larger)

Criminal organizations as part of the surveillance landscape

A potential issue tha blurs some of the harms would be allowing - deliberately or through flaws - sharing of VCs and identities. While their may be no malice in 90% of cases, we’re back to the “gun to the head problem”.

Traveling problem - what data travels with a transaction as it crosses jurisdictions? How can that be avoided and subject to regulation.

Existing problems of non-repudiation - disputes on credit card charges. Who has the most data wins disputes, vs where the actual problem in unexpected or illegal charges lies vs. how to detect actual fraud claimed as a miss-applied charge. Scale that up to all online transactions.

How is ensuring that mis-use of data is detected (auditable) such that breaches of consent/data contracts can be detected?

Right now, issues that need to be addressed in tech are currently (and maybe enforced) by the law, which has the ability to prosecute, but not the ability to detect both the harm/crime or the actor who deliberately or inadvertently caused the problem

Enabling Native Mobile UX for OAuth/OpenID Connect flows

Session Convener: George Fletcher

Notes-taker(s): Andre Priebe

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

Native/Mobile Apps - Why don't we give back control over the UI to App?

There are many issues if the app were in control of the presentation of the login:

- Many security considerations that login and confidentiality of the credentials are not handled properly
- Users getting trained to enter their credentials on different login pages have a higher risk of phishing.
- We lose the flexibility on the login flow, for instance, adding something new like Passkey to it without aligning closely with the/all apps.

But there is the risk of losing business because of a bad user experience - opening a browser, having a visual break, inconsistent UX.

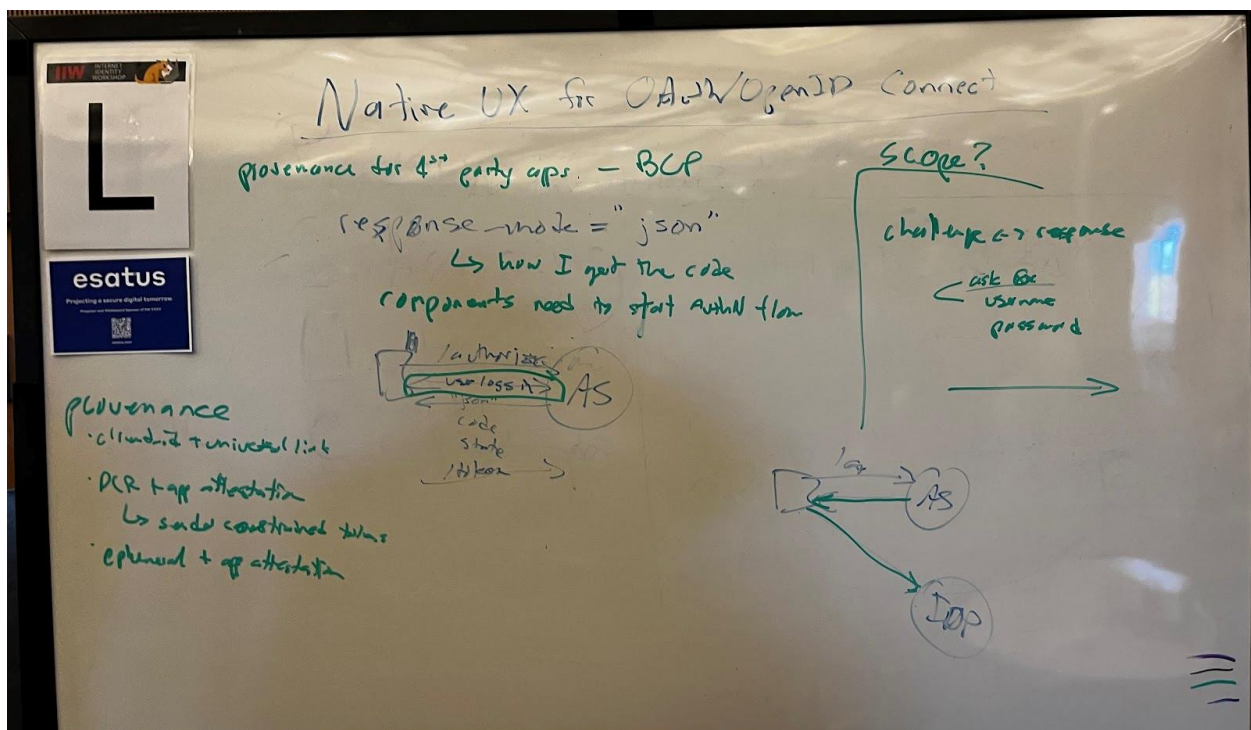
Let's consider adding a new response_mode=json to OAuth, which returns a JSON-based description of what has to happen for the login and which is meant exclusively for first-party apps.

JSON can describe flows with elements like username/password, fido, and onboarding/registration. It has a version. It might make sense that the app has to provide its capabilities upfront and has to fail back to browser-based login in case it is not able to provide the required elements - or if 3rd party/social login is used.

A prerequisite to allow an application to request response_mode=json would be a robust provenance:

- client_id + universal link
- DCR + App attestation

Defining just the OAuth response mode without the JSON-elements might make the situation worse, as it is likely that there will be a couple of weak implementations out there.



eIDAS Revision: History and Updates including ISO mDL and ICAO DTC

Session Convener: Dan Bachenheimer

Notes-taker(s): Dan Bacheheimer

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

Presentation is here: [eIDAS Revision BACHENHEIMER.pdf](#)

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

Provided a brief background on eIDAS, the legislation for Europe's electronic identity and trust services, which provides European citizens trusted national ID cards to enable a means for cross-border authentication.

We then jumped into the eIDAS revision which is intended to be more SSI friendly and walked through the EU Digital Identity Wallet functional components from the initial Architectural Reference Framework; specifically what makes it distinct from other wallets - and what is similar. We spoke about the initial inclusion of a unique, persistent identifier requirement which is now deprecated.

The final topic of discussion was ICAO's DTC - after a brief history of ICAO and machine readable travel documents; what it is and what it isn't and how it fits into the EU Digital Identity Wallet.

The next point of discussion was the ISO mDL; what it is and what it isn't and how it fits into the EU Digital Identity Wallet.

One specific point of deeper dive was around what EU law may determine to be an "authoritative source" for biometric authentication. From the EES legislation, it is clear that ePassport photos from third-country nationals are not considered authoritative - they must be taken live. What about FIDO? Biometrics are self-registered, on a personal device, remotely - are they authoritative?

I concluded the session with where ISO stands in the area of Digital Identity Wallets - and where they MAY lead..

People are Lazy – how do we make it easier for them to do the right thing?

Session Convener: Scott Phillips

Notes-taker(s): Joshua Coffey,

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:

- Cookie Banners are a good example of convenience overriding “the right thing”
 - Most people tend to click “Accept All” just to get it out of the way
 - It’s intentionally made difficult to deal with
- There’s a difference between what people tell you they want and the actions they actually take
- What is the right thing?
 - We all tend to agree that we should be in charge of our own data and our privacy, and it shouldn’t be in the hands of someone else
 - There’s a difference between user control and privacy – users can choose to violate their own privacy and give their data away.
 - Is the end goal to maximize control or privacy?
- User control is more work. People will tend to go with the path of least resistance.
- We all come from the same space — most of us are highly educated, tech savvy, etc.
 - Not everyone is working with the same level of technological expertise
 - How do we make it possible for people to make decisions that are in their own best interests?
 - Philosophically, user control is a good thing, but does that still lead us to harmful outcomes when people don’t want to put the effort into exercising control?
- In the US/UK/etc., we have certain expectations of privacy (even if that might not be the case)
 - You can get at privacy by design, or privacy by policy
 - Ultimately, we want both – regimes change, the world is changing; it’s becoming easier to imagine large swings in these countries than we might’ve previously expected.
 - We should design systems which enhance privacy without the added benefit of government support or enforcement
- Privacy By Contract
 - You share data with an entity and have a contract which prevents them from (legally) sharing it
 - “If you don’t have [a contract], you don’t have much.”
 - Contracts are a good language for expressing the various parties involved in a transaction and their interests
 - Granularity can be expressed by contracts – prove that you’re an adult without sharing your age
- There’s a difference between a YouTuber putting a sponsored segment in their ad (it’s a contract between the sponsored and the sponsor which has nothing to do with the watcher), and an ad playing on a YouTube video served by Google due to data collected from you
- The incentives / aims for different entities are different
 - NGOs have the purest incentives
 - Governments have less pure incentives but still close
 - Corporations are likely to have perverse incentives

- GDPR was trying to provide user control, but it ended up with another popup that people ignore
- Could we have sane defaults or other mechanisms where it's easy to make better choices?
 - We already have a lot of things solving these problems
 - Certificate Authorities are in all our browsers. Users technically have control over them, but largely don't exercise it, because they don't need to.
 - How much can we expect users to make individual decisions?
 - Should we have them proxy everything to smart agents / etc.?
 - Most of us already proxy out a lot of control to password managers
 - "Accept only necessary cookies" is helpful
 - Defaults are often chosen maliciously as opposed to beneficially
- The tools we have at our disposal are not equally accessible to all
 - Many people will never transition to password managers because of how involved that process is
 - We should invest in the UX of our tools to make them more accessible to all
- We need to have an overt discussion over what it is we're optimizing for – privacy and user control have many mutually exclusive elements
- What if we had a smart agent which helped make these decisions for us automatically?
 - "Always accept only necessary cookies on my behalf"
 - Agents are a stopgap – they don't solve the core issue of having no control over your data, but they do solve a problem.
- How do we get to a public/private partnership to lay the framework for what is allowable and expected?
- "Good ID" and "Bad ID" are problematic ideas – different of ID are acceptable for certain use cases while vastly inappropriate for others.
- Technology moves much faster than policy
 - Privacy Act was made in 1974 and hasn't changed since
 - EU chartered a path with GDPR and everyone else said "oh, let's do that"
 - The political left and right both have anti-big-tech threads for different reasons
 - We may conceivably see improved privacy laws for this reason
- There's a big difference between "consent" and "informed consent"
 - "Informed consent is a fallacy – it doesn't exist"
 - Consent isn't exactly control
 - If you want to use a service, you don't really have a choice.
 - GitHub's ToS specifies that all source code may be used to train GitHub Copilot
 - There's no real alternative, so it's essentially a false choice

SESSION #9

From Twitter to the Data Palace - product brainstorming

Session Convener: Johannes Ernst

Notes-taker(s): Johannes Ernst

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

<https://dazzle.town/>

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

Just a few people showed up. We didn't spend much time on the stated subject of the session, but instead talked about gory details of the technology behind Dazzle.

Digital Identity for A Nation: How Singapore implemented National Digital Identity using OAuth 2.0 & OIDC

Session Convener: Wei Lai, Tze Yuan Lee

Notes-taker(s): Tze Yuan Lee

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

Singpass API portal - <https://api.singpass.gov.sg/>
Login OIDC flow: <https://api.singpass.gov.sg/library/login/developers/overview-at-a-glance>
Myinfo OAuth 2.0 flow: <https://api.singpass.gov.sg/library/myinfo/developers/overview>
Presentation: <https://www.youtube.com/watch?v=Xg8iWouMTJA&list=PLVs2bLtIMGhI5A1tQemmUfcTPGKZ1cUj&index=6&t=38s>
Login API demo: <https://youtu.be/AOt4WE6aueg>
Myinfo API demo: <https://www.youtube.com/watch?v=NGj3XXU-HgE>

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

| Topic | Notes |
|--------------------------|--|
| Introduction of Singpass | Singpass comprises the smartphone application and a back-end managed by GovTech. The smartphone application is the user-facing component, which is |

| | |
|-------------------|---|
| | <p>accessible for free to all Singapore citizens, permanent residents, and Foreign Identification Number (FIN) holders aged 15 and older.</p> <p>It enables users to leverage their legal identity to carry out a wide range of online and face-to-face transactions with government agencies and businesses. Singpass was first launched in 2003 as a username and password to sign into government websites and has since significantly evolved.</p> <p>Today, Singpass includes several products and features for citizens and residents.</p> |
| Suite of products | <p>Introduction to suite of products</p> <ul style="list-style-type: none"> ▶ Login: Users can verify their identity online in a secure and trusted manner when transacting with websites and smartphone applications of government agencies and businesses. Verification can be performed using a six-digit PIN code or the phone unlock mechanism, such as a fingerprint or selfie, on most devices. ▶ Verify: User identity is verified for a face-to-face transaction and the secure transfer of personal information through scanning of QR codes or tapping near-field communication (NFC) devices. ▶ Myinfo: Manages the use and sharing of personal data for simpler online transactions; data is pulled in real time from authoritative sources, and consent is facilitated through Login or Verify. For example, this feature can be used to pre-fill forms. ▶ Identiface: A stronger method of authentication than Login or Verify that uses face verification based on the latest facial image enrolled with the Immigration and Checkpoints Authority (ICA). ▶ Digital IC: Enables users to present a digital version of their National Registration Identity Card (NRIC) or FIN card. ▶ Sign: Users can create secure electronic signatures using a preferred third party digital signing tool compliant with Singapore's Electronic Transactions Act. ▶ Document Wallet: Users can store digital versions of other official documents, such as a driving license and HealthCerts (including COVID-19 vaccination certificates). ▶ Notify: This feature enables users to receive push notifications and alerts from government agencies, as well as information related to Singpass transactions. |

► **Shortcuts:** Users are able to log in directly to commonly used digital government services, such as the Central Provident Fund (CPF) for social security, HealthHub for health services and records, and the Inland Revenue Authority of Singapore (IRAS) MyTax Portal.

Hyperledger ICAM Solution for a Data Centric INDOPACOM Training Environment

Session Convener: Paul Watkins

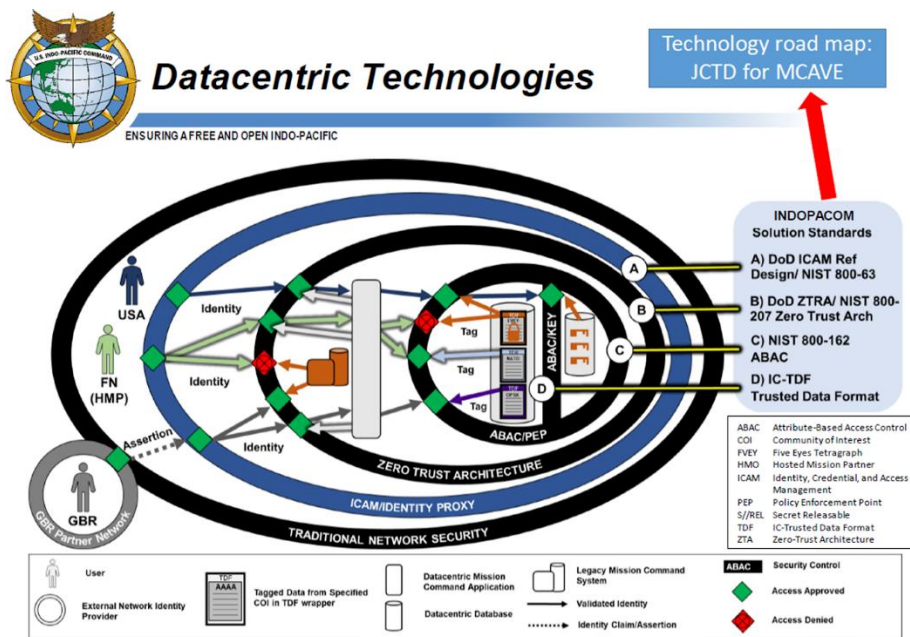
Notes-taker(s):

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

Discussed Solutions using Hyperledger ecosystem.

Three solutions discussed were:

1. Hyperledger Fabric (w/ Anon Creds toolset)
 1. Pros - Private Channels, Lower Processing speeds required, Containerized for scalable, PBFT, Has an ATO for DoD usage.
 2. Cons - Availability of data has time and latency concerns
2. Hyperledger Indy
 1. Pros - Granular credential attributes, containerized, BFT, ZKP
 2. Slow
3. Ethereum BESU
 1. Pros going through ATO started in July



Identity & IoT

Session Convener: Phil Windley & Andre Priebe

Notes-taker(s): Neil Thomson

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

What is the need for IOT and Identity

Identity is need for data traceability (from the IoT device), for upgrade, configuration and management access, and control (active device, as opposed to a passive sensor).

Identifier vs Identity

- Identifier is (possibly) the serial number on the housing of the device
- Identity may be “bathroom light”

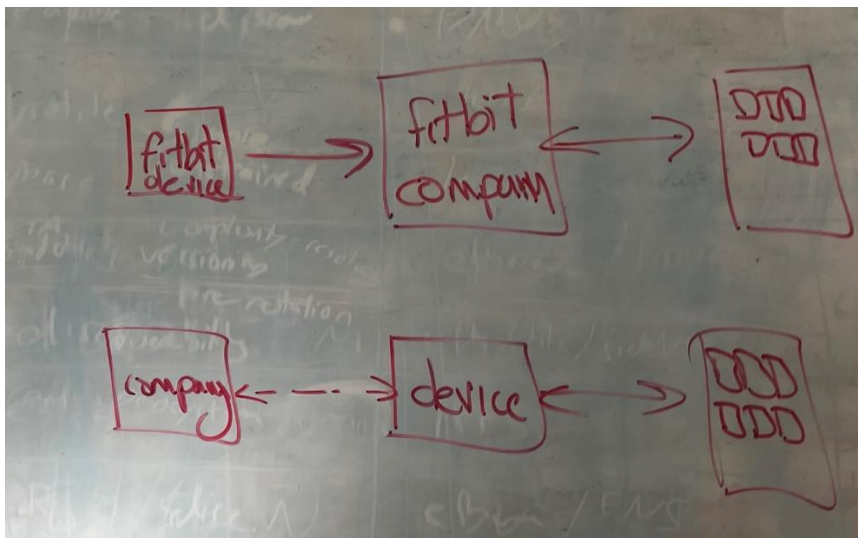
An issue for devices (including smart home) is providing a device with permission/authority to act either on behalf of the (home) owner on it’s own behalf (order consumables or maintenance parts).

Identity is also key to managing relationships with devices. Note that a device may be in several networks or accessible by multiple entities. Example: an appliance may be directly accessible by the home owner, the home automation application and a maintenance/service which monitors for faults or routine service needs.

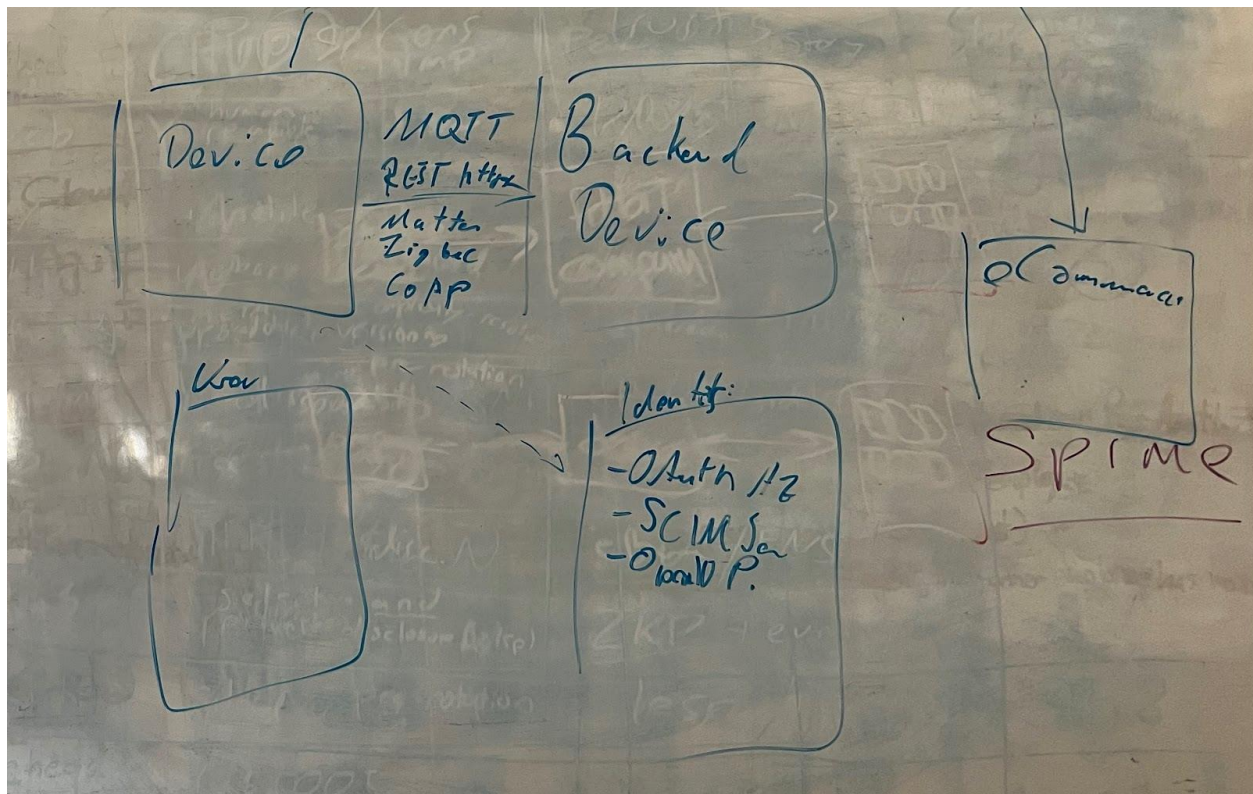
There is also the consent of a digital twin where most of the computing power and metadata information about the device may run on a server - e.g., as a “digital twin”.

See the diagrams, below:

Discussion: Control over FitBit data



Discussion: Different types of devices, digital twins, authentication and qualified relationships:



Advice for managing relationships between users, organizations and devices: Don't try to use existing and established protocols at any price - better design the protocol and figure out what is already there.

Many IoT devices are not upgradeable, so may need smart, upgradeable aggregation/management hubs to provide for network security, and also as a host for additional computational power for low level/basic IOT devices

Capabilities need to be known, including what a device can do with and without authorization to act on its own.

There are several models for IoT devices communicating. As an example for a FitBit Device.

1. Fitbit IoT device -> FitBit corporate server -> users server, phone or laptop
2. Fitbit IoT device -> users server or phone -> FitBit corporate server

The first essentially puts the FitBit corporation in charge of the person's data as it is the first to receive data from the IoT device, and is the actual FitBit configuration. The second puts the person in control of data/privacy

Discussion on [MATTR](#)

What is the role of a back end or phone in IOT - could be for storage, could also be for computational services beyond what the IoT device can do on its own.

Identity (vs Identifier) may be handled by the back end.

- Authorization provider
- SCIM
- OIDC provider

May also have a digital twin on another server. So the “whole device” may be a distributed device.

Use Case for a supply chain - where a device may be included in different chains with chain specific identity (and possibly identifier)

[SPIME](#) - Science Fiction author Bruce Sterling concept - Space and Time

- Gizmo

Everything has a unique identity through **SP**ace and **tI**ME

Principle is to trace the “life” of the item from creation/birth to destruction/death.

The smarter things get the more interesting data can be collected over time.

How to you correlate/synchronization of the device with its “digital twin”

Picos - persistent compute object - Phil Widdley concept

Can get IoT devices - which can capture and transmit (e.g., bluetooth, cellular network)

Car Area Network (CAN).

Device in a car to monitor car activities/events to see what information was gathered and what interesting information you can provide to the car owner.

CAN Bus never considered that external devices or agents could get external access for remote control (bad assumption).

Somewhere @ Tesla, they have a connection to each car - have a model to each car - which sync both ways - Another example - aircraft jetliner engines - have been digital twinned for years.

Another example - Amazon auto cashier - you just take things off the shelf and are automatically debited.

Digital twin is where most of the smarts and storage is - the IoT is there ofr inputs and outputs - a remote I/O channel capability.

There can also be a digital family - a fleet of vehicles - a both individual and a composite object (With their own operational data and aggregated composite).

Another feature for digital twin is that other users can have access, but restrict what information is released.

“I just bought your smart-house, now what”?

- Does the new owner have full access?
- What about the former owner?

Giving up a car or house, will also give up the history, which you may want to extract prior to ownership transfer.

Then there is selling the data collected from smarthome devices to appliance manufacturers, usage patterns, social information.

An issue of providing permissions to the device to act on your behalf. Risk of having to give too many permissions for the functionality wanted by the user (e.g., giving out the credit card).

Does a device belong to a single “controller” or all the people in a family or by the family and some outside agency (that manages a device for maintenance reasons).

Example: weigh scales - who do they disclose the weights to - only to the individual - how would the weight scale know the difference (without identifying each individual)

Another example - shared TV - how to handle multiple users/viewers

Problem of rental cars - which share driver/renter information with many different services (including your contact list).

How does that interact w SCIM.

Providing a toolset ow to model and link devices and back/ends/digital twins via different communication channels.

Protocols talked about are not compatible with more complex interactions and relationship use cases.

Manufacturers are taking “simple” use cases. Selling device for someone who uses it, which would be very different for a TV sold to a hotel vs. an individual.

Manufacturers have not worked through the more complex use cases.

Sounds like a need for a raw i/o interface where the back end

What is the gap between MATTR and other things.

Most of that is the complexity of the relationships and inclusion in higher level processing/uses.

Cars and their smart systems were designed for a small number of users over 15 years vs. daily different users for 4 years (as rental unit).

That level of engineering is beyond the manufacturer.

There is the problem of upgrades - for lost cost devices there will never be security upgrades - which leaves security gaps as a long term risk.

If leveraging the full capabilities of IoT is complex then they won't be useful.

Classic techy dev assuming that users will also be techy is endemic.

Capabilities like this have been available for a long time, but not generally known about (or usable) by your average consumer

Toasters getting security upgrades - for toasters - burn ads into the toaster to provide a revenue stream to afford the ability to upgrade.

Co-ops: A Business Model of our Future for our Future

Session Convener: Chris Heuer <https://linkedin.com/in/chrisheuer>

Notes-taker(s): Otter.ai

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

Several related articles are linked from Chris' LinkedIn

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

The session was recorded and transcribed by Otter. Audio is available here <https://otter.ai/u/sPW3-k4eKN4E-pVjZfDArZyXwuA>

Transcript:

Chris Heuer 0:00

Yeah. Anybody kind of settle in. Also breathing for a minute because I've just done like I made three introductions for people I met today via LinkedIn. I delivered something or client. I wrote something up and then I have like an opening that I had to write. So we're all good to go. I'm Chris. Nice to meet

you here for the session. Okay, great. Well, as you can see over there, let's okay let's get into this

so let's get underway then. This is the conversation. Okay. I'm sorry. Yeah, you can go It's okay. You have to go this is asking you to open face opening. Thank you so very much. Thanks for coming. Yeah, well, you know what, it was the last one left but I wasn't too sad. So it's good to be out here. I have to unfortunately cut this a little short today because I have a three o'clock meeting. I have to run to so I can actually get paid to keep doing the fun stuff. So anyways, I just wanted to put that up front. Before we get underway. Hi, my name is Chris Heuer. I got short story to introduce the topic and then to ask a question and to propose that into the middle. I've been into the circle for conversation. I've been kind of leaning towards all my life as being a stand for integrity. It's gotten me into trouble in a lot of places as well, but like I'd rather do that and suffer those consequences and not I tend to overshare and do TMI and all that. So if I do that, I guess that just kind of who I am. So forgive me for that. But, you know, I think that if you're better off, I'm better off and for the central principle of my life, without getting it all the background behind it. It's just what I learned from a very early age as part of the lesson in that way, you know, whether you want to use the religious side and say We are brothers keepers or whatever else, it's that, you know, we are interdependent upon each other. I think when the biggest

challenge is that it's not as visible. You know, particularly in rural parts of the country. It's just not visible you have to be independent. You have to stand on your own. So when we don't see it, we don't pay no mind to it. So a big part of what's missing and one of the reasons why I do like conscious capitalism, although every you know, sort of structure talking about this stuff is a little different, is the idea of bringing consciousness to it. And in fact, one of the things I think that's hurt society that's led to this right now, is the general absence of conscious value. You know, we look at something on a sticker price, we say that's the price. It's a value and we have shorthand to do this sort of stuff. So one of the big challenges it has created a lot of this income inequality, a lot of other challenges out there from businesses. And somebody else had said this a few times too. It's really the tyranny of convenience. Like we give up a lot just so that we don't have to do much and I'll tell you as well a lot of people don't agree with me on this, but I use Facebook ID to log in and get people connected. I need to log into place because it's easier and I just don't want to remember all those passwords. And I look at the consequences of who am I sharing it with, you know, Expedia, instead of great side hustle, travel agent.com And I feel a little better sense of it, even though they're bigger companies and everyone has their different degrees of comfort with that, and that's fine. But where I, where I started a number of years ago was a realization that too few companies, but let me say it this way instead, that we needed to shift from serving the stock market to serving the market. And so that's kind of a big lead into this where I started working on my book and a bunch of other concepts about it was around that. Last year, I ended up getting into web three a bit and crypto. And really more than that the underlying architecture in the future potential than the existing use of it, but what I recognized was that it was finally a way to shift from the sharing economy concept into what we call the CO ownership economy. And the difference there is that there's a higher degree of stewardship responsible for CO owners. And so that changes kind of the mindset of it. But what it also means is that the way we derive value or the way we generate value is also different. And so that led me to looking at the Creator economy and the rise of what's going on there. And the real need for more smart people to figure out how to work together so that we can improve, improve our collaborative EQ, so that we can improve our collaborative productivity. purely looking at that, you know, what it comes down to is the incentives. Obviously, mission and purpose is a big part of what we're doing today. And at the center of co ops, that's kind of the heart of it. We have a purpose. We have a mission. We're aligned together. We're working towards that. But what it also means is that the incentives need to be aligned. And there's a whole bunch of psychological problems to be worked out. I don't think it's all fixed and ready to go as it is yet. But I do believe we're at a new age of the rebirth of the co op as a new model for us to really go going forward and in that thing, one of the titles for this book that I really hit on recently, in trying to figure out how we can get that world that we all would like to see, that isn't what we're seeing right now and the way corporations are taking advantage of us and harming us and not caring in so many ways and you know, 30,000 times salary for the CEO to the lowest paid employee and all that stuff was that we weren't necessarily going to get Tim Cook or other people to become co ops with Apple or anything else. And like with the early Internet era, we needed to create a groundswell and the current attitudes and activities of Gen Z aligned with purpose tends to fit within this sort of group. So I've been kind of pondering the Gen Z entrepreneurs choice and sort of a kind of working title for it being that you can either, you know, started company, as a Gen Z entrepreneur, and make the fatal sin that I did, which was when I started my first company, I thought I owned all of it. I could give out a little bit of stock here, a little bit of stock there and that you know, I was just entitled to it. So that's like an original sin really to think that just because I've started something that I own all of it, and then I'm going to own all of that. And so I start thinking about, you know, how do we reward the value that CO creates it? And so ultimately, that's kind of the landing of the big phrase, if you will here, which is while we are finding new ways to co create shared value, that not only you know, benefits of the company and the employees and the customers, but also society. Is anyone familiar with shared value, by the way, the concept of it and the Institute and all that? So Michael Porter, about 12 10 12 years ago now, he is a US competitive intelligence guru typically works with all the top government folks out there and the top business leaders put out this paper in Harvard Business Review called shared value. And basically He

admonished the corporate powers that be for their exploitation, and saying they need to do more to like, give to society that they weren't doing enough. And if they didn't change that they were gonna go extinct. So shared value has a little more meaning than that. But if we're going to learn how to co create shared value, then we need to now think about how we're sharing the value that we've co created together. And so that's what ultimately leads me to Dows and co ops and, and more than that, but what it also led me to and one of the reasons why I'm here is this idea of a zero profit company instead of a nonprofit company, nonprofit company is specifically not to get to profit, whereas the zero profit company is really about balancing that. Yeah. Like when we get to a certain point of growth, where we have retained earnings to be able to operate and we have some r&d money to invest in growing and that other stuff, there's a certain point with growth, decelerates, and which we can then look at how do we pay back dividends? And in fact, this is a real core concept of stakeholder capitalism, with a little more extreme sort of, let's take it out to the heart vision and not just through the easy stuff with the idea being that you have five primary stakeholder groups, employees, management, investors, customers and partners. You also do have communities by the way, but maybe you have a 1% pledge. We can talk about that later. But the idea being is like we need to basically bring consciousness to the value contributed by these stakeholder groups, and keep them engaged in what we're doing and cooperatively develop something that is for all of our mutual benefit, and which people are fairly able to participate in. So that leads me to the question of why did you come here to talk about coops are you in one? Are you trying to start one? And then of course beyond that, is this even possible? Or am I just fucking full of shit and spouting marks? Because I've had people telling me that by hand please if I can, so we can, please. So a co op is a cooperative. So literally, that is a cooperative organization. You've probably heard the term building coops from New York because New York has everybody in the building. It's actually an alternate. It's not an HOA actually, Hoa is a dirty word, but it's literally how they manage that building together. And it's really more of the individuals involved. Instead of an HOA board and all that stuff. So it's actually a form of a sort of legal entity. And there's a lot of other ways that it's been implemented. But ultimately, the idea is again, the stakeholder capitalism that it gives voice power and some greater amount of equality or equity to Yes, an employee owned organization or an employee owned business, although they're not necessarily you know, it gets into what's the difference between a sub essence of it seeing Yeah, thank you, thank you, please.

Unknown Speaker 10:49

Think generationally, you're probably right. A lot of different kinds of things, you know, and Gen Z and how they, you know, they value, you know, sustainability a lot more they can see where this is all going and then what, you know, capitalism has given to us, you know, done to the environment and the process of everybody kind of getting a little bit better off. And I think that I mean, the way I've always seen it is like, dolls are essentially a block can improve living for coops large largely, you know, not all Dallas but, but plenty of Dallas have as spouses in values that, you know, traditional coops do, and then you know, credit unions and other similar sort of, you know, organizations that I've I've seen this process, right, I think there's there's something to that. Cool.

Chris Heuer 11:47

Charles, should I respond to that? Well, whatever you had to share before respond to it, whatever it is, it feels like

Unknown Speaker 11:57

in some ways, I think like Bitcoin is a cooperative currency, which is, you know, fascinating because it's one token and you know, with different fees and things like that. And so, so that, to me is just this, like, boom, we can create cooperative web scale that works

Chris Heuer 12:13

very much open infrastructure and open infrastructure.

Unknown Speaker 12:15

I think you're spot

Unknown Speaker 12:17

on with this idea of the American Dream being to get rich in a company because you started the right idea really quick, and that's, I do think that what they're seeing and that's not so what's rewarded in life and going to a documentary, this couples looked at the phrase, the American dream, and a lot of time it is about monetary riches, where it should be about spiritual riches and something different, so they call it the dream we choose and highlight some of these but I think that is, is growing. And in fact, I'm really interested if anyone wants to start a co op where we can rely on basic income, maybe a minimalist income but basic for everyone. That's, yeah,

Chris Heuer 13:07

that gets really interesting when you start with a UBI time banks and other forms of the cooperative operating out there. I actually entered pre pre pandemic, I was working under the sort of idea at the time that the 2020s would do the era of the guild. So one of the things that's really interesting when we start looking at these cooperative models, and being able to share is actually the rising power of human capital over venture capital. We're literally all of us with our SaaS services that we're already paying for many of them are free. You could literally start a service providing business right here together, use your contacts, reach out to people you know, to your design. You know, we can literally in the course of three hours, have a webpage up that offers a service that we can then go off and sell to people we know and we can make money together. It's literally that easy, right? So I look at the professional service firm as that and then of course, we go back to the old concept of the guilds. Not to create monopoly protections that are given feudal society, but to band together to ensure quality and to actually assure quality to the people who are buying those goods and services. So that like if somebody's delivering something as part of the guild member and they screw up, the guild is responsible for they're in accountable to go in behind it and make it right and figure out where it is. And then there's educational and learning opportunities for the person who messed up. And then eventually, if there is determined to be malfeasance or something, there's a little year out, and we've got to maintain our integrity and our quality so it's a really fascinating sort of opportunity right now. And of course software as a service.

Unknown Speaker 14:47

My Groups are talking about this kind of thing. In and out very much more complicated. People they're dedicated to the government's are going to make their job but a lot of us are software developers and designers that are about how can we have a level of humanity through consciousness and get rewards for doing good deeds, whether it be eco tourism, or, you know, getting rid of your pain body and I hope she got pissed off at someone. You know how can I see the love or whatever like I'm an adult. I've seen a lot of people suffer and older generations, and even in my generation, because they're, they can relate to that. So how to get rid of the conscious evolution. I'm into this conscious evolution. So So what are what groups created a group little weekend dream synergy,

Chris Heuer 15:41

awakened really synergy.

Unknown Speaker 15:44

Right now, I have a website awakened dream, but because I didn't do the membership model and yet people besides me doing the administration itself. It's not understood. We have a lot of developers and designers, specifically more developers who want to come together to create a system, but we've got different parts.

Chris Heuer 16:05

Yes. So I'm interested in what you owe. The complexity of that is a whole different thing. And the Dow complexity is even more the rise of Dows and the rise of these coops and actually this is the reason I'm here because old friend of mine, Deckard doing Hello, and he's doing it as a co op. I'm like, You kidding me? I'm working on a book, I go out, and my missing thing is to help stand up a really big talk. So anyway, so we're exploring that right now. I'm not working for him yet. I'm just friendly helping him.

Unknown Speaker 16:34

But he's doing it as a co op.

Chris Heuer 16:36

Yeah, yeah. And in fact, you can go online now legal entity. Yeah. Oh, no, we're already a verified Co Op and all that other stuff. So we have a co op domain and

Unknown Speaker 16:44

we'll easily refund that the way he's taking investment but it's like we can't take investment. This is a co op. We can't execute. Sorry, we can take. We can't give you equity, but we can guarantee you an ROI. Yes. And so there's there's alternatives to all this. But we just you know, we just have to cleverly navigate that regulation.

Unknown Speaker 17:05

Right you can get an ROI or the

Chris Heuer 17:07

well, okay, so it ends up even what you were talking about before, and I I'm a Reiki Master as well. So I mean, I'm kind of down with all that. But there's a challenge in human behavior when we start mixing intrinsic and extrinsic motivators. And so as I look ahead, that's my biggest kind of, how do we solve for that as we started playing with different engagement models with the different stakeholders, so gotta figure that out. But the one thing that I know from past experience and I built a global nonprofit, it was only a official nonprofit in the US and we were operating dangerously in the rest of the world. Thankfully, nothing happened. But, you know, we made it a community organization and a community market. It was one of those first sort of global meetup sort of networks, called social media and club it's still around in about 80 cities now. But, you know, I literally tried to make the first people co founders who would even associate because I wanted them to have a sense of ownership, so that not only would they spread word of mouth, contribute ideas, but that they would, you know, basically feel a part of, and feel that sense of ownership. And over the last five years in particular, we've studied organizational design and culture. And the organizations that foster a sense of CO ownership are the ones that are outperforming because the individuals feel they have agency in their jobs. They have respect, they have dignity. And actually the interesting thing that's happening today to go back to what you were saying before is the greater realization that the well being of our people determines the well being of our organization. And it's so much friggin common sense. Why are you burning out all of your employees? Why are you doing all this stuff? Because they're not able to produce at the level they need, and then you get a great superstar and play. And then of course, superstar ends up being taxed 130% Because everyone goes to him with all their stuff and no one protects them and they get burnt out sooner and they deliberately CIT all of us can raise their hands on that right yeah. Yeah.

Unknown Speaker 19:12

Take care of my braces, you know?

Chris Heuer 19:14

Yeah. Then you can't be happy. It's just like kids. They can't learn if they're not that it's very simple. Go ahead.

Unknown Speaker 19:22

Curiously, Foster is it ownership that the members is ownership the right word for what they're getting like? Or is it about governance?

Chris Heuer 19:40

So So this to me gets into like the world of folksonomy. So are you familiar with that concept? So we can go ahead and define the taxonomy in any way we want, but people come to it with their own language. So you know, they're not exact specific, literally equivalents, but they're conceptually equivalent that people feel related to, and two different people could come in and choose a different word. And it's that sense and that's why language is one of the poorest crudest method for collaborating and understanding each other. What are you gonna get?

Unknown Speaker 20:27

There's less than that. transferability I think I got an expert.

Chris Heuer 20:30

Yes, that's correct. So, so we and that's a part of the very subtle shift. Good point. Okay. A part of the element is that we're not and when I talked about a zero profit company. It is a company that's not built to be sold. Right. So that's an important bit and there's actually a firm over in Sweden, that I'm including, as a case study, its professional services group consulting group called Chris. And that's Chris that Fe and they put all their stuff out so you can learn from it, how they're doing it, etc, etc. And that's where I actually got the term zero profit company from, but yes, it is that point. And even in thinking about, really the nature of the organization, I was fortunate to meet a bunch of good people over the years like all of us here, one of whom is Tom chi. Tom was one of the original founders of Google X along with Dan Frydenberg. And Tom has become a human factors expert and all that stuff. Anyways, ran an accelerator for a little while and he had a different model to it, which really included things like not blocking up smart people with four year vesting agreements for them to get their value, when they've already delivered the value in some algorithm that they're the only person in the world can deliver. So they sit around for three and a half years doing nothing being bored, not contributing to society. We got to solve that problem. That's one of the other problems, stock buybacks, all the rest of it. But at the end of the day, what he basically said in a little bar graph was is basically we're looking at three players, individuals, organizations, and society is kind of a big sphere. And I know there's more than that, because simplifying it right, for a very long time, organizations existed to take away from individuals and take away from society. And what does that leave us with? It's literally how it ends up and his model is very simple. And, you know, for us, I'm really big on attribution. That's why I keep making sure I get this out. But what if we flipped it where the organization was just a model for organizing work? Right. And so now we're talking about future cash flows. We're talking about growth. We're talking about well being we're talking about accomplishing our purpose. And so it really shifts the game and you know, I just know that you know, a lot of the old folks are not going to get this and not gonna want to get it because the world as is a lot of things be fearful out. You know, I need my 25,000 foot underground bunker out in the Arizona desert so I can survive whatever's coming. And so fuck you. I need to make a billion dollars.

Unknown Speaker 23:07

Like when I was talking about driving down there to pick her up every Friday or whatever, like totally got.

Chris Heuer 23:21

Yeah, well, I mean. Yeah, and guilds even longer, and they're all based on the model that we're in this together, and you know, whether you want to go global or whatever. That's why most of our local farm coops, buyers coops and things along those lines as well which are a little less business structure, and more just like if we band together we can get a better price. Right? Become a buying group and things like that. Yeah. So interesting. I'm sorry, I've been kind of rattling

Unknown Speaker 23:55

a number of people. Like if I ever have like enough runway, like what I want to do is basically what you've articulated here exactly, which is the zero profit model. Never designed, which is like also kind of like a D centralizing the like the role of the founder as like the primary owner and then like the hierarchy that comes up. And the importance to me and that is the Yeah, these institutions that we build, especially when you go public, especially when I'm financialized and like have this concept of equity, which can be sold. One of my Like, I literally work in web three, like I was and all of that nonsense. But like the biggest objection I have to kind of the way that this format is if you just simply tokenize and like, the whole point is to sell off as soon as you have this financial incentive of like, my value out as perceived by external people in a way that that changes the incentives. Like it takes your focus away from each other, the more are there in the organization. And perhaps most importantly, a lot of cases, it takes away the focus on society, like both your customers and just the broader effect in your community. And so that's how you have these like boards of companies that are like I am obligated by my function in this board to make the number go up, even if it means like, maybe plan agenda.

Chris Heuer 25:35

And worse than that the short term focus without understanding long term and and then again, one of the things I didn't mention when I stood up but one of the things that Roger McNamee mentioned on Monday as well is to outlaw acquisitions beyond a certain size of say 50 to \$100 million, because it destroys competition. And in fact, most of these acquisitions are done to destroy the competition and not allow the market to work. The way all these capitalist say the market should work freely. A lot of hypocrisy as we know in some of those arguments. Yeah. Any other thoughts questions? So let me just ask this. Please go ahead. And then I got one question.

Unknown Speaker 26:15

Do you see any deals you see here, but I sat in a creative morning's talk last month that was given on a you know, food hall concept is really hot right now. So two chefs both work with Jose Andres, one of them plan, Ferran Adria and Alicia and spean. There is a trending topic is the TLDR but they're opening a food hall cooperative. So it's collective buying while the alcohol one butcher downstairs, they use the whole animal for everything. So they're kind of centralizing that buying process, especially pandemic because so many restaurants had to shut down. Because how do you order with the laws change and in between, and then they're charging their rent on a progressive model so that your success is their success, and they're not trying to price everybody out. So I think this cooperative model is catching fire across all verticals. So I think the industries are ready for it. And I don't know if it's the pandemic just showed us how, how individualism fails. With that kind of bootstrap technique for how you're how you're deemed successful. So I don't know I think it's a catch fire.

Chris Heuer 27:25

Thank you. It's really great to my one of my dear friends on medium rare, and so he put he was one of the first people to put the refrigerators out of the street to have people leave leftovers for homeless and other people walking around so yeah, and they actually are doing Yeah, well and they're doing now they're doing a whole Thanksgiving thing for seniors. Anyways, marks really cool. This is a restaurant in DC actually. A steak and steak fruits restaurant in DC. So yeah, and I went to American so

I spent a lot of time there over the years. Oh, really, um, maybe one, maybe one Click. Click. That's International. Mine was I was undecided. So please

Unknown Speaker 28:14

doubt he's also had a disco disco class. I think having this capacity and it's like website, you can go to cisco.com and I believe that it's like got a manifesto that you buy for guerrilla marketing, basically like a co opted as translation as a service. So there was like a partnership with like, a lockdown or something. But it basically had like a playbook for doing something cool with like, certain language around the different kinds of work that need to go into sustaining that organization to make sure that like, all of that work and labor is compensated appropriately, like not just the translation, but the care work to make sure that the translator has an advantage. Yep. That just thing is really good. It's a little bit.

Chris Heuer 29:12

What's the URL? Let's go down. Just discoteca Thank you. I would hope that you all can stay and talk a little bit more. I'm sorry, I have to run into this client call but I've literally got like 30 minutes to like you know, finish the project that I'm delivering to this guy. So I gotta go do that. But I encourage you to continue to talk and share more and if anyone finds anything else, you know that please add it to the session notes. I've recorded this instead of taking notes because I didn't have friends coming in to do that. So I didn't want to burden anyone with that. But if you have anything else that comes up with any URLs to share, please add it into the session notes whenever you get a chance. And I'm happy to be around for the next few days. So I'll be here through tomorrow afternoon. And in fact, if you're interested, we can meet again tomorrow morning and talk a little further because I'd love to hear more of your feedback and you know more research and things I can include as examples I don't have the book title yet even so. All that stuff. It's just my name Chris Heuer, everywhere. He we are like the Watch Company, and I'm involved with them sadly. Although I'm not allowed to have a lot of like domains and shit because they blocked everything. So I can't even have my own name on stuff because it's, anyways, I really gotta run. There's one last thought I can and whoever else. Oh, there's somebody who made me think of that was really important. I'll think of it again tomorrow. Thank you so much for sharing and we'll talk more tomorrow please. Thank you. Thank you Sorry, Hey, are you around? Are you staying for tonight? Hopefully you're gonna be here. I'll be I'll be here tomorrow too. Okay. Good. Then tomorrow we'll catch up.

Introduction to The Trust Over IP Foundation

Session Convener: Judith Fleenor

Notes-taker(s): Judith Fleenor

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

Home Page

<https://trustoverip.org/>

Join US

<https://trustoverip.org/get-involved/membership/>

Review our newly released Technical Reference Architecture specification here:

<https://trustoverip.org/our-work/technical-architecture/>

Learn about the Evolution of our Stack here:

<https://trustoverip.org/our-work/evolution-of-the-toip-stack/>

Enjoy our interactive Model Here:

<https://trustoverip.org/toip-model/>

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

Permalink to the slide deckL

<https://trustoverip.org/wp-content/uploads/Intro-to-ToIP-Deck-IIW-35-Fall-2022-for-Notes.pdf>

Wet/Naturally Formed Systems (People) and Interaction with Dry/Human Structured Systems (Digital Landscape)

Session Convener: Jeff Orgel

Notes-taker(s): same

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

People are built/designed in nature to exist in a natural realm of forces, none of which are designed or driven by active intelligence or decision making. Naturally formed things evolve to exist in naturally formed realms of convergence between light and dark, hot and cold, rain and drought, fire and ice.

Thereupon, and binding it all together, is a naturally formed atmosphere flexing the beautifully chaotic, yet ordered, fractal flight of “the butterfly effect”. Those effects entangle and dance across the planet every single moment...of every single day...concurrent and bound to each other.

Undeliberate chaos, beauty in natural forces, a structured realm of happenings with no plan or

purpose. This is a complex system of forces, that flows without concern or even awareness of itself.

After a brisk conversation and whiteboard session on the topic my associate Jenn Greene* surfaced an exquisite example by David Sime** (link to full visual below) discussing Digital Twins and VR complexity modeling. Here we see a wet/natural environment, water, being impacted by washers representing dry/intelligently designed influences such. This great gift, mined by Jenn and brought forth by David from RIIoT Digital Ltd***, crystalized the idea of, and results of, the significant influence of dry/design. How does intelligent (dry) design, a washer, in this perspective, software, influence natural (wet) environments, like people?

This “water and washers” visual gave a vivid example of how I perceive humans (wet) being impacted by intelligently designed software (dry). The dance between dry design and wet nature is strikingly beautiful. The demonstration of how we people may be moved to behave in ways we were not designed for is as intimidating as it is beautiful – possibly more so.

How could the influence and sorting out of natural things like people occur with less abrupt reformation of the natural realm by impacts of our own design? How can the influence on people by software occur in a way that is maybe less dramatic? How can the influence on people by software occur in a way that is maybe less malformed? More in April at IIW 36!

Water/Natural & Washers/Intelligent Design = People & Software

https://www.linkedin.com/in/jenn-greene-mcsm?trk=people-guest_people_search-card https://www.linkedin.com/posts/davidsime_cfd-flow-digitaltwins-activity-6950593083998711808-IV4K

*** https://www.linkedin.com/company/riiot-digital?trk=public_post_share-update_update-text

How to use FIDO for everything – As alternative to SAML, as an alternative to OpenID Connect, for privacy-enhanced identification, and for user-centric identity

Session Convener: Francisco Corella

Notes-taker(s): Francisco Corella

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

Slides can be found at <https://pomcor.com/documents/FIDOforEverything.pptx>

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

FIDO is intended for authentication by proof of knowledge of a private key after registration of the public key with the relying party. But in combination with the service worker API, it can also be used for identification with a third-party credential without prior registration with the relying party.

The third-party credential could be a public key certificate, such as an X.509 certificate, that binds the public key to user attributes.

Privacy-enhanced identification can be achieved with a public key certificate that binds the public key to an omission-tolerant checksum of the attributes, enabling selective disclosure by omission of the attributes not requested by the relying party.

FIDO can be used as alternative to federated authentication protocols such SAML or OpenId Connect by having the IdP issue an selective disclosure credential. The Relying party redirects the browser to the IdP, but the redirected request is intercepted a service worker in the user's browser. This achieves the further privacy enhancing feature of unobservability, and obviates the need for the IdP to be always available.

User-centric identity can be achieved using an email address as the identifier and having the email service provider issue a selective disclosure credential augmenting the email address identifier with self-asserted attributes. Other attributes can be provided in by binding them to the email address in attribute certificates.

What do government's need to do to unlock transformation in digital identity?

Session Convener: Gail Hodges, Elizabeth Garber, Wayne @ Spruce

Notes-taker(s): Heather Flanagan

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

See also recording of OIDF Workshop session on November 14, 2022. The workshop included discussion of the white papers underway, including the government and government-issued credentials papers. Recording will be available later this month here:

<https://openid.net/workshops/>

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

1. Who are you, why are you interested in this question?
 1. DHS, Office of Biometric Management - working towards a gathering in the spring where we'll discuss how move towards congress to bring identity to the same level as cybersecurity.
 2. Trust Framework Expert Committee for DIACC - open wallet and understanding how to bring gov't into the conversation at the product level for the development of open wallet fore projects for the Open Wallet Foundation
 3. Recovering federal employee - key partners include national governors association; deal with data around education of the workforce. Desperately think that gov't needs to change, and there's a perception that government is just one thing. There are different types of government and so different avenues available to encourage change. Want to bring technologists to all the types of gov'ts.
 4. Recovering NSTIC participant - domains of identity and identifying where technology can help solve the issues is a thing. Wants to make sure thought leadership is brought in from the work Kaliya has done.
 5. Cirrus Identity - largely working in higher ed, often with public schools and they have to bring credentials there, then at a college/university they have an identity they need to carry with them going forward them. There are lots of stakeholder groups interested in this problem.
 6. Community manager and activist - see the power of clear messaging. Wanted to hear more ideas on how that can be done.
 7. Spruce - a startup in this space; hard to work with any government agency, so would like to clean that up to make it easier to work with the governments
 8. Curity - have government cu stompers in Europe; want to make sure this isn't a US-centric conversation
 9. BC government - much of what they're doing is figuring out how to deploy. Have the capabilities and starting to engage with citizens and corporations, figuring out strategies to use many situations. This includes driving adoption. In relation to this conference, focusing on citizen-centric systems that are not enabling surveillance. If the effort is misconstrued, you can undermine the effort regardless of the viability
 10. Blockchain labs - vaccination codes for citizens in Korea. Want to share their experiences with working with that government, the advantages and resistances they had.

11. CENTRE Consortium - complement of the concern to even out the advantages that large companies might have. Want to promote healthy competition and a reasonable playing field.
 12. MUFG - would like to reduce friction for banking customers (individuals and businesses) and the KYC processes which are grounded in gov't documents. Also to improve the veracity of that information which drives all our policy based rules on what they are and are not allowed to do. Because the government does some regulation, would like to consume better identities to make business processes easier.
 13. Factor - advocate for consumer-facing ability to use identity as a tool to filter what's out there, to protect and filter the info one is getting from and giving to the government. Digital identity as a tool to empower people.
2. What is the potential in this space?
 1. Digital finance would see less fraud and so less cost.
 2. No more standing in lines at government agencies. All your identity documents are in your control. More government services being able to use remotely.
 3. State agencies have had to deal with massive fraud during the pandemic. If California had had a decent drivers license check, that would have been better.
 4. More services and more processes handled entirely digitally
 5. Rather than minimizing fraudulent actions, emphasize enabling actions. There should be automated enablement of your rights.
 6. Need to combine digital identity use cases with the tools we create. A skeleton key that can unlock a variety of services and be suitable for a variety of users. A system of identity rather than a set of endpoint, point-specific solutions
 7. Being able to present digital identity and allowing the ability to selectively disclose the information included. (Data minimization and selective disclosure)
 8. What you say about yourself can be easily validated (to allow for inclusion to employment opportunities)
 9. Let's them rethink the digital relationship between citizens and visitors to a country; people cross borders. Enabling digital services without becoming a surveillance state
 10. We're after an improved quality of life, utilized through your identity, in a public-private partnership.
 11. Cross-border opportunities for investment.
 12. In 10 years, how many people do you expect to see use government-issued identity, after digital identity capabilities are enabled? 20-30% says 80% of the people, 15% says 50% of the people, and many people just didn't raise their hands. BC already sees 50%.
 3. Biggest concern?
 1. Want to make sure that as the government unlocks transformation, it doesn't lock out the current ways.
 2. That we get overrun by conspiracy theorists.
 3. Widening the gap on marginalized communities.
 4. Surveillance.
 5. Control in the hands of hyperscalers.
 6. That they can't be built by little-g governments. (Governments are not software companies)
 7. Politicization of digital identity solutions (weaponizing digital identity by governments; using fear of tech to influence behavior)
 8. Policymakers not understanding anything about technologies
 9. People sense that the information "out there" about them, they don't want to contribute more to it and be further surveilled.
 4. Ideal future? What would a successful pilot look like?

1. As the owner of my own identity, I can disclose only what I want to, when I want to.
2. Want digital identity to be a protective shell.
3. No digital fraud.
4. Mutual authentication and trust.
5. Anywhere you can reduce friction will increase adoption.
6. Organizational use case of proving who they are to individuals. (How do we get organizations to hold credentials? The future of entity identity is missing.)
7. Must learn to do better public engagement to build trust
8. Open, published architectures to encourage trust via transparency
5. How to cross the chasm
 1. The "ideal future" above is how Sweden works. Sweden has generally more trust in their government than the US has.
 2. Don't come up with the first program; come up with smaller so you avoid big bad things.
 3. Support and engagement all the way up; in the government, support all the way to the executive level.
 4. There are already seeds of this in our trust frameworks, public-private relationships exemplified in OIX, OIIF, etc. The development community needs to lean into that and engage at that level to understand what regulations are and engage in a bidirectional conversation
 5. Government has an opportunity to force interop in ways that companies can't. The incentives are against companies driving interop.
 6. Need to have a thoughtful piece that's of value both top down and bottom up.
 7. The privacy rights groups, the digital rights groups, they need to be at the table as well. There need to be someone hired to engage solely with that sector.

What do government officials need to do to unlock transformation in digital identity?

1. Who are you, why are you interested in?
 - US DHS → Congress → critical infra
 - DIACC - gov't product-level engagement (esp OWE)
 - Gov't is not 1 thing → how to target the right part of gov't w/ key msgs + not a US-centric conversation
 - Foundational knowledge (policy + tech), past experiences working w/ gov't rollout
 - BC gov't deployment, adoption - managing citizen perceptions citizen empowerment/control/continuity
 - Fair playing field / healthy competition
 - Consume gov't creds for better KYC / KYC reqs keeping up
2. What is the potential?
 - Remove friction in financial services (KYC), government services
 - Reduced fraud + Maximizing legitimate use of government services
 - MANY more services available online + much more ability for verifiers to verify → leads to more inclusion, e.g. in hiring
 - Systems, cross sectoral infrastructure
 - Selective disclosure - user control
 - Democracy supporting
 - QUALITY OF LIFE ENHANCING, ID SYSTEM / public-private partnership
 - Cross Border opportunity / investments
3. Biggest concern?
 - Inclusive of existing ways of consuming services
 - Overrun by conspiracy theories and/or politicization of everything → actual disruption futures
 - widening gap in marginalized communities
 - surveillance
 - hypercontrol
 - Can't be built well in government / implementation
 - policy makers not knowing enough actual tech to make wise decisions
4. Ideal future? // Use cases / Solutions
 - Tools to maintain + selectively disclose my data
 - Orgs held accountable to prove trustworthiness to individuals
 - Electronic medical records
 - Large-scale public engagement (BC)
 - Open architectures
 - Non-uniform successful online financial
 - Individual participation in care decisions
 - Sweden
 - No digital fraud - VAW!
 - We have power to verify verifiers - mutual authentication
 - reduced friction breeds adoption - offers great use cases / examples → control narrative
5. How to cross chasm?
 - Government needs to build more trust
 - Not big bang - smaller rollout, flywheel style
 - Wholesale support for select use cases (not pet projects)
 - Nonprofits as bridge for pub/pr partnership - including privacy rights groups
 - make sure development community understands val prop
 - Private interoperability (govt opp)
 - Educating those groups who are programming + architecture

IIW 35 Trust Registries - A Meta Network Approach

Session Convener: [John Walker](#), [Savita Farooqui](#)

Notes-taker(s): John Walker

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

GCCN, TRAIN, DNS, DNSSEC

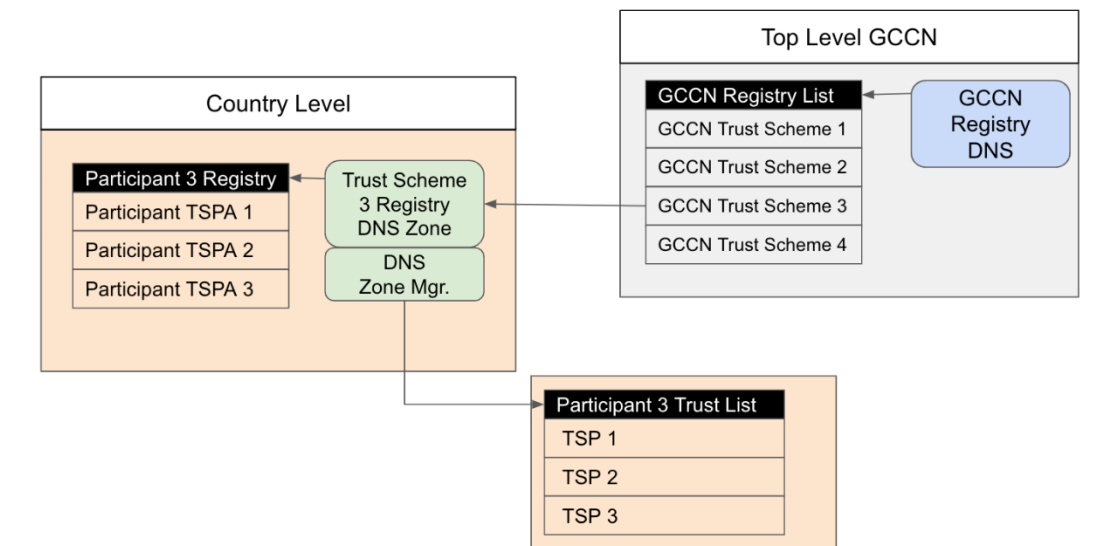
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

The Global Covid Credentials Network - "GCCN" - An example of a Meta Network Approach

IIW 35 Trust Registries - A Meta Network Approach

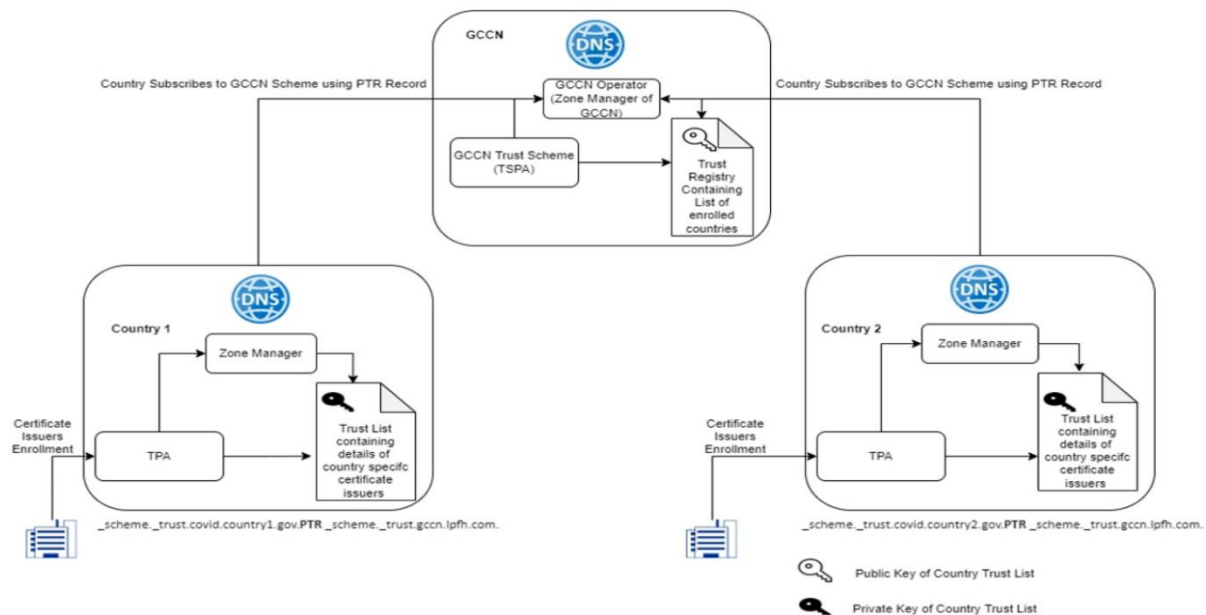
- What is a Registry? Why do we need one?
 - Determine who to trust - trusted issuers, verifiers, others?
- Global Covid Certificate Network (GCCN)
 - Working with UNDP and other UN Agencies to establish a global registry of registries for trusted issuers/health service providers

IIW 35 Trust Registries - A Meta Network Approach



- A set of signed “Trust Schemes” → Trust(ed) List
 - An example of an established standard: ETSI TS 119 612
 - [TS 119 612 - V2.2.1 - Electronic Signatures and Infrastructures \(ESI\); Trusted Lists \(etsi.org\)](#)
- Accessible Secure ‘publishing’ of such a list → DNS with DNSSEC extensions
 - Projects supporting the publishing of secure trust lists - from eSSIF Lab :
 - LIGHTest
 - <https://www.lighest.eu/>
 - TRAIN
 - https://gitlab.grnet.gr/essif-lab/infrastructure/fraunhofer/train_project_summary

Trust Registry - Leverage DNS / DNSSEC to publish ‘Trust Scheme’



- What roles are required to operationally support Trust Scheme publishing?
 - Network or consortia operator
 - Scheme Publisher (country)
 - Scheme Participant (service provider / issuer)
 - Participant onboarding and verification
- Metadata standardization
 - Network operator information
 - Trust scheme publisher (country) (registry operator at the next level in the hierarchy)
 - Health service provider (issuer) metadata
 - Service information
 - Service operator information
 - [User Roles and Flows](#)

- Governance / Business Rules
 - Issuer
 - Verifier
 - Jurisdiction / Regulations

Questions, please feel free to contact us:

- John Walker : www.linkedin.com/in/john-walker-32b40117
- Savita Farooqui: <https://www.linkedin.com/in/savita-farooqui-b8812b1/>

Show Me The Money (Business Models of Identity)

Session Convener: [James Monaghan](#), Zack Jones

Notes-taker(s): Ankur Banerjee

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

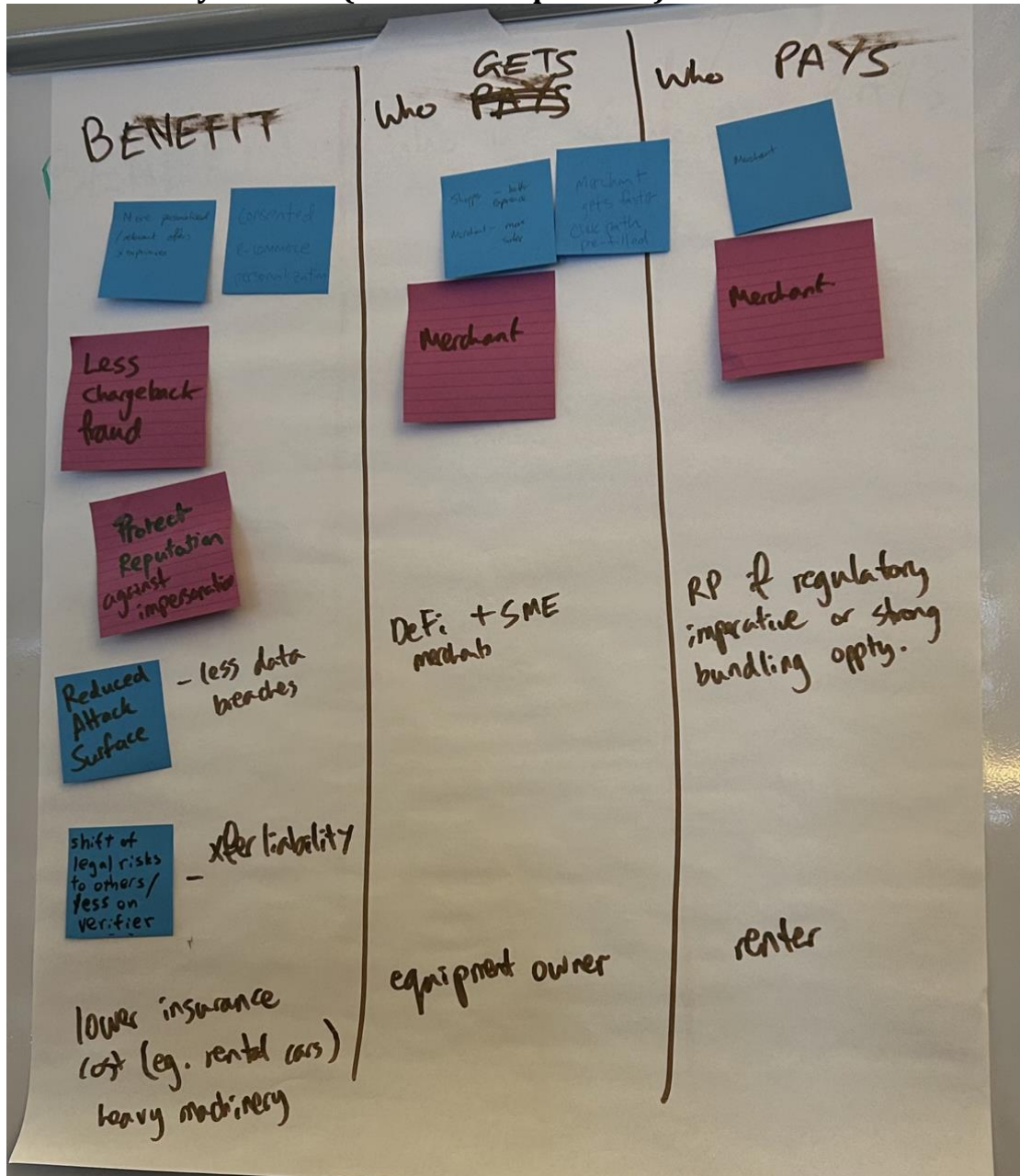
Discussion notes

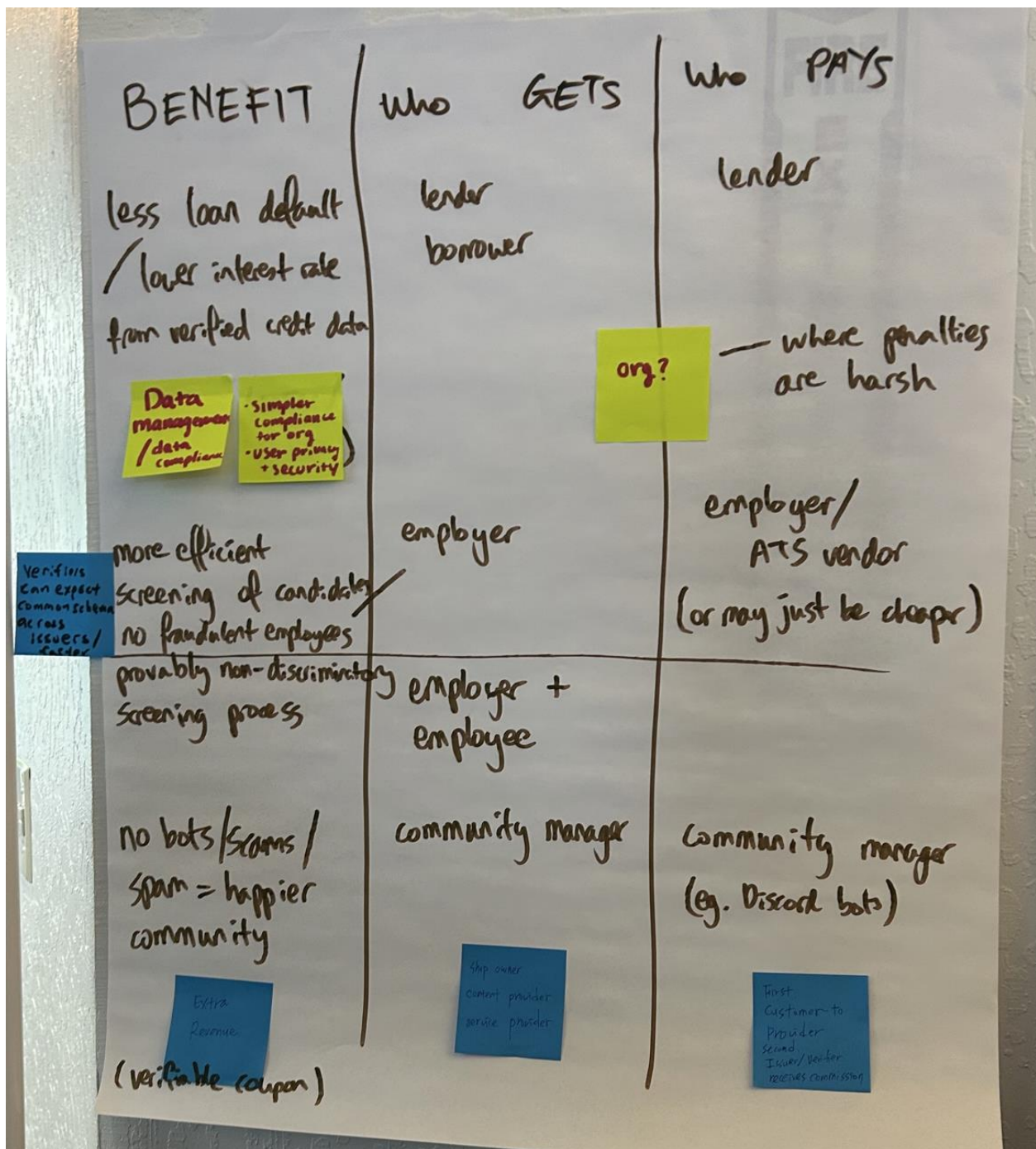
1. Ecommerce
 1. Customisation, e.g., this is my dress/shoe size, why do I need to enter it again and again? Can I just pass the data to ecommerce site and show curated results.
 2. Or, I want to buy a gift for my friend/sibling/spouse, and don't know their size/preferences.
 3. Fraud loss prevention:
 1. Scammer buys an expensive item (e.g., TV or iPhone) using a stolen credit card
 2. Ecommerce site sends the item, but after a few days gets a chargeback. Net result: they'd lose the item *and* the money.
 3. Friction for doing a traditional ID check is too high in ecommerce, i.e., selfie-scan-check would be too cumbersome.
 4. Cheaper/faster checks to know if it's a real person living at that shipping address will be valuable.
 4. Some ecommerce outfits prefer to NOT process credit data and outsource this to external payment processors to reduce their PCI-DSS risk.
2. DeFi
 1. DeFi marketplaces won't really do or pay for KYC unless compelled by regulation.
 2. However, smaller marketplaces will do some form of check to reduce
3. Background/employment checks

1. If there's a regulated profession, then reducing the cost of background checks or reducing risk might reduce costs of insurance.
2. Fundamentally, risk management to reduce costs
3. Verifiable education and employment history
 1. LinkedIn is considering this?
 2. Can be used to prove DEI hiring goals are being met
 3. Removing bots from applications, since companies get inundated with fake applications
 4. Maybe this can be integrated into Application Tracking System (ATS) software for better sorting and verified history
4. Financial institutions
 1. Better, more comprehensive credit-scoring or loans data rather than what's reported by the credit bureaus
5. Healthcare
 1. Covid credentials
 1. Venues did NOT want to know personal details, vaccination dates etc.
 2. However, some employers WANTED to know
6. Community moderation (e.g., Discord, Telegram)
 1. Reducing spam bots and low-quality spammy users
 1. Mostly this is done using CAPTCHA checks right now but this is less likely to catch low-quality *human* spammy users
 2. A lot of large communities on these platforms already pay for software tools for automated monitoring and flagging, as well as pay for human moderators
 3. Knowing through a credential that a user is authentic and high reputation can be extremely useful.
7. Open source software
 1. Highways etc are built as a common good and funded by the government. Is there a similar example of this in software?
 2. Government pays, because it's a public good
 3. Companies fund a lot of software since it reduces their cost and embeds their idea

(whiteboard captures continued on next page)

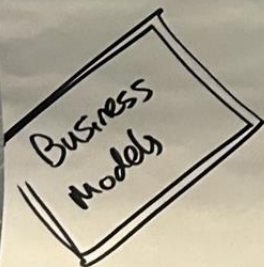
Benefits analysis table (whiteboard pictures)





| Benefit | Who Gets | Who Pays |
|--|---|---|
| <p>cheaper/more</p> <p>faster onboarding of new FI customers</p> <p>less unemployment fraud</p> <p>greater control of policy by govt.</p> <p>defends my monopoly</p> | <p>(receiving) FI</p> <p>monopolist</p> | <p>FI</p> <p>big cos / cabals / etc</p> |

| BENEFITS (not actions) | WHO GETS the benefit | WHO PAYS for it (& how) |
|--|--|---|
| cheaper KYC regulatory compliance | RP pays less, faster for user | RP, possible rev. share to some others membership of network |
| control + auditability of rights | creator | licensee or creator (via commission) |
| less counterfeits in supply chain | brand (max. equity) buyer (not defrauded) | brand (buyer w. ESG premium) |



Can SBT (soul bound token) be a practical tool for identification

Session Convener: Kana Paek

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:

- SBT is public. It is not good as a medical license.

- A medical licence could be an example of a SBT since it is non-transferable, its about a single entity and can be revoked.
- Since SBT's can be recovered through community, there was a question on how is a community defined

Discussion topics

1. In what salutations will SBT be utilized the best?
 1. What type of data is suitable to be stored in SBT, since we don't want too much PI
 2. CivicIdentity.com along with other companies work on a KYC pattern to be used for many different use cases such as financial loans so it could be used in parts with SBT
 3. What information can be associated with SBT: potentially biometrics such as the driver licence, and the other is non-biometric information like someone is over the age of 13 years
 4. There is no single authority that is checking only one SBT is given to single entity so the potential to trade will impact the value/benefit
2. Can SBT be a reliable identification tool in decentralized society?
 1. Question: Who is liable in a SBT instance?
 2. VC operate around the idea of a known issuer, but with SBT it does not solve the problem of the issuer
3. Can SBT be Money in credit economy?
 1. No they are non-transferable doesnt protect from double spend problem
4. I believe that SBT is the most effective way for web3 or "decentralization" concept to mass-adapt. What do you think?
 1. SBT can be used for low-level things like proving you're not a bot
 2. Someone could sell their SBT (private key) for money and one could collect souls
 3. There is no one to one mapping with an actual soul to the token
 4. If it is non-transferable, why is it being put on a blockchain - its too expensive
 5. Putting all my credentials on a single -- could create a correlation risk
 6. SBT was proposed to include some PII but its public for everyone to see.

Ask A Federation Operator

Session Convener: Nicole Roy (InCommon)

Notes-taker(s): Dmitri Zagidulin

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

Federation, SAML2, InCommon, IdPs

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

InCommon runs US single-sign-on federation, for authentication and global WiFi Roaming.

(Demo of InCommon's Metadata Explorer Tool)

InCommon was created by Internet 2 (CIOs of universities etc) to do a single sign-on federation. (Legal structure, governance, policies intended to create trust among the participating institutions).

REFEDS (refeds.org) - Research Education & Federation Governance group (worldwide)

eduGain - Global querying service for Web SSO

eduRoam - global WiFi Roaming service. (Connects educational institutions, regional/state networks, libraries.)

InCommon community produced a number of open-source software projects (& Docker containers)

Also provides training (on how to use all those) - <https://incommon.org/academy/>

Q: How easy is it for a random Relying Party to put up a 'Sign in with InCommon' SSO button?

A: Quite easy (examples with community newspapers, etc). (Demo -- 'Join InCommon' link)

Eligible - Higher ed, Research organization, or (if you're a commercial org) as Sponsored partners (a lightweight process).

Highlight - An RP can request that an IdP requires a particular auth security context (for example, require multi-factor auth). (Progressive step-up auth is also available.)

Change management (for giant federated systems) is incredibly challenging. (If you introduce a new protocol or feature, it takes a long time for it to be deployed/propagated).

Issuing to Orgs for fun and profit: Watch us do Multisig KERI, GLEIF, ACDCs, and all that Jazz

Session Convener: Daniel Hardman

Notes-taker(s): Daniel Hardman

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

Provenant is a small start-up in the KERI/GLEIF ecosystem. Previously, GLEIF has demoed various things in that ecosystem, and Sam Smith (the inventor of KERI) has also demoed. However, the technology has been very young. This session was an hour-long demo of Provenant using production tools to create KERI identifiers (AIDs, which are a specialized form of DID), to authenticate other parties with those identifiers, to setup a multisig scheme for officers of a company to control an official corporate identity, and to delegate authority to an identifier.

The scripts that we demoed are mostly located at <https://github.com/provenant-dev/vlei-qvi>.

The steps we went through in each wallet include:

- create-local-aid
- generate-oobi
- resolve-oobi
- generate-challenge
- respond-to-challenge
- multisig-shell
- multisig-incept
- multisig-join

SESSION #10

DID Comm/OpenID & VC Comparison

Session Convener: Sam Current, Torsten Lodderstedt

Notes-taker(s): Neil Thomson (after photo)

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

Crowdpleaser!!



OIDC/DIDComm throwdown Sam Curran v Torsten L

For the purpose of exchanging VCs.

Can from a discussion in Dublin about DIDComm and other communication channels.

Looking for feedback and questions of better understanding of both ODIC and DIDComm.

Really need the slides
Sam Curran

Message example DIDComm V2

- Type of message - created from a message family then version and message within the family
- From, to, expiry time
- Message and attributes of the message

Both of parties have DIDs and DID Docs

- Each as an endpoint for DIDComm and what is supported : endpoint DIDCommMessaging
- Have routing keys, etc.

Information sufficient to send to the other party

If you don't know the DID for the channel, Alice creates an invitation to Bob with the DID, etc. so they can interconnect

Receipt of a message can be delegated to a mediator (e.g., server) by the DID owner

Encryption to protect delivery target and the content.

Sender does not need to know about the mediation of the receiver

No concept of a session, but there is a thread (connected messages)

Peer DIDs do not need to be written to a ledger.

Can add your own protocol within a DIDComm channel without any dependencies other than to provide information to the recipient to know what protocol is being used.

DIDComm is not a broadcast tool - peer/peer - pushed out for future consideration

Torsten L

OpenID for Verifiable Credentials (OIDC 4)

Specifically designed version

Issuance - simple OAuth API - all OAuth 101

So for authN/authZ - can use any OAuth workflow.

Interface between issuer and wallet

Can use all the common VC cred formats.

Interaction model assumes credential user interacting with a wallet

Alice connects through wallet via OIDC for VCs to Issuer, that authenticates the user and provides the VCs back to the wallet.

Verifier is a resource which you would use an auth token, which the service can then request those from the user's wallet via RP requests. This includes different disclosure/presentations.

Can support within same device and across devices

OIDC and DIDComm - are comparing apples and oranges. They are both fruit (claims Sam Curran)

The interaction on VCs is determined by specific exchange information (including the keys used to sign the VC, type of VC and other VC specific parameters). This is how this version of OIDC is different than standard OAuth 2.X underlying ODIC.

The OIDC model does not have a preferred communication channel.

DIDComm supports presentation of VCs as you can add protocols within the DIDComm channel to do so. Otherwise DIDComm is just a secure communication protocol channel.

The DIDComm model allows establishing authN/authZ and then that is associated with the DID pair (the two parties), so you don't need to re-auth for each message.

With DIDComm can map an LEI to a DID and as the LEI is public, the DID (may be) public as well, so it is possible to create a connection directly to an Issuer without needing a DID search or lookup service.

OIDC could use DIDComm as the communications channel vs. HTTP(s)

If the OIDC user provide includes a DID then one will be issued. However, in OIDC DIDs are not the mechanism for identifying the endpoints to communicate through. Set the point above on OIDC/https

DIDComm - the DIDS for communication are likely different that in asking for VCs that the DIDs involved are likely different (e.g., DIDs strictly for the DIDComm channel are likely not the ones used for general online transaction. Channel DID vs Entity DID.

OIDC and DIDComm (and any protocol are both heavily dependent on (configuration) metadata

Assumption is the OIDC issuer can also be an authorization server (OIDC Server) or may just be a service (AuthN/Z with an other OIDC server)

Need common binding elements between OIDC and DIDComm to mix and match.

Multi-protocol future - yes. For bridging from new to old. For legacy or change resistant ecosystem backwards compatibility.

Reality - these are two different protocols for different purposes.

“Don’t cherry pick your favorite privacy characteristics and say “PRIVACY”

Session Convener: Nat Sakimura

Notes-taker(s): Heather Flanagan

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

- <http://oecdprivacy.org/>
- <https://bit.ly/3EFdqw5>
- Links to slides:
<https://docs.google.com/presentation/d/1qsdhjdJPhgwOiHxIkSRiqYrzLoUoLwLi0-KHRY0pbF8/edit?usp=sharing>

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

[Nat has a slide deck]

Most of the privacy regulations around the world are developed from the OECD Privacy Framework

It is very common practice for people to cherry-pick their favorite privacy characteristics (e.g., unlinkability).

Overview:

1. What is OECD privacy guidelines
2. Relationship among OECD, Legislation and ISO
3. Overview of ISO/IEC 29100 privacy framework
4. ISO/IEC 29100 and related standards
5. Example: where would “unlinkability” fall in the framework?

OECD is an inter-government organization among developed economies. It is sometimes called the “Rich Man’s Club” which means it’s low on the diversity scale, but on the positive side, you can receive the greater common denominator.

OECD create legal instruments which member countries are bound to implement them in domestic legislation (e.g., GDPR, state-based legislation, etc). OECD then monitors the fact that the governments have implemented as required.

First OECD privacy guidelines were published in 1980.

Privacy is not about secrecy. It’s about having control in expressing yourself.

How does one determine if obstacles are justified? That’s subjective and possibly culturally based. If enough country feels something isn’t justified, they’ll create new agreements. Example: GDPR makes it difficult to ship the data to countries not deemed “sufficient” wrt privacy protection (like the US).

Does the OECD public compliance reports? They publish progress reports; not sure if all the figures are made public. It is shared within the OECD participants, but sometimes shared only as “room documents” on paper only available in the room.

Privacy Principles

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
 1. This one is often violated
8. Accountability Principle

Relationship among OECD Privacy Guidelines, Legislation, and ISO standards

OECD feeds government regulations, including GDPR and many others, including Japan act on personal information protection.

- Note that Article 42 on certification points to ISO/IEC 27701 PIMS

OECD feeds ISO/IEC29100 standard which informs industry. This includes standards on 29134 - PIA, 29184 - Notice and consent, 27551 - Unlinkability, 27701 - PIMS. It also informed OIIC (created parallel to 29100)

Overview of ISO/IEC 29100 Privacy Framework (see bit.ly link above; it is available for free at the right link, though they will let you pay for it if you insist (and go to the wrong link))

29100 defines four actors (PII principal, controller, processor, and third party) and two roles (PII provider, recipient). Note that the principal and controller may be the same entity (but not necessarily). What's the difference between the third-party and a controller? The third party makes its own decisions on how to handle the data. Processors cannot make any decisions and only acts on instructions from the controller.

In discussing SSI and the “evils” of the IdP model, that's because the IdP is the PII Controller and can make its own decisions. If the IdP were the PII Processor, the story would be completely different as it would be required to do what the PII Principal/Controller wanted. The same model will actually apply to the wallet. As soon as the wallet becomes a Controller, we have the same challenges as with the current centralized IdP model.

There is no enforcement teeth on the controllers. That's a huge risk. From a regulator point of view, decentralized is a huge headache because it's not clear what to regulate.

ISO/IEC 29100 also talks about interactions (8 scenarios and role of actors), recognizing PII, privacy safeguarding requirements, privacy policies, and privacy controls.

Privacy safeguarding requirements cover legal and regulatory factors, contractual factors, business factors, and “Other factors” that influence privacy risk management.

ISO/IEC 29100 privacy principles include 11 different principles

1. Consent and choice — OECD 4 Use Limitation Principle
2. Purpose legitimacy and specification — OECD 3 Purpose Specification Principle

3. Collection limitation — OECD 1 Collection Limitation
4. Data minimization — OECD 4 Use Limitation
5. Use, retention, and disclosure limitation — OECD 4 Use Limitation
6. Accuracy and quality - OECD 2 Data Quality
7. Openness, transparency, and notice — OECD 6 Openness
8. Individual participation and access — OECD 7 Individual Participation
9. Accountability — OECD 8 Accountability
10. Information security — OECD 5 Security Safeguards
11. Privacy Compliance

Companies that have done ISMS have privacy components; 27001 certification includes 29100. Security management system is about controlling the risk for the organization. In the case of privacy management system, it's about managing the risk of the principles.

Certification is a big deal in Singapore.

ISO/IEC 29100 and related standards

| ISO/IEC 29100 Privacy Principles | ISO Standards | OpenID Connect |
|--|--------------------------------|--|
| 1 Consent and choice | ISO/IEC 29184 ISO/IEC 27556 | prompt=consent |
| 2 Purpose legitimacy and specification | ISO/IEC 29134 | policy_url |
| 3 Collection limitation | ISO/IEC 27701 | scope/claims, PPID, ephemeral sub |
| 4 Data minimization | ISO/IEC 29184 | (RP management. |
| 5 Use, retention and disclosure limitation | ISO/IEC 27555 | Documented at policy_url) |
| 6 Accuracy and quality | ISO/IEC 27701 | (realtime nature, trust framework) |
| 7 Openness, transparency and notice | ISO/IEC 29184 | policy_url |
| 8 Individual participation and access | ISO/IEC 27701 | (OP and RP policies) |
| 9 Accountability | ISO/IEC 27701 | (Trust framework) |
| 10 Information security | ISO/IEC 27701 | formal verification, (Trust framework) |
| 11 Privacy compliance | ISO/IEC 27701 | (Trust framework) |

One has to fulfill everything on the list, not just a few. The challenge is there is no way to police/enforce compliance, though ISO/IEC 27701 helps by defining the trust framework model, and countries may have specific legislation.

OIDC explicitly left out offline cases; would like DID to solve for those. (See also notes from this morning's Session Management session at IIW; Session 6 M)

What about unlinkability?

"Protocol itself is said to be unsinkable if its executions cannot be linked, given explicit settings for the adversary and target entity role."

RP + AP -U = unlinkability

RP + AP is the adversary and U is the target entity

Document describes eight notions of unlinkability:

| Notions of unlinkability | Adversarial role(s) | Target role(s) | Explanations |
|--------------------------|---------------------|----------------|--|
| Passive outsider (PO-U) | PO | U | Attempt to track U across authentications while these are being monitored (read-only) |
| Active outsider (AO-U) | AO | U | Attempt to track U across authentications while these are being controlled (read-write) |
| RP-U | RP | U | The RP attempts to track the U across authentications. (anonymous) |
| AP-U | AP | U | The AP attempts to track the U across authentications. |
| RP+AP-U | RP and AP | U | The colluding RP and AP attempt to track U across authentications. |
| AP-RP | AP | RP | The AP attempts to track the RP across authentications. (Tracking by an IdP) |
| AP-RP-U | AP | RP and U | The AP attempts to track the pair (U, RP) across authentications. |
| RP+RP'-U | RP and RP' | U | Colluding RPs attempt to track the U across authentications. RP may be able to track U in transactions with RP, but cannot track the same U communicating with RP'. (PPID) |

(source) Based on Table 1 of ISO/IEC 29551

Note that that rigor for unlinkability only talks about one part of collection limitation; there's so much more!

The incentives for privacy have to be aligned between business bottom line and regulatory (but unenforced or unenforceable) requirements.

Does cherry-picking happen because of ignorance or is it a purposeful decision? Both.

Privacy Enhancing Mobile Credentials = Continued

Session Convener: John Wunderlich

Notes-taker(s): John Wunderlich

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

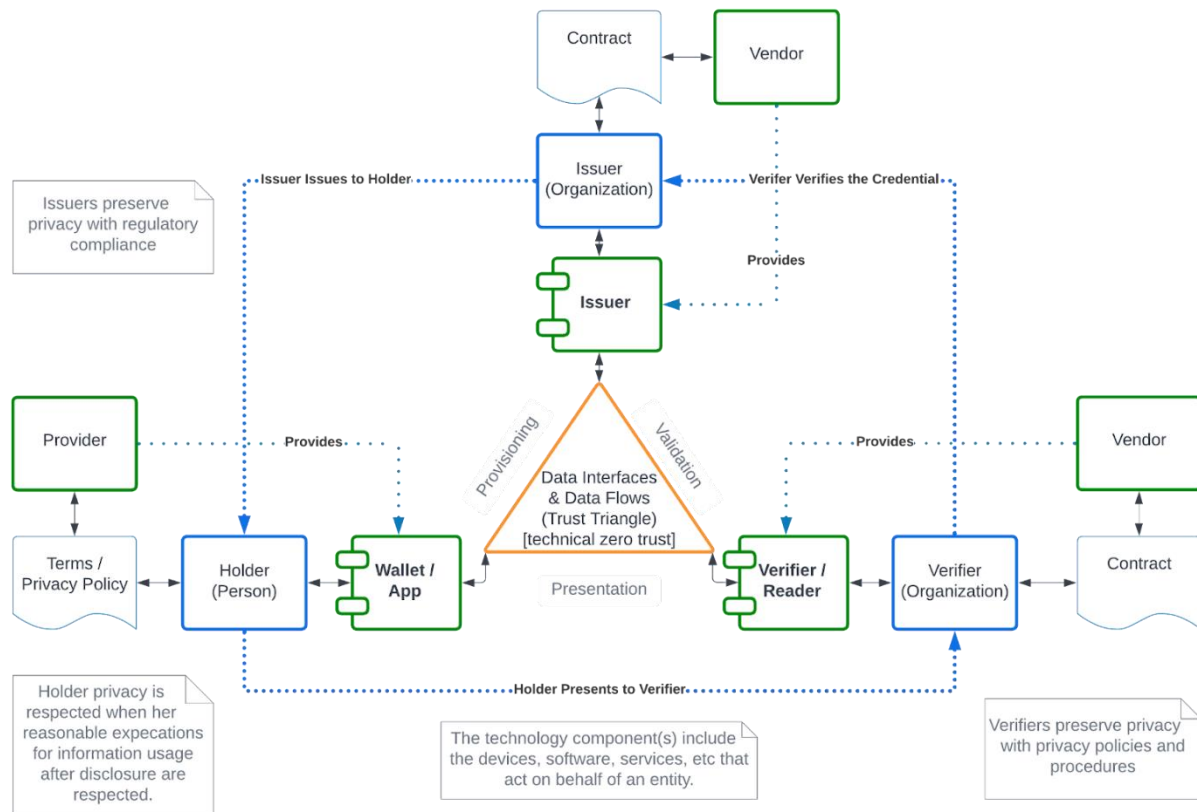
<https://kantara.atlassian.net/wiki/spaces/PEMCP/overview>

PEMC Draft Early Implementors Report (WIP Commenter Access)

https://docs.google.com/document/d/18gNx9wcE6-8o9K9usv085KCPpWLuPOQjGTekpII_cA/edit?usp=sharing

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

Diagram below summarizes the whiteboard discussion



ID Scheme Landscape: What are the leading Identity schemes/Frameworks/Models being worked on in UK, EU, US, China

Session Convener: Michael Becker

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

Roger & We: Collective Action for Collective Action

Session Convener: Chris Heuer <https://linkedin.com/in/chrisheuer>

Notes-taker(s): Otter.ai (and Doc Searls)

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

#Activism #EndSurveillanceCapitalism #Movement #CollectiveAction #Community #DigitalRights #UserRights #HumanRights

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

[Audio Recording on Otter](#)

Request Access to our Signal Group:

Leave your phone number here, or give it to one of the existing group members in tomorrow's session

ACTION: Submit here, drafts for a simple change.org petition

- End Surveillance Capitalism: People aren't just being exploited for exploitative corporate profits, they, and our whole society are being harmed. It's time to end the efforts to make trillions of dollars of profit off of our data, our rights, and our very lives.

An initiative of the Customer Commons and the Internet Identity Workshop.

-
- ????

TRANSCRIPT:

Chris Heuer 0:00

Bring him here to that was about exposing more people and getting them to sense the energy

Unknown Speaker 0:06

to come anyway cuz you could actually hang out in the closing circle and say something yeah think circle which I thought would be pretty cool. Absolutely dial in yeah

Chris Heuer 0:21

oh yeah could do that hey welcome drew

Unknown Speaker 0:24

my sense is he's gonna fly in and come straight from the airport I'm coming in sometime in the afternoon just straight use very, very like I'll do what I think I can

Chris Heuer 0:39

well again what is the what are the things that you know we've all heard maybe not all of us but most of us have seen our or cause driven friends tilting at windmills for many years and getting tired. Yeah. And so that's where he's at in this whole thing. I was really shocked to hear were the first people who responded with any energy to what he said. But I do think that it is a post COVID realization as sort of the world's at war and sort of, you know, shits failing. So, you know, Tony Robbins quote that I've always leaned on over time Well, we, we did that and they closed they don't want to hear

that but the Tony Robbins put out is gonna reference a very simple one. When we succeed we party. When we fail, we ponder and so I think that kind of describes the overall sort of situation that we're in as a world right now and more people see it. So there is literally an awakening going on right now to the new potential in our need for coming together and developing new models for doing this and our need to free ourselves from, you know, many calls, being slaves to corporations or being exploited by them or any other way you might say. And so it's a really big moment to do that. And so in looking at the things that are going on, right now, the proposal here for this group, and I'm gonna start with that and then want to hear from everyone around this a little bit is is this and I'm trying to form this in my head a little bit. I shared some of it yesterday at the closing circle, but I believe that what we can do is a really interesting a quick project that we could stand up here, you know, in the next few days, actually, if we wanted to, it's not going to be perfect. So you know, that's all fine. We got to you know, be willing to not let perfect be the enemy of the good and what it would be would be a really core pledge for the members of this community to make to privacy, openness, and literally, I mean, you know, three, four points, not getting into everything. It's not going to cover everything. It didn't need to be rewritten over time. And that sort of stuff if we're to expedite our path forward, but that the signing of the pledge would allow those companies within this community to be included in a directory that upholds the standards and are representatives of the broader movement in this direction, towards a world in which we take back control of our data in which we remove or we remove the shackles of the tyranny of convenience and you know, the many other sorts of phrases that we can pick on and look around. Um, give me one second. Let me put out a proposal and then we'll talk about it and we'll get from there. And so that's, that's step one. And what we're actually doing as part of the call is relating to our conversations last few days. We don't know where things are going, you know, there's been 10 posts in the past week or the end of social media. So that's the other angle of something that's happening right now. But the idea of tapping into the Twitter and Facebook employees have been laid off and bringing them together and taking this moment as an opportunity to shine a light on all the good work happening out of the last 35 sessions and out of the 18 years almost of conversations and lists and meetings. And everything else. I think it's really going to be very impactful to that. Because it's not just something that just came around. It's something that's been developed and all the great people are in this space already and then working together. So second component of that is the call to get people to download their data, opt out of GT GDPR unnecessary cookies, and just to raise the understanding of, hey, it's not just those little actions. This is a bigger surveillance capitalism problem where we're being exploited and to let Roger tell his story of how he does. So we don't even need to necessarily stroke

that all out other than to say, tell the exploitation story. Let's seize the power back and tell your story because you do that. And then the third component of which is coming back to the Facebook and the Twitter layoffs. And what I landed on was, we're not, we're not going to be able to agree on well what we need is the next great personal media app or networking app or personal data palettes even at this point, we're not all going to be able to agree on that. So we need to both get enough of a direction that there's an invitation that if they receive it through media, or friends or anyone else or as we talked at the end of yesterday was then were you there, as we talked the end of yesterday getting some of the early Twitter founders to actually promote it. They don't even need to go on press, they can just promote it to their networks, right. And so we don't need them to risk themselves too much, but to invite them into an online open space. I'm actually thinking December 1, because we need to move quick in order to seize this like little moment. Also, because a lot of these engineers hopefully will be working again soon and full time jobs. And many of them have the ability to invest into causes and these sorts of efforts. But what happens is is when we invite them to an online open space, you know, as here, I'd set up a little more structure around some of it, but the main intent is we'll let everyone else come together and figure it out. Everyone present certain solutions and to have those conversations, but we can actually structure an open face it like firstly is exploration of what's out there with what it is and the problems that we saw. In fact, that's why the invitation as I wrote it previously, was let's see if I can get this right off the top of my head. We invite you to help us explore what went wrong. And to fit I'm sorry, into and to discuss the there we go and to ideate and move towards the something better that wants to emerge. Because there is something better that wants to emerge and all of us have ideas of what that is, but we're describing the elephant. And so join

Unknown Speaker 7:02

us to figure out what went wrong and define something better that wants to

Chris Heuer 7:08

cool. A plugs that we all put together and then that leads to a directory site of companies who worked with these values. So that when we make the call out and the broader press picks it up, they can come in subscribe on a mailing list through all that stuff and that we can stay in contact with them. And we're building the basis of a grassroots movement with the people who care about this and might not be developers. The second component was the Baba Baba. The proposal to do what did I say? Well, that's the third one that I was gonna go with

Unknown Speaker 7:46

to do. It. offline events.

Chris Heuer 7:48

Yeah, definitely do do the online open space to convene the developers to work on what it is behind it. And this is important because if I didn't convey it, and the fact that I don't remember it doesn't mean that you don't really have the directory so maybe that was it. Maybe I combined the two. My first question

Unknown Speaker 8:08

is there's two organizations coming my data, which has a declaration that one can sign in as there is a list of companies and has been for a while that have signed a declaration and I think the declaration would be more or less the same as would probably have and then the most More recently, the collaborative technology around alliances as a declaration, but you don't think there's companies behind how you say this is different. Why do we need

Chris Heuer 8:34

well then then because so one of the things to consider

Unknown Speaker 8:37

is for this highly high overlap call of these organizations. already.

Chris Heuer 8:41

So then maybe because of the intersection that's created here, that this is the aggregator of aggregators, and it's not that we're competing with those other organizations or pledges, but amplifying them in the same way we're amplifying the law that you can download your own data and that you own it, and everything else. So let's point to the available resources people and organizations who back the valley there's a bunch of things. And let me be clear, again, that's the proposal because I you know, that's just where I'm at. So none of it needs to work. That way or anything duck.

Unknown Speaker 9:18

What went wrong thing? I don't think there's much doubt about what that is. I think we were already there. I think a bias for action is the bigger thing. I think that's the right thing for, you know, like, let's, let's let's minimize this Sisyphean. Part of this. Okay, right. And this is always the part where you're pushing a rock up the hill, you want to have a snowball going down the other side. How do we make the snowball rolling down the other side? What is going to be the most has the highest coefficient of adherence for the snowball to grow on themselves. So a couple of things about that. years ago in a conversation with Tim Juan, who wrote one of the many books, too many books in that advertising, about how it sucks to be affiliated with Praful con but he is the awesome foundation you started oh cool and the idea of party with you awesome fetish these other things are no complaining. Just what's constructive. What did you know this is barn raising shit. Just to switch metaphors. You know, what can you add to the snowball? So So homeless is a design in principle we're looking to do this constructive. With that goes somewhere, even if where it goes to is we're gonna fuck these big companies. But I think rather than fucking the big companies, they're they're all facing an existential partially existential thing right now, which is, you know what this all is tracking based advertising not only avoid the shit out of people who was morally compromised, to say the very least, it actually didn't do shit a lot. It really wasn't very good. So we average life expectancy in the CMO chief marketing officer is nine months before they go on to the next one. And this is one of the many tools it takes 18 months more than average the cost of nine months to play out. So you're gonna be firing a lot of these people. Okay, and so what what do we do as constructed what is we do that that's how do we replace tracking? You know, I really like what done done. About half the road. In his book, app and scan, is concluding chapters, just ban tracking, but that waits for regulators to do that takes too long. Make it so socially Outcast as it were, at the same time, as we're, you know, there are better ways to communicate with people listening to those, you know, or they communicate with you. And all this stuff has been on the table for a long time. So another piece is that there is a privacy manifest that we've had sitting at customer comments and project pireenne For the last eight years, something like that. It's not bad. It's in a wiki. It can stand improvement. So

Unknown Speaker 12:19

these choices. Cool, cool.

Unknown Speaker 12:25

I was just gonna add to that the snowball notion I think is served by you know, incorporating and not not trying to be the one to organize them all or anything but incorporating the collaborative Technology Alliance and my data and ch T and, you know, eff in terms of like, pointing at and all the platforms and nascent platforms that are doing things in this area, pointing out as many of them as possible, inviting them to join and trying to build a move, you know, we're talking about movement building, as opposed to organization yessing where you have, say the environmental movement or the civil rights movement, or, you know, whatever movement has many organizations with little

differences around the edges, but, you know, we're trying to get people to buy organic, you know, at the supermarket and and we're saying here are a bunch of labels that say organic and to that and one of the things that we've been talking about in the sketch t that I'm sorry, the CTA, the clever technology last is is doing labeling that is you know, adversarially interoperable, you know, essentially being able to label both ourselves and a platform like, you know, Facebook or Twitter or tick tock or, or Instagram to say, Okay, open source, no, advertising free No, you know, this, yes, this No, and so that there's a comparative thing for people to look at. And we can hold ourselves to those standards and and just be you know, there. There are things that are otherwise great but happened not to be open source. Things that are, you know, I smelled the nutrition label. Yeah, that's what we call.

Chris Heuer 14:29

Yeah. Oh, that's great. And I think again, just the idea of having a scoring system, and again, the call yesterday he was talking about harms, like just gathering all the harms that are that are people suffering to be able to identify some of that

Unknown Speaker 14:44

a little bit behind. So is the output here because I missed the first session. So is the out here a, like some sort of standard business practices? And if so, like, are we kind of more targeting the labor side of things or about more of like a structural businesses are doing with, you know, such and such.

Unknown Speaker 15:13

Jump is, the idea is to stop surveillance capitalism. That's like if we could just say, We're signing on to stop surveillance capitalism. And these companies are all in favor of stopping surveillance capitalism, so you're automatically a good guy. If you sign on to stopping it. You're not doing it on your side. That's fantastic. Be like a simple thing like that. You know, these are the individuals that want to stop it and he these are the companies that want to stop and and just just to list like, also Train Manifesto when it was out, it's like, we've got all these signatories. Right? And if they were some were individuals, software companies, some or whatever, but you just say what it is you're trying to do. Yeah. And I think rather than saying all the thing, you know, own your own data and all the different things that there are, if you could just have the one thing be stopping surveillance capitalism, we've been a long way.

Chris Heuer 16:16

Also doesn't know me know, I'm verbose. So that's one problem. I have many appreciate that. I think you're spot on with that. That sounds great. Very

Unknown Speaker 16:25

good, I think to your point. You know, these different like, if we just reuse what's already been made, and maybe it's a matter of making a page that, you know, we whatever we create, we say, you know, look, all these people already did this. We're not reinventing the wheel, sign this pledge, do this thing. Here's a list of the people we just point to that and move on to the actionable chunks that we could do to carry it forward. Because there's a lot of organizations that have tried to do different pieces, and somebody just mentioned just now, I think the harms thing. I mean, there are a couple of harms repositories. Okay, if we, you know, an actionable chunk is yesterday, I think you mentioned could we get individuals instead of, you know, people like us, we're like way on the far end of the spectrum of how much we know and care about these issues, and most people care but they don't know that much. If we could get regular people that just come in and we take account and then we take the count, we take that to the press, we get Roger to do it like that's, that's an action that so far that I know of nobody else in the marketplace of ideas has done, but that would be a thing to generate publicity. But then once you have the publicity, what are we doing next? Are we concurrently getting a group of Twitter engineers together to build a piece that we know doesn't exist and architected in a way that doesn't harm people and then we go forward with that in parallel? And so we, I mean, people have lives right,

like actionable small chunks that we can all jump in and do and have like a three month to your point yesterday on us about, like maybe we have three months to get some kind of a little men, that if we can, if we can kind of define what those are and each pour on them a little bit. We can all contribute. We get something done. You make a win, and then people want to come in for the next three months and the next three months. I would say you know being as efficient as we can be reusing and just carrying it forward. But making something that doesn't exist so we're not repeating stuff to me makes a lot of

Chris Heuer 18:47

sense. Well, if I may just add one point in your house was trying to go before I'll go back, which is that part of the reason to throw the complexity of trying to build the directory in it is to drive interest awareness and development talent into the companies and into the with the other people who are doing it. So that that is kind of the next action. The next action is we've got 300 companies who have been a part of this community for so much time, and they're already working on these solutions. Mastodon needs some more development support, you can go be a part of that, you know, the standard body that standard way. So we're not trying to be the standards body. We're trying to put the flag in front of more people and say March behind us and then to your point, you know, how do we keep that momentum up beyond and so I totally agree with that. And simplification. The other thing, by the way, here is that I just opened a proposal. So now we're going to continue to anyone who has ideas and the rest of it, please we'll put them together and figure it out.

Unknown Speaker 19:44

First, I think there's a point somewhere I don't know exactly and where it is, but I think there's a point here. Number two, I think we are making our lives already much harder than it needs to be. If there's only one thing, which is what's the simplest possible thing we could do. That wouldn't make an impact in three months, cut everything off. This isn't that simple. I think if the only thing that it is, is you can declare your interest in public declaration. You want surveillance capitalism, and that's a no code. Organization. We're not saying just the declaration changed your point of view about maybe the organization or the movement and organize the organization, so historically that has been possible. And all these ways, however, in 2022 that will not be seen again, he started asking the impossible to get all of these people doing all the other organizations to collaborate and anything everybody has said that it is possible that now that's just not true anymore. That's a conjecture on my part, but a main lesson is not

Chris Heuer 20:58

entirely off all the time. Maybe right,

Unknown Speaker 21:00

exactly. So if the if what this is is movement building in the sense of public demonstration, okay, we go on the streets and demand machines, then everything else falls into place. Right so I think what I'm proposing is that the pony is a very small pony, but maybe one that gets some legs that can grow over time. As the press writes, There is already 12,070 years so the 743 people from 43 countries saying they want surveillance capitalism to end local politician. What do you think? Yeah, so

Chris Heuer 21:42

I just want to add one thing to spectacle. The power of spectacle of people on the street is still a very big part of it. So moving it to a big public demonstration is fantastic. Thank you. Thank you.

Unknown Speaker 21:56

I mean, what I was gonna say and what, what actually is sort of elaborating is that we need to think of this as, you know, going back to the environmental movement metaphor, this is Earth Day, you know, it's just it's for everybody, there's going to be the Sierra Club there. There's going to be average people

there and there's going to be, you know, corporate greenwashing there. So be it, you know, but we're just trying to point to this crowd. This crowd that's already gathered, you know, we're trying to say, Hey, look at all this stuff in and what you were describing as a heavy lift in the directory. I don't think we want to do that. I don't think we want to give ourselves the complication of having a pledge that we have to all agree on that. You know, everybody signs up because that's the thing that gets

Chris Heuer 22:46

well if I may, I think she got it. Yeah, I think she got the pledge. Yeah, we pledge to end surveillance capitalism. It's just

Unknown Speaker 22:54

it's, it's what we're doing. But it's, you know, we're we're doing something that doesn't require the you know, the signing of anything by a whole bunch of people, but rather, we're, we're recognizing the whole bunch of people that have already doing this. We're not building ourselves up. As the smart guys who finally got this. We're saying, Hey, do you realize that there's a movement here, and this one and this one and this one and this one, and you should sign on to it to like not literally sign but you shouldn't be part of it. So we're just we're, we're proclaiming the movement. We're doing that and an amplifying what's already happening,

Unknown Speaker 23:38

please, yeah, I it's exactly right. I I'm proposing that you just say you just stay that top thing is like stop surveillance capitalism. Now who wants to sign on to this? That's it. It's just the list that continues. Of course it'll come stuff will come from there. And I like the idea of adding you know, letting organizations already that are in the space, say, you know, like, add your name to this. You know, no joining just

Chris Heuer 24:06

because you have to do the heavy lift to your point. I totally agree. Exactly.

Unknown Speaker 24:09

But that I mean, remember, stop. So yes. Yeah. Movement stop sofa. And when, you know, people came together, because I think the other thing that can happen here is you'll get political people to see that this is a movement so it's not even just, you know, like getting packed to notice or getting regular people to notice. We'll get political people in notice like, Okay, well, actually, this is a thing. So but it has to be a very, very simple straightforward thing and that's, that's why I say it just make it only about surveillance capitalism. I want my own data. I want a lot of different things. But I realized I talked about so many things and people were like, yeah, yeah, yeah. But they don't know what to do. But stopping surveillance camp, if

Chris Heuer 24:58

I may synthesize and try to put some words in your mouth to do that. Then what I would say your from what I hear you proposing and based on the conversation at all, and I'm throwing a little bit into it, so I hear myself saying some things too, is that all we need to do is start a change.org petition tonight, and surveillance capitalism. Okay, we can do it on and that's all it needs. And there can be two sentences underneath it to kind of say we convened internet identity workshop, a source of privacy and you know, however we phrase your boilerplate sort of language, and have decided that now is the time and that's all we need to say change that or it's up tonight. We can ask everyone to sign it who's here? And then we can have Roger say, look, you've got 200 signatories already. I'm sorry.

Unknown Speaker 25:48

Not just me, Roger. I mean, I true. I think it's very important that we not make a figurehead in this. Roger and, but you know, it has to be rod this is iwon and Kara and Sophia, Ethan and you know, people who may not agree on everything, but

Chris Heuer 26:09

absolutely, absolutely. We want it. It's a big tent. It's a little big tent and we need to ensure it is and make that as the ground rule, right. Yeah, so agree I'm sorry, Ben.

Unknown Speaker 26:23

I think that I'm comfortable with the like message that like one of the totally separate proposal. So in terms of like, the longer term like continuing to like form and build community, I don't know how many people are familiar with, like the Code for America brigade system. But it's an organization where in various like locations around the country, people come together and they kind of find civic projects. This was something that was started like quite a while ago now. Like a bunch of like little individual projects. They're kind of focused on whatever's needed in that community. And they've had a lot of success and getting people to just volunteer their time and their talents and the various professional skills that they have of coming up and supporting some of these projects. stuff has gone to support like CalFresh and a bunch of things, but my thought would be there's a sense of like contribution, particularly to standards bodies, particularly to like a lot of these identity style projects that we've talked about the mass of our project and how they're like notoriously nervous before requests to these amazing I think that like some kind of gathering of like, contribution to open source things that are supported and are invested in, in a way of like actually accepting contributions in the actual moments of like, sit down with people who are involved in like, I'm not even pitching pitch projects, but having a system for that around this identity space, with the goals of explicitly defining surveillance capitalism, like there. I think there are people who would invest some time into that. And then that's mostly funneled into the kind of companies that actually have assets and resources and are trying to hire for these sorts of people. It's a way to like build community to actually meet and work with people. So that would be my proposal is to have some sort of Yes.

Chris Heuer 28:36

So I think that's where I was saying that's going to be the heavy lift part and you've added a lot of color to it, which is needed. First of all, no bad proposal, so we have to keep doing all this stuff. So what I like to do when I do this with product or other stuff is this is on the list of like we got to figure out how to prioritize, operationalize. And when can we execute on it is as simple as the dark is right? We need a bias towards action and what we talked about and do here, and we need a bias to action for people coming together. And you know, that's been the one issue in almost every community I've been involved with a lot of talk and not a lot of action. So definitely solving for that very important. If I can go didn't I'm sorry, is it Danny or needs to be some Sorry, bad reading. And then we'll go actually him in the back.

Unknown Speaker 29:22

Designer and I've been trying to build something like this room. So we have some tech people that we don't, so we don't so we need its operations and we need people who are going to hold down like big prebendary this way are we doing it that way? committee that's like, helping design the system, not just me being the designer. We're both tech people. Design committee. I like people that know, you know the law and legal part of it and how it works and systems and things like that. So, I mean, I'm on board for this kind of thing. This is what we were talking about Microsoft we just don't have that together. So how do we actually really make this happen?

Chris Heuer 30:05

So we need you need a few more people into more knowledge

Unknown Speaker 30:09

about this. What we're doing about that, and that's where we've been like

Chris Heuer 30:17

leaning back on your hands before, if we can raise the flag and start marching in our parade, we get more people to follow us and then you have the chance to find those people and for them to find you. So I think my thinking on it is that you are the leading tip of the type of people that we want to come together to find the other talent in human capital to actually advance those sorts of actions into the world. Couches Well, my friend's house and I'm saying let's get us at least I got his kids bed and I kicked his kid onto the couch, but I'm with you. And I'm going to climb first and Yohannes Quebec

Unknown Speaker 31:02

organization signing up. I think one of the key things is driving to trees and the environmental trees. Interesting carbon footprint and understanding what can you do to help against that a lot of differences if it's open enough to use this browser other than that, because people don't know what to do, and then they don't want to take your point about you don't want to care about a lot of people care about what to do. So the movement part of that enabling tools and enabling conversations maybe in smaller communities that that's movement as opposed to an opposition.

Chris Heuer 31:48

Right. That's one of the things that that was brought up previously is to build an activist toolkit for enabling organizers and activists to inspire and organize collective action. So I think you're right at the heart, I got Yohannes and then coming back to Robert.

Unknown Speaker 32:05

So listening to what people say, and I'm noticing there already they are punching on different levels. Meaning some people are very practical, we need you know, these things done and then a year in surveillance capitalism, which is a proposition on the level of the economy, the world economy, you're talking trillions of dollars that go from one place to another. At what level do we punch and what low was the message? If the message is, we want to end we want to move trillions of dollars from point A to point. And the answer is use a different browser, then that's the end of the story, because these clearly do not match. Right? It's much more complicated. Yeah. So I think, personally, I think, if we pick the I think we should go and go in as much as we can. So I'm, I'm in this end surveillance capitalism. Leave the details to a lot of people who come in and do all these things. And the analogy is this for me, is I'm German. I learned through the 89 You know, East German singing, okay. And the slogan was, we are the people. Nobody can figure out what that actually meant. But it got everybody excited on the streets and the government got tackled. So that's what we talking about. The government can talk not the government but the economic system. That's the luxury punch. So the the analogies are on the political level, they are not in the standards body level. They are not all right. So today we are watching what's happening around what is it woman life freedom, well, what it was one of the slogans, right, it's another level, and nobody provides tools for these guys. At least not on that level. Right? Nobody August. And what you do is, is built environment where lots of people can come in emotionally relate to what this is. And then all these tools get built by all these people. Right? And so that goes back to the organization. So if we punch on that level, our target audience is actually not developers who's been delivered as we lead up into the our target target audience. Is everybody in the quote unquote, civil rights movement? Yeah. Who has the ability to organize me? Well, Wall Street occupy that's exactly. The calls would be stopped. So but it's on that level. It's actually a higher order. Yeah, suppose is much more tough to know. No, I

Unknown Speaker 34:40

know. But I'm just saying it's on a thing. That was a big call to action. That was just kind of a one thing you know, I had one little simple

Chris Heuer 34:47
lesson.

Unknown Speaker 34:49
Basically, if we were to go down that route, and I'm just observing that this is a possibility, right, that comes with risks for both sides. But then the people who call up the call to action is the top 10 Or maybe the top 30 relevant organizations in the world. Start with the EFF probably yes, probably at the top of this list and say we can you help us put this movement together? It's quite modern civil rights are some some statistics, civil rights, and it starts with stop so it's got this

Chris Heuer 35:17
Yeah, that's really good. Thank you.

Unknown Speaker 35:20
I have a privacy list all of those privacy all the GCS of all those privacy organizations, epic eff Consumer Reports, all of them I am on this

Unknown Speaker 35:30
list. You know, I may be wrong about this. But my feeling is the type is right fit time.

Chris Heuer 35:35
The time is right. That's why two years ago, that's different time is right. Take it to that level. I just want to say one thing falling back on this last bit, the digital rights movement is pretty straightforward. And no, it's bad. Okay. It doesn't work now.

Unknown Speaker 35:58
unfortunately died some years ago. Who walked around with the new digital deal.

Chris Heuer 36:07
Please, I'm sorry, Robert,

Unknown Speaker 36:09
the various tools that we can use, and I know that there's a bias towards simply doing something simple right now to get the ball rolling and to not get too sidelined by the technical developments. But there is a need to communicate the complexity of the problem in simple ways. And I guess I'm envisioning a situation where someone took a quiz, or there was some sort of your honest level test that just people like I ran this thing, and I created a button for me and that button, demonstrated my personal risk. Yeah, how much on reviewing or how much on and I'm impacted by surveillance capitalism. Next person wasn't their scores, their scores, it becomes vital. These things show up on Facebook

Unknown Speaker 37:06
page. I don't understand it. With cruel

Unknown Speaker 37:09
education. Yeah. But it's gonna end up being a button. Or think about the number of movements over time there's a movement, and everybody's gonna turn their Facebook page. So we need something like

that. But those things are they're not bias towards action or simply to say yeah, it's sort of feel that element.

Unknown Speaker 37:37

Yeah, but you know, we've gone back and forth on this through the years and I like on it says, I really do think it's a moment that we have this moment in time and I just keep thinking about Kim Cameron. Three or four years ago, when he came to IW. Just he just remember, he just had retired from Microsoft, and he said, I want to be an activist net. Now this is what I want to do. Okay, I'm enough with corporate now. I want to go back to my childhood when I used to be on the streets, you know, in the civil rights movement and all that and he goes, that's what I want to do now. And actually, it was still too early then. You know, now he's gone. But really, I think it actually is time now. And I love the idea of a tool that could be on there for people I'm not exactly sure what surveillance capitalism is sounds kind of bad. But hey, you if you want to see who's tracking you on a website, use this tool. It's called paychecks right. And Oh, guess what? Look at all these people that are tracking me on this website

Unknown Speaker 38:43

to get on with it.

Unknown Speaker 38:48

On the LA Times, I mean anything that's like,

Unknown Speaker 38:51

close, but something that simplifies that because we're the experts in fact around this in our entire networks. Like we've got people close to us. business wise. Yeah, they understand.

Unknown Speaker 39:03

Right? The rest of our networks go down.

Unknown Speaker 39:07

All the moms, the grandmas

Unknown Speaker 39:09

who are having bad health and you don't know it, you better back that up

Chris Heuer 39:13

Yeah. Good. Thank you, Robert.

Unknown Speaker 39:16

One question was if there's a day What is the name? Like? Just speak up a little bit.

Chris Heuer 39:29

If there was something I'm sorry, we're out here. By the way. There wasn't anything left by the time we?

Unknown Speaker 39:33

Yeah, there was something like an Earth Day what would the day because that is really like stop that. Gotta

Unknown Speaker 39:38

name the day.

Chris Heuer 39:41

Let's think about the action and the action will lead us to the day and I think that, you know, I think that one of the actions is tying it into that new law that lets you download and own your own data. It's like literally clean your data free from these systems.

Unknown Speaker 39:57

Yes, not exactly. Exactly. Okay. It's not imminent.

Chris Heuer 40:00

We have sense of 10 which are not aware of it. But the point being the action is like, what's what's the one thing that we could all do in maths to start, like, create a salvo to lead over data from all these networks that have them? So could we create a plan to say this is a day we go around, leading all day? I got Yohannes. Who would want to say something Jackie?

Unknown Speaker 40:20

There is a bunch of formulas, if you work with organizations, existing organizations, they are orders of magnitude better at doing this kind of thing that we are we should say this is what should happen. Help us do?

Chris Heuer 40:32

Yes. Yeah, absolutely. No, no, we can't do this alone. You're right.

Unknown Speaker 40:39

Also, just like, how do we the people that are currently and have been on the streets for the last five years, not like a couple of decades ago that aren't here? On average? How do you ask them? How to use like MLM, but also ask them

Unknown Speaker 40:55

how to do like the Black Lives Matter people

Unknown Speaker 40:58

or rise, or like, showing up for racial justice? Those are the posts of the people that have been in the streets asking for a green New Deal. For five years. There are laughs at them, like, doesn't that mean? The digital new deal can be a part of that. But like that those movements for a new deal already exists. So do we really need to fork from those or can we and provide us just like, the other way? That's

Chris Heuer 41:21

that's why I like the end. Surveillance capitalism, because that can be an umbrella for everyone to follow their Go ahead.

Unknown Speaker 41:27

I don't think any surveillance capitalism I mean, I think it's great, but I think it's one of the digital wrongs that a digital awareness has to address and particularly if we're going to elevate people who use the digital ones, on whom include, you know, AI bias in there, all kinds of things that feed into this, and we don't want to, we don't want to, like Make, make the movement so narrow that that in this cludes yes, those sub parts so I don't know I think there's I know DRM is unfortunate, but I mean, digital rights, putting aside the movement, digital rights and and numerating Digital wrongs. And, you know, marching for digital rights, whether that's the name, I mean, that seems like the thing. Rents are kind of bred for.

Chris Heuer 42:26

Well, what I would, what I would suggest is that we're still in the diverging stage and let's go through all of the language that we have and look at it together and start testing it because that's what we have to do, Doc.

Unknown Speaker 42:42

I think we tested that experience, and I have a bias for action. Right? I think, if, if I can speak for Roger here, just from what he sent us, you know, pick one thing Yeah, pick one thing focus on that. I think ending surveillance capitalism works. He had a best seller. She shot us through I've met a best seller.

Unknown Speaker 43:03

Bob Hoffman has a best seller right now. That's all he had scanning

Unknown Speaker 43:07

was just man tracking right? Part of the same

Chris Heuer 43:10

thing. Absolutely.

Unknown Speaker 43:12

We can loop that if he could be here if he could have been there. So I just think if we start with that as the arrowhead with the wood behind the arrow, we can then pull out other arrows to say this is or similar once or other quiver.

Chris Heuer 43:27

And again, that's just part of the moving fast like you know, it isn't that thing. If you want to go far go with others. If you want to go fast go alone. And that doesn't necessarily mean we have to be inconsiderate. We can we can wrap them in we could amplify we can reach out and say help us and we will help you and explain what the opportunities are. So we can all use our relationships to bring in the people who think that this is an important thing to have their voice included in it. But it's not the tip of this arrowhead, as Doc was saying, but I do agree with you and there's a lot more complexity to it as you're getting to. And the problem is complexity. You know, as I've shared with a few other people here this week you know, there's been a lot of people over a lot of years putting hundreds of millions and billions of dollars into helping people sell their data. And the only one that really is working is Rakuten, and that's because they don't talk to you about the data. They go buy stuff and we'll give you money back. It's a simple human message that people can understand in parts and that's what we have to go to and that's why I like the simplicity of stopper in surveillance capitalism, but it does mean more than that and there again, language. So biggest problem I have please, if we can like trick him then back to you.

Unknown Speaker 44:42

Okay, this is a digital rights movement. And maybe that's the site or the landing place we go to but the first change. James couldn't be stopped for being this kind of points to the site. So one possible thing for the site. We've had a lot of ideas, good tools, educational things that are resources there. And the pledge love it because then you can count people. We may have multiple pledges. So the first pledge is just Do you agree with this? Second pledge can be hey, if we get 100,000 people assigned, I will spend an hour on whatever projects you bless. Or the third one might be Hey, I will go further. I will pledge to march on this day. I looked up a whole bunch of Facebook locations, and maybe we'll choose December 1, and I will plan to march and maybe there's no maybe there's different levels. First, if you have counts, there could be generally some interest

Chris Heuer 45:32

or even or even that just I mean, it doesn't even need to be a march. I mean, it could just be a demonstration at your local library. So you'd make it as simple as that and everyone knows where their local library is, and whoever shows up shows up and then you get the groundswell and sadly we use social media and a hashtags like aggregate it all because that's the easiest way to do it. But yeah, I'm sorry, who else

Unknown Speaker 45:55

starting to get at why the problem exists, and that is that it's profitable.

Unknown Speaker 46:02

So until we can basically shine a light on the average profits made back then. It's good. It's, it's gonna be mysterious. to people. And we can demonstrate to them that oh, well, in some way.

Unknown Speaker 46:21

Yeah, I think I think we're almost out of time. I think we need to come up with something what we do next year, okay, it may just be another session. But I would suggest that instead of doing things ourselves, we should let organizations that exist already do their thing with our support. It's much better to get them involved rather than competing. Take a pledge if we aggregate. So many people signed the MyData pledge, and so many times signed the CTA pledge, then everybody's gonna be happy. If we say it's a new pledge, need to sign this one, not that one. Then we turn off all these organizations. So if we amplify them, you're doing a much better job than if it were our own thing. And to that extent, I would suggest that maybe we do a weekly conference call with the initial audience being people we know at organizations that know how to do this and say, Hey, we have this wild idea and we really know nothing about this because you were about know about organizing, we don't, but as subject matter experts, we think there is an opportunity market today to put out some kind of strange, stupid message like incidents, copies, what do you see? And that's all that happens. There will be some good conversations and there will be some more conversations the week after, and we either resonates but we don't if you don't resonate, nothing happens. Nothing. We can't accomplish anything because we don't resonate with those people. But if we resonate the same in can double every week. Yep. And I think that's the right. I've generally been very successful in organizing people have been very unsuccessful organizing people. And I said, here's the answer, and been very successful organizing people say, What have you speaks to the idea, tell me how to make.

Chris Heuer 48:11

So you're involved in the CTA now, right, you're on your board or who's on board. Okay, so then you know, who is in charge? Well, I mean, I mean, there's a group of people and yeah, but who's like chair in

Unknown Speaker 48:24

charge? person, I would say is Tibet. Sprague

Chris Heuer 48:28

so I think you're absolutely right. I'm talking to him this week. So awesome. That's what I was gonna suggest that we talked to them. I'm trying to get them up but I want to really amplify again, the specific tactical point you made, that if were to do something like this, you know, phrase that the next step to take is investigate CTA, investigate EFF and go support them and find the different things they're doing and make visible those numbers.

Unknown Speaker 48:53

Just tell them here's the cause. I said we can no actually make something happen if we all you know, coordinates, and it's not even we do one thing, it's just a coordinate. You know, we are thinking of doing this one would you like to merge with us? Yeah, it's like there's some people out some girls out there on the street. or complain about the principal's. Wouldn't you like to also show up because you complaining about getting money? You know, it's not even as a complaint about the mom and Suba is the complaint about the principal, but the people who complain about the mom also show up. I think that's the trick to do that. And what am I planning

Unknown Speaker 49:29

to not name ourselves and have a subject be? What do you call this movement? We're all part of, you know, I mean, let's, let's recognize that we're in a movement together. And, you know, as we're going, we'll name it. I mean, and the project is then sort of surveillance capitalism for you know, something else. But let's convene this movement and name this movement with the people who are here.

Unknown Speaker 49:57

So I have a thought here. We have three board members and customers. It's an existing five one c three. That could be whatever we want. If we want to say yes,

Chris Heuer 50:13

and that saves us from going into a fiduciary to handle any cash if we need it, so that would be great.

Unknown Speaker 50:19

This is kind of along the same vein, but I was gonna suggest I like the simplicity of something tonight is created chairs that are efficient, like that's pretty good. And to do that in like 10 minutes. Similar, a lot of that madness a little different. Make it over to London for I think there's one site called Open raise money, rose into Fiscal Sponsorship to care about, I don't know exactly how it works. It's kind of a former colleague of mine, you could just make it over budget for anything and unlike change, which is probably just gonna have like, inside it, but like everybody has a bit more and like, I want to chip in \$1 a week. I want you to know about your sub projects within this kind of Web. Whenever

Chris Heuer 51:08

I gotta say honestly, that right now, given this emergence, I'd rather not do anything that involves us handling money, unless it's for small things to pay for quarter feeds, like if we had to pay for software and

Unknown Speaker 51:22

be like, Hey, do you really want this to do it? \$2 a month.

Chris Heuer 51:24

Yeah. But then when people give you money, they expect something they didn't have to like do a lot more. Please.

Unknown Speaker 51:32

Here's what we need to get done. You want to donate, buy one of those things. Do one of these things, empower people, no central organization of money and disbursement

Chris Heuer 51:40

or donate eff

Unknown Speaker 51:41

organization exactly on these platforms. To these other people.

Unknown Speaker 51:47

We need signs in front of the White House. The quote is \$1,000 Who's picking it up? Yeah, yeah, right. Do you pay for it and you get a batch somewhere,

Chris Heuer 51:57

but I still want to explore it. But I think again, in trying to be biased towards action and simplicity, the first steps or the first steps and then as we see how it evolves, we can evolve the planning and strategy and tactics.

Unknown Speaker 52:10

I would like to point out there's some energy this is good. Yeah, really. leaves just too much energy there might actually something be happening.

Chris Heuer 52:26

Yeah. So here's what I would request from everyone here. If you can. We have even more. We're closing circles about Okay, good. Then we're wrapping right now. What I propose we do is it so I've been recording and I got an other transcript. I will post the outer transcript of everything we've said. It's been pretty good. Some of the noise might overlap some of it so the quality might drop. Oh, awesome. So we get the notes on to the wiki or onto the Kiko. And then what I'd ask you to do is write a proposal for the change.org petition into the session notes. So that tomorrow we can see 1012 Different language examples of how we might phrase it and keep it simple. And then we can actually talk about one and literally tomorrow after this session, write it and ask everyone in the community to sign it and get it going.

Unknown Speaker 53:21

Until the trillions of dollars that are in use already. Who's making the money face who's making the money, a bunch of intermediaries that they can play with the source of the money or country companies and they don't want to spend the money that they're going to spend in some other way? So that's sort of the critical thing, like the funding for this is not the people making money.

Chris Heuer 53:41

Yeah. Awesome. Thank you all so much. Thanks. Wow. Really got bored

GODIDDY.com

Session Convener: MarkusS

Notes-taker(s):

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

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

NO NOTES SUBMITTED

What is the Perfect Key Recovery?

Session Convener: Matthew Vogel

Notes-taker(s): Matthew Vogel

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:

Types of key recovery:

- deterministic
- social network
 - fiduciary
 - multi-sig
- Problem: as the network grows, the problem becomes worse
- custodial
- Talked about the using memory. Old memories with low frequency of testing memory vs new memories which require more frequent memory tests.

Security requirements are use-case dependent:

- low value = less security needed. 4 digit pin
- high value = more time / energy required

In many cases, there's no way to know if your password is compromised.

Multi-signature models with time constraints to unlock a key. All signatures are due before a given deadline to be approved.

Methods for key storage/recovery that are actually used:

- store on device
- store on trusted custodian
- writing down on paper

What We Can Learn from Sports Brackets, Tinder, Netflix - Ranking

Session Convener: [Ankur Banerjee](#) (cheqd)

Notes-taker(s): Scott Phillips (Trinsic)

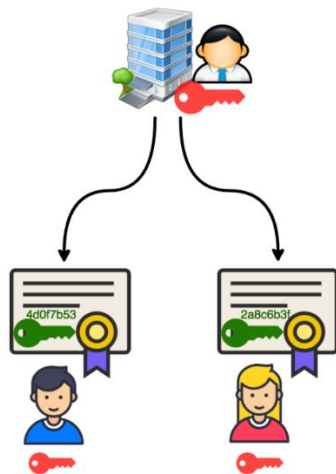
Tags / links to resources / technology discussed, related to this session:

1. [Dynamic & Decentralized Reputation for the Web of Trust: What We Can Learn from the World of Sports, Tinder, and Netflix](#): Primary source for this talk, originally published as advanced reading for [Rebooting Web of Trust \(RWOT\) #11](#) at The Hague
2. Worth reading to understand concepts:
 1. [Soul-Bound Tokens \(SBTs\)](#): Probably the most prominent recent idea around decentralized reputation outside of the SSI community. This particular talk posited a method different from SBTs
 2. [Elo hell](#): A trap video game players sometimes fall into, where they find it hard to dig themselves out of a rut/bad streak.
3. The [references section of the original paper](#) also contains an extensive list of related RWOT readings.

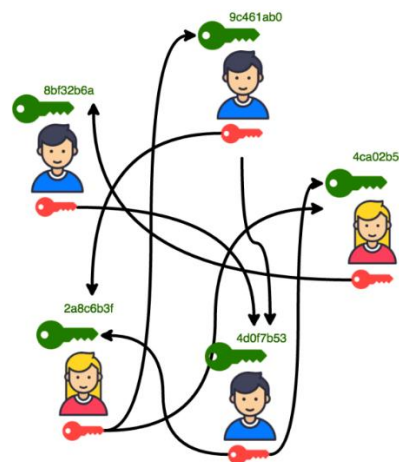
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

- In some industries, there is no need for a ground-up web of trust style reputation since they are regulated industries.
 - DMV issues all driver's licenses.
 - Eg, government
- What about less centralized / unregulated issuers? Eg coffee verifiers (rainforest alliance)
 - What happens with management changes, buy outs, etc?
 - Trustworthiness of an issuer can change as a function of time.
 - Trustpilot, yelp, etc.
- You can be a licensed doctor, but are you a *good* doctor?
- Problem with the proof authority concept is that your ranking only goes up over time - it doesn't diminish.
 - Can your quality decay over time.

CERTIFICATE AUTHORITY



PGP / WEB OF TRUST



Whom you trust depends on who is giving you the information

- If it's a regulated industry, there's an objective answer. If it's an unregulated industry, there is a subjective answer.
- What about trusting DIDs?

There exists an Excel spreadsheet of trusted DIDs for World Economic Forum or National Health Service

- It's easy to know if a proof has been tampered. It's hard to know if an issuer is trusted.
- UK has one issuer of COVID vaccines credentials (NHS), but 1000s of issuers of covid test results (currently issued as PDFs or paper)
- How do different degrees map across countries?
- We fall back to FICO/Experian/Transunion, etc. Who individually keep lists of trusted issuers/verifiers
- We have side-channel usages of issued identity
 - Drivers License to open a bank account
 - Utility company bill to prove residency
 - You need to model the credential that it will be used in other areas.



- Elo rating:
 - Bidirectional, zero-sum, asymmetric scoring system.
 - Start with 1200 points

- Beat an equal rank player, +5 pts you, -5 pts them.
 - Beat Federer, +100 pts, Federer -1 pts
- Tinder and Uber use similar systems.
 - Vast majority use 1 or 5, 2-4 have the same impact as a 1.
- Because so few people use 2-4, 1 & 5 are all you need
 - This turns into thumbs-up and thumbs-down (Nero Ranking)
- Captcha box: 2 words, 1 known, 1 unknown
 - Elo ranking you against bots
- How does this come down to Decentralized representation
 - Somebody is maintaining a list, possible if the number of possible answers is low. Very hard if the
 - [.wellknown](#) file as a DNS record / domain file is used to verify ownership of DID.
 - But how do you know that [microsoft.com](#) is a trustworthy domain?
 - You're back to the curated list of valid domains from the big-3 issuers
- Requiring DIDs to be linked to a domain just slightly shifts the target

Similar to how Elo rated games work, you could rank the interaction with a did

1. Are you a doctor?
 2. Are you a good doctor?
- My reputation for showing up to flights on time is very bad.

Reputation is multi-dimensional, and calculating that is very hard.

- Saying a public key is a trustworthy public key is a much saller problem.
- Spamhaus project to rate spammy email domains.
- Depending on the context, the ranking of trustworthiness of a credential can be a requirement
 - Maybe 1 high-trust cred, or several low-trust cred.
- The idea that lower-ranked users can send the signal that a high-ranked user is no longer trustworthy
 - Some kind of proof-of-stake model can be involved, but it needs to be time-dependent
 - [Cheqd network blockchain](#) uses moving-average window of the last 24 hours for liveness-based penalties.

Trade-offs for SSI Adoption

Session Convener: Elina Cadouri

Notes-taker(s): Joshua Coffey,

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

- Convener is building an SSI product and wants to have a conversation about the possible trade-offs of adopting SSI
- Key management is really difficult for individuals
 - Is it worth someone not having their own keys in order to make the user experience easier?
 - DeFi / crypto group would likely never accept anything but managing their own keys
- Terminology issue – should we be using “VCs” and “DIDs” when people have no idea what those mean?
- Value proposition of attacking someone’s phone is massively increased – I can take everything from you solely by hacking your phone
 - I used to have to break into your house
- Onboarding is not easy
 - One has to understand many things before they can get a footing
 - Is it better to educate users about SSI, or just deliver a product to them that does it without them knowing the terms?
- Companies have to choose between adopting a standard as-is and not having everything they might want, or going proprietary and breaking interoperability
- Might be linked to financial speculation / web3 / etc. due to shared terminology
- “Decentralized” is not a selling point, but “owning your own data” might be
 - Many people are scared off by the word “decentralized”.
 - Many companies really like centralization and don’t want to give you the power to own your own data
- SSI is incredibly complicated and implementation is very difficult, which encourages people to make use of abstractions which remove some of the benefits from the system
- We should all leave this conference / industry and go get jobs in other industries and bring SSI with us
 - We have to go to where the users are, rather than thinking “if we build it, they will come”
 - Does any of this actually matter to those external companies? What do they actually view as value propositions?
- Accepting smaller user bases as a starting point instead of trying to do the whole world at once
- This building should have the highest concentration of people who have self-sovereign identities in the world, but basically nobody here even uses it
- What are the barriers that need to be brought down for SSI to happen?
 - We need to figure out what we’re doing in regards to interoperability – do we dedicate resources to it or go our own ways?
 - Interoperability needs to come about as a result of a strong desire to link multiple ecosystems together, as opposed to building the bridge first and hoping land arrives around it
- We need more people focusing on actual verticals as opposed to building platforms and abstractions

- Stop renaming things every six months
- We want people to share our vision and love SSI with us, but instead maybe we should just deliver things which work for them
- Standards elsewhere come about to standardize existing proprietary products/protocols/interactions – it's very unusual to start with a standard and attempt to find a use case later, as we are.
- Anyone who says that SSI is the solution to all problems is giving bad advice
 - Sometimes traditional solutions are just better
- Could be an opportunity cost where we're not thinking about how to improve the current centralized/non-SSI solutions we have, and spending all our time on SSI which might not happen
 - Maybe the best option is to just lobby for strong data protection laws – that might be the best thing for the state of Identity in a long time.
 - It'd also help drive adoption of SSI as companies need to find alternatives to just guzzling data
- There are cultural and jurisdictional differences between countries
 - Chinese government requires that all encryption be backdoorable
 - Things we take for granted as being “value-adds” (privacy, security, etc.) may simply not be something that certain cultures care or think about
 - Maybe we should spend more time in Europe than in the United States
- Where is the call for SSI going to come from?
 - Governments? Citizens? Companies?
- Blockchain / Web3 could be a huge driving force behind improved identity standards and protocols
- Maybe we find one unified use case that we all work towards

IF CA DMV offers VC/mDL what would you do with it?

Session Convener: Gail Hodges, Wayne Chang, Oliver Terbu,
Notes-taker(s): Gail Hodges

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

CA Assembly Bill 149 Section 21 Article 6
<https://legiscan.com/CA/text/AB149/id/2425119>

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

1. We discussed what CA DMV was authorized to do with Assembly Bill 149 in September 2021
2. Two standards are in plan to be enabled by CA DMV, ISO 18013-5 (named in Bill) and W3C VC (using OIDC for VC) to enable verifiable credential provision and presentation
3. We brainstormed on use cases that would be relevant to CA Government, economy wide
4. We Talked about what state needs to think about to achieve those use cases.

Contact gail.hodges@oidf.org for questions or to reach the co-facilitators Wayne and Oliver for followups.

Introduction of the new EthrRevocationRegistry2022 method w/ Delegation, Owner Change, Meta Transactions, ...

Session Convener: Philipp Bolte, Lauritz Leifermann, Dennis von der Bey

Notes-taker(s): Philipp Bolte

Tags / links to resources / technology discussed, related to this session: **EIP-5539**,

EIP-712, revocation method, ethereum, smart contract, registry

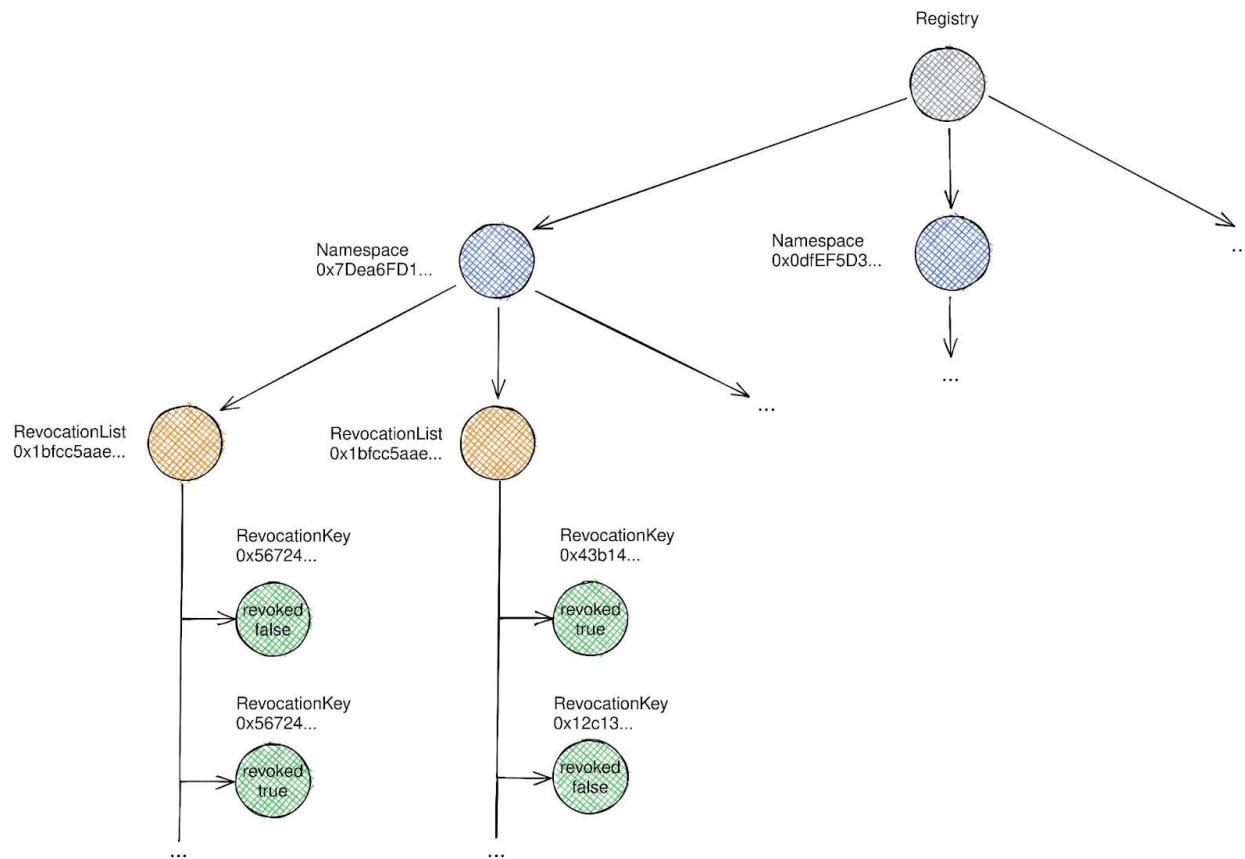
Useful links:

- EIP-5539 (basis): <https://eips.ethereum.org/EIPS/eip-5539>
- SSI revocation spec (early): <https://spherity.github.io/vc-ethr-revocation-registry/>
- Smart contract: <https://github.com/spherity/ethr-revocation-registry>
- Typescript library: <https://github.com/spherity/ethr-revocation-registry-controller>
- Veramo verification plugin: <https://github.com/spherity/ethr-revocation-registry-veramo-plugin>
- Slides: <https://docs.google.com/presentation/d/1Ud6ltXTTK9WbR09ksqvAIYwWC-cVk3WJ/edit?usp=sharing&ouid=114691100214339208423&rtpof=true&sd=true>

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

- New revocation method based on an Ethereum smart contract
- Registry approach → singular deployed smart contract can be used by anyone in the world to track revocation statuses, e.g. of Verifiable Credentials
- *Data structure:*
 - Registry is divided into namespaces that represent Ethereum addresses
 - Every ethereum address has implicitly an already reserved namespace that only it can write in
 - A namespace can contain an infinite amount of revocation lists that a namespace owner can write in
 - A revocation list is a mapping of an infinite amount of revocation keys to booleans
 - True means revoked, false means unrevoked; revocations can be taken back if needed
- *Cool management features:*
 - *Delegation:* a namespace owner can invite other Ethereum addresses to one or more of its revocation lists → this address has then writing access in the granted revocation list(s)
 - *Owner change:* a namespace owner can give up its owner rights of one or more of its revocation lists; useful e.g. in the event of key rotations
 - *Meta transactions.* A revocation list owner can prepare a signed payload that describes an action it wants to do in the registry (e.g. revoking a key). It can give this payload to a third party that can publish a transaction with it to the registry; useful e.g. if the revocation list owner does not have any ether to pay for transactions (e.g. on a platform/ SaaS)

- *Batch revocations*: Multiple revocations in one transaction or revoking a single list at once



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

- Another approach: offline merkle tree with revocation information and we just publish the proof in a public smart contract
- Is the smart contract audited: Not yet, but we plan on doing this before we deploy it to mainnet. (it's only on Goerli for now)
- Which upgrade pattern are you using? Diamond pattern? → UUPS for now, but want to try diamond pattern?
- Are you using hardhat? We are using truffle at the moment but it really limits us and has some weird quirks with upgradable contracts we had to work around

Signing XBRL Document with vLEI

Session Convener: Phil Fearheller

Notes-taker(s): Phil Fearheller

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

[vLEI / XBRL Pilot](#)

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

Lots of great questions from the audience ranging from vLEI governance structure to the layout of the data that seals a delegation request in an interaction event.

I understand identity...Do you really? Let's find out. It is so much better than the movies.

Session Convener: Ken Gantt "ID Guy"

Notes-taker(s): Travis Edwards et al

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

Referenced website: www.biometrics.gov, www.dhs.gov/obim

Referenced email: info@obim.dhs.gov for sending info to presenters...

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

Concept was presented with speaker and slides, animations, videos

Questions:

Q1 - What level of community engagement is done in the aspect of identity from DHS?

Q2 -

Q3 -

Q4 - What does it like if identity is elevated to a critical infrastructure sector?

2 - Edged Sword: the wallet metaphor in SSI

Session Convener: Daniel Hardman

Notes-taker(s): Daniel Hardman

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

Slides for this session are at: <https://bit.ly/wallet-meta-iiw>

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

We talked about the benefits and drawbacks of building the mental models for new technology atop metaphors. This often allows people to make intuitive connections and guesses about what they can do, and how they can do it, in the new environment. However, metaphors can also be problematic when we attempt to use them outside the cultural, linguistic, and demographic context where they resonate. They can constrain the user experience, create scaling problems, and lock people in to a way of thinking that prevents progress when a better way would otherwise be possible.

We discussed the example of early tractors, which were modeled off of a plough steered with reins. Farmers actually hooked up the tractor and sat behind it on a separate contraption, with reins as the steering device.

We then explored the use of the wallet metaphor in SSI. It has benefits and drawbacks. We talked about some of the ways that we talk past each other, depending on whether we approach that metaphor with a background that is primarily rooted in physical wallets, in cryptocurrency wallets, in SSI wallets, in Apple Pay/Google Wallet, etc.

We explored several points of misalignment in assumptions: the significance of possession, the degree of intelligence, the behavior patterns that should be supported for users, whether a wallet is a public interaction surface or a private tool, etc.

The call to action was to be advocates for people to be very crisp about what assumptions they are making as they use the term "wallet".

Thoughtful Biometrics Workshop - Prep Idea's Questions Issues

Session Convener: Kaliya @identitywoman

Notes-taker(s): Kaliya

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

<https://www.thoughtfulbiometrics.org/format.html>

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

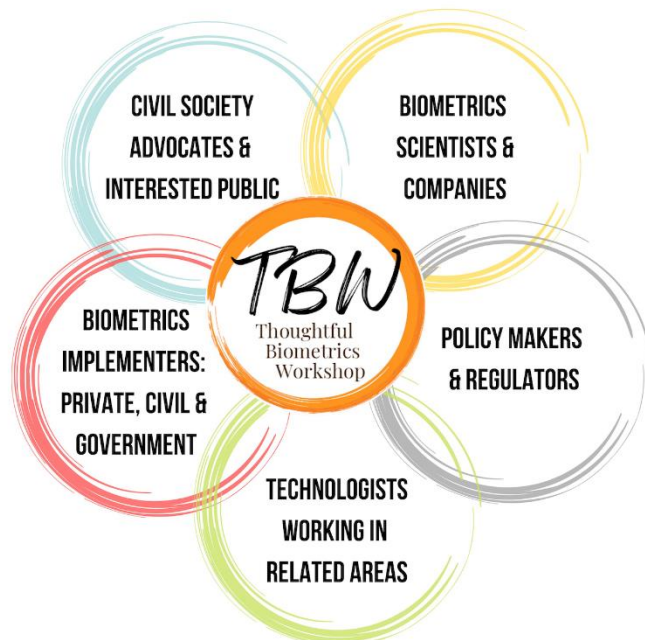
This session was covered to share information about the upcoming Thoughtful Biometrics Workshop.

The event was inspired by Kaliya's experience learning about Biometrics from Jack Calahan who engaged with the SSI world from his position at Veridium.

This paper was written several years ago [Six Principles for Self-Sovereign Biometrics](#).

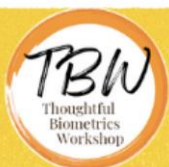
The Frist Thoughtful Biometrics Workshop was put on in the winter of 2021 in the middle of the pandemic as a virtual unconference. It was run using Open Space Technology the format that we use at IIW - where the agenda is co-created live the day of the event. You can see the [book of proceedings from that event here](#).

This 2nd Thoughtful Biometrics Workshop will be in the First Quarter of 2023 and bring together a range of constituencies.



You can learn more about it on our website <https://www.thoughtfulbiometrics.org/>

It will have a format that looks like this - but the dates may shift to March.



Thoughtful Biometrics Workshop Feb 2023

Format Overview

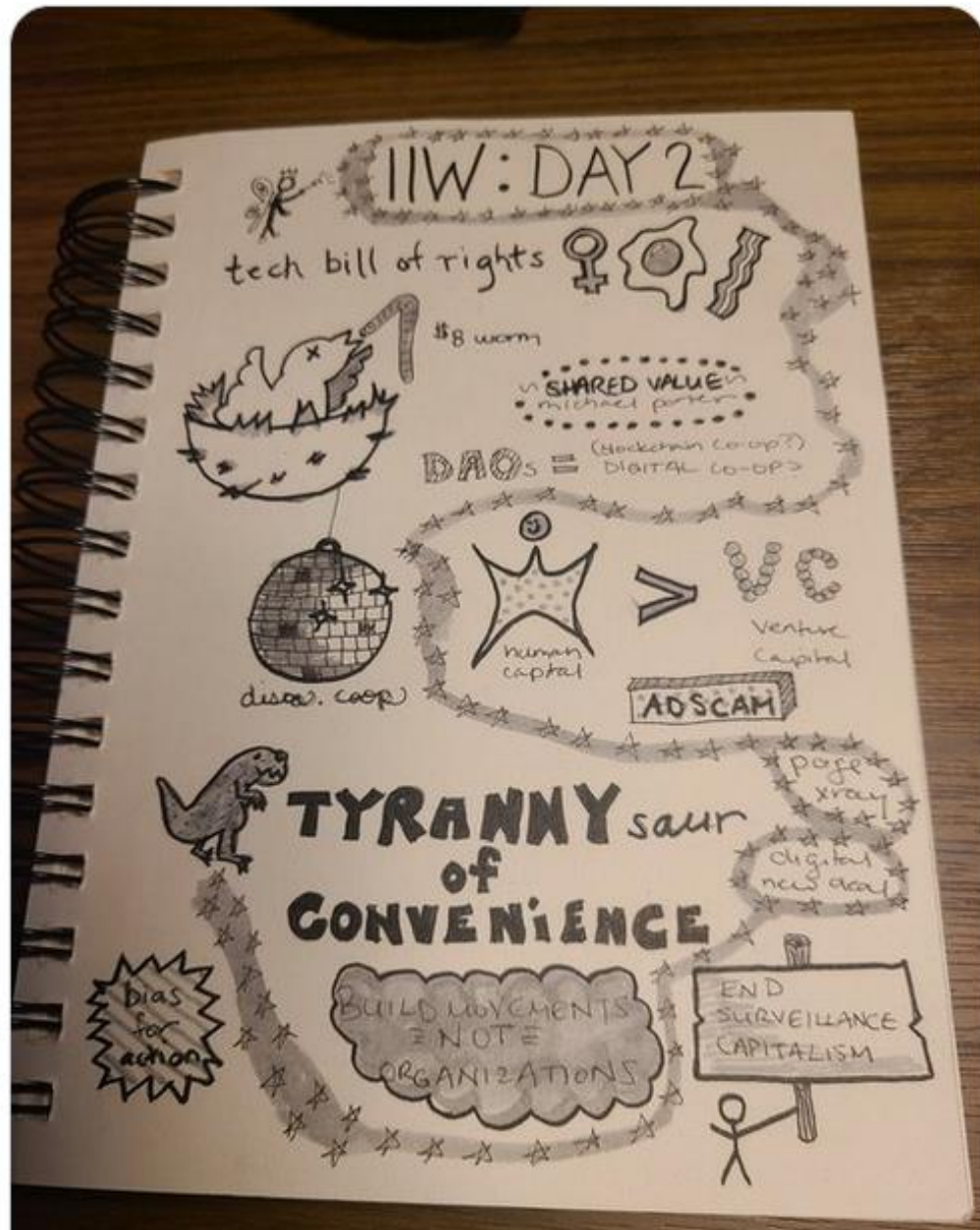
| MON 13th | TUE 14th | WED 15th | THU 16th | FRI 17th |
|---------------------------------|-------------------------------------|--------------|-------------------------------------|-----------------------------------|
| 9-11a Pacific | 9a-2p Pacific | DAY OFF | 9a-2p Pacific | 9-11a Pacific |
| Opening Day Conversation | Agenda creation | screen break | Agenda creation | Synthesis & Next Steps |
| World Cafe | Open Space Technology 3 sessions | | Open Space Technology 3 sessions | Event Closing |

thoughtfulbiometrics.org

We are seeking participants and sponsors.
You can reach out to Kaliya@identitywoman.net



Jessica Tacka she/her/Mx. 🐙 @JessicaTacka · Nov 17
Final day of #IIW, LFG! @idworkshop @TransmuteNews



Notes Day 3 / Thursday Nov 17 / Sessions 11 - 15

SESSION #11

CESR for first year wizards

Session Convener: Sam Smith, Drummond Reid

Notes-taker(s): Neil Thomson

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

- [IETF Draft CESR Spec](#)
- Full [CESR for First Year Wizards](#) slide deck presented in the session (Google Slides)

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

7 Main features (only capturing in session discussions)

Format rationale

Ability to convert between domains as required - text, binary and raw (text, binary)
Conversion follows the slide triangle.

Naive base 64 does not meet the composability requirements for the raw format

Why do we want composability? Why is it desirable? - if you are streaming events (streaming protocols), you can do it in many ways and the intermediaries don't have to parse the components to ensure round trip delivery (which may otherwise be required)

Problem w Base 64 is you can't concatenate and guarantee delivery or composition, decomposition)

Example of mixed content stream through concatenation.

You call that readability?

In other mechanisms, the encoding of "raw" data is required. With CESR, if you stick to the supported raw data types, then they are supported by CESR without additional encoding

Similar to mult-codec - where you have to specify specific characters which have special meanings (cherry picking dual purpose characters (letter/number + special character)

Comment - so this is self framing (simpler, one less stage of package/unpackage)

The base rationale to make it compact, composable/decomposable and transformable

Why text based primitives?

JSON replaced XML as less “wordy” then to CBOR.

Rationale for compaction efficiency - bandwidth is orders of magnitude cheaper than CPU cycles

As CESR is text streaming, can use REGEX to parse (as pure text)

CESR is also designed to allow partitioning for both CPU Affinity and multi-CPU partitioning efficiently (scalability)

JSON/CESR mix example - a JSON structure, plus signature block for the JSON (as CESR

Self-Addressing Data Structures

Quote of the day: [Cryptography is biting us “in the hash”](#)

Building the verification hash into the data structure, you always know where the hash is and lends itself (with SAIDs, which are also the hash) to making it simple self-verifiable data into any data store.

Saying we don’t need block chain. Yes, but the main point is not needing (blockchain like governance).

SAIDs - any data (obj) anywhere can be address with a verifiable identifier

Why Legally Valid Digital Signatures

There is a spectrum of zero trust

Goal make all data as verifiable as possible. This includes verifiable in transit and at rest.

End Verifiable - if the original signature, does not make it to the end system, then it’s not “End Verifiable”. This also relates to data provenance (chain of operations on data)

Benefit #5

Benefit #6

CESR documents can be verified at any point in the future.

Archiveable PDF - is pure text (text based structure)

CESR addresses issues with encoding via data structures or (other alternatives - see slides)

This leads to CESR enhance XBLR - in that CESR encoded information is embedded as native XBLR components.

Showing the GLIEF business report using “XBLR with a side of CESR”

#7 Verifiable Audit Log

E-CFR regulation defines time expiry for verification

CESR allows signing of parts (vs entire) audit log

CESR only uses 65 chars of the 127 ASCII set - which allows other chars in the set, by annotating with the chars not used in encoding (embedded comments).

Don't have to transmit - can use this as the recorded stream (audit log, at rest)

With verifiability it becomes self verifying.

OpenID Connect Federation - What is it and what's new?

Session Convener: Mike Jones and John Bradley

Notes-taker(s): Nicole Roy

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

OpenID Connect Federation - Mike Jones and John Bradley

Day 3 Session 1

This is not an authentication protocol

Not even specific to an authentication protocol

A way to build trust between deployments

Can be used to model things like traditional academic identity federations

Have learned a lot of lessons from the SAML identity federation experience

"What's old is new again"

Now that I have a self-sovereign wallet, why would anyone have any trust in the stuff in my wallet?

You have to have a layer to bootstrap that trust between parties/entities/claims

R&E federation has somewhere around 15,000 endpoints

We need trust between millions of endpoints globally

How do you figure all of that stuff out as a participant?

OpenID Connect federation metadata allows us to describe the trust relationships

Hierarchical delegation

About a dozen years ago, we were working on drafts of OpenID Connect, did five rounds of interop testing

That's the process we're in for the endgame of the OIDC Federation draft

Giuseppe from the Italian government is here to talk about their deployments

Helps do trust establishment

Parties signing trust statements about entities in the federation, hierarchically, in a delegated model

You can be a member of multiple federations

Core of this enables you to make statements about yourself, others can make statements about you, chain these up cryptographically to build a full picture of trust in an entity in one or more federations. Example of how this works: A professor at University of Washington can access the large hadron collider at CERN in a trusted manner, after being issued claims by the trusted identity provider at University of Washington

In order to book time on a telescope, you have to know authoritatively who that person is, and that their organization is vouching for them.

A lot of this is **not** engineering. It is building a policy framework and a massively distributed legal framework for trust, and representing that trust and security in metadata that represents and attests to the characteristics about deployments in one or more federation. Establishing massively multilateral trust.

Financial industry use-cases globally. The complexity exists in non-academic sectors.

Why do we call this "OpenID Connect Federation"? This intentionally doesn't change anything about OpenID Connect except for the trust establishment. That is a huge thing for the GAIN implementation. Andreas Solberg in Norway suggested that we make this generalizable / not protocol-specific. There is an example of how to use this to do trust establishment for OpenID Connect federations, but that's not exclusive to OIDC. Can be used for OAuth, SAML, Verifiable Credentials, etc.

Roland Hedberg, who is the creator of this specification, has a lot of experience with academic federations, was able to learn from that experience and bring better ways to handle the complex use cases into this standard.

Wallet in a trust federation of California for issuing an mDL. The driver is in Florida, gets pulled over. The police officer needs to be able to trust a wallet created in a different jurisdiction, with a claim/credential issued in a third jurisdiction.

OIDC federation name should be changed to something much more open. It's a branding challenge. Branding is important in standardization.

VC for access to a bar? Risks, benefits, privacy-perserving ways

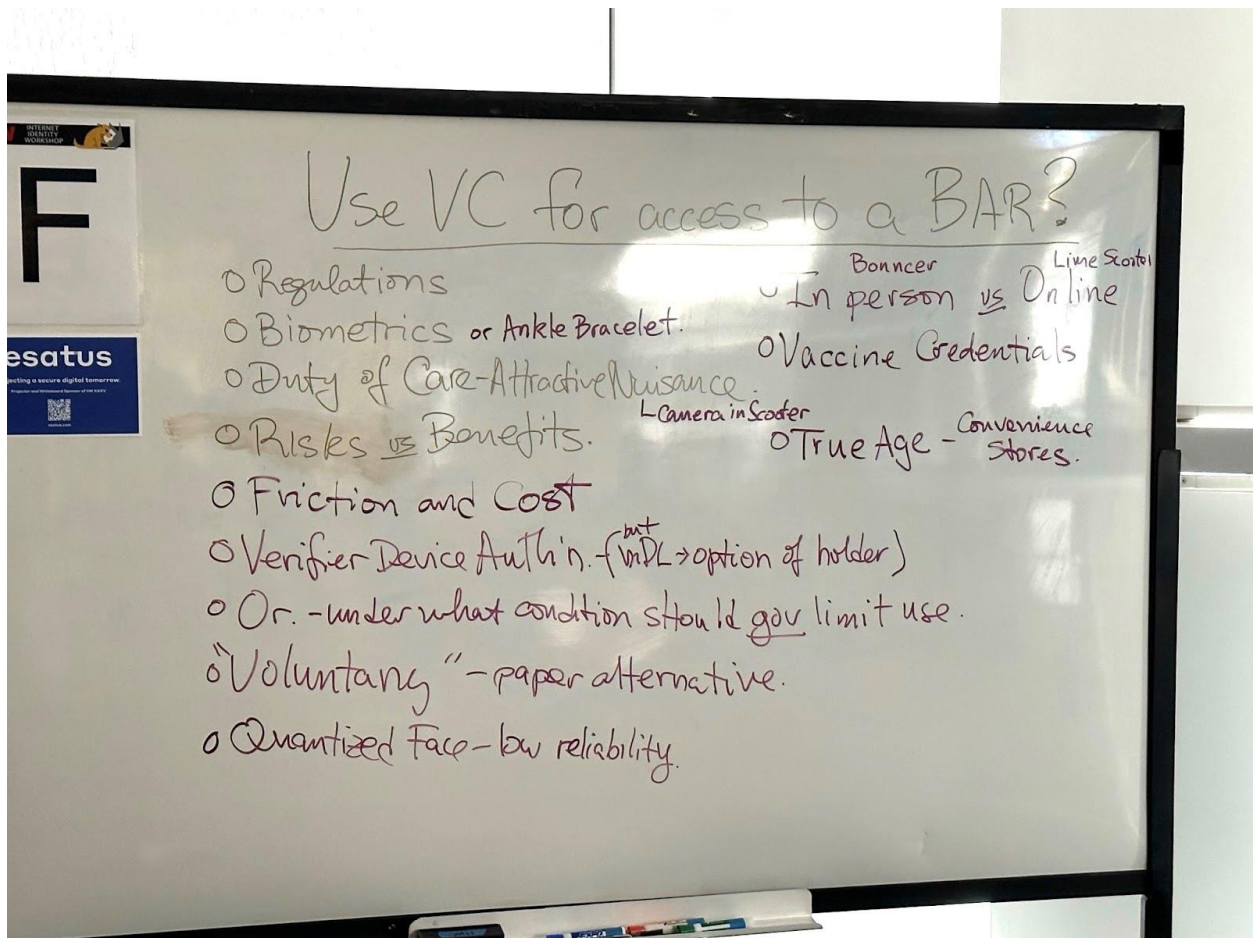
Session Convener: Micha Kraus

Notes-taker(s):

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

Slide deck: <https://nextcloud.idunion.org/s/YyFyPdBf5LsaYCd>

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



Passkeys are great until they're not...

Session Convener: Dean
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

SB786: California law signed in Sept by Gov to allow vital records to be issued in the VC format by county recorders. Learn what we did :-)

Session Convener: Kailya Young
Notes-taker(s): Ed Harris and Herbert Spencer and Kaliya Young

Tags / links to resources / technology discussed, related to this session:
AB2004, SB786, SB1199, VC, Verifiable, Credentials

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

Session leadership by Kaliya Young with. Jamie Minor lobbyist participation by video Conference

SB786 signed into law in in September

Allows California county. recorders to issued vital records in the VC (Verifiable Credential) format

- o Permissive statute, allows counties to implement VCs at the County Clerk

This came about via the Verifiable Credentials Policy Committee, which is nested under the [Blockchain Advocacy Coalition](#).

.

SB 786 is a successor bill to

AB 2004 (that was put forward during covid to do test result sharing and passed both houses but was vetoed because a large fiscal note was attached to it.

SB1199 (that got suspended in appropriations) That is a Trust Framework

CA governor Newson had previously issued an executive order on Web3

There is a working group on verifiable credentials that we participated in.

Pivot this summer amended for verifiable records to be released per blockchain by County
Recorders responsible

An Individual with a large health in the state of CA was present and state there are issues with current handling of health records and in particular birth records

What are the counties doing ? There is only one sentence in the bill. that defines Verifiable. Credentials (VC)

Placer. county and some other (Santa Cruz). Workin on. Some systems

One question is how do we get counties to use uniform standards ?

There multiple state agencies involved in defining how records are formatted

How does a county get the records into a format that is useful to residents of the states?

It was a two year process to get SB786 through the legislator

Do we need to work to make the verifiable credential more defined?

Should the sound ty look at the work for CA state wallet mobile driver license?

One participant thought CA county CIOs and their association will likely play a big part in the implementation of SB 786.

Kaliya will send follow up emails to the signed in attendees of the session.

Improving the UX for Digital Wallets + Brainstorming about User Experience

Session Convener: Sukhi Chuhan, Francisco Corella

Notes-taker(s): Ankur Banerjee & Kimberly Linson

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

Slideshow:

https://docs.google.com/presentation/d/1mgRmr5_qHE5o7znnFrp5Jk6MSHz_te9Oo4cRvDc9uFM/edit?usp=sharing

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

1. QR codes
 1. Have challenges for visually impaired users. Can be an accessibility issue.
 2. QR codes have a limit on how much data can be encoded in them, so if the full data cannot be encoded, it is a link to connect to an endpoint.
 3. UX flow: who shows the QR code? The holder or the verifier/recipient?
2. Social norms
 1. Would you try and check the vaccine status of a friend?
 2. In a high trust society like Sweden, people might trust the government but not in others
 3. Try and reduce the cognitive load on the user. Most of the complexity should be on the verifier, but not the holder
 4. Potential danger to the user of asking users to choose what needs to be shared
 5. Maybe the wallet could prompt the user in case a verifier is asking for too much information on whether they still want to share.
3. Aries DIDComm
 1. Can be used once handshake established to do things like chat
4. Low-internet/offline scenarios
 1. Maybe the rich functionality is in identity wallets, but there's a lowest common fully offline QR that has basic data that can be printed
 2. E.g., when people are travelling they don't have mobile data or wifi to be able to an exchange

Hand written notes below

Sukhi Chohan - Ontario govt

digital wallet - Hyperledger Ames

* customizing based on feedback
from Ontario

Key Findings

anon cred
verifiable credit

* Scan QR codes
- smart health card

*

Methodology

- general research interviews

promoted marginalization

1-1
sessions

test flight

in front of us...

20-30 interviews.

50 for usability

Origins and Heritage.

mobile
application
data on
phone.

research
centers

1.) Giving users options
- identity is personal

*users expect to update
information themselves

→ hell of bureaucracy - Eliminate

log of wallet activity → change the setting / new log
→ what you stored, when etc...

"spectrum of perspective"

✓ connectionless

"decluster the experience"

law doesn't allow selective
disclosure

connection is automatically accepted:

2.) Nudging users to right
actions

→ mental models around physical
ID cards

QR code / Flash the card vs. Scanning QR.

* masking ^{just} attributes *

- Scan QR on the bar.
- This bar is requesting to know over 19
- Yes/No
- Yes - then bar keeper sees the sends photo for in person.

~~~~~>  
Usability test:

Simple & clear to use to  
explain WHAT is  
happen:

- \* Include branding of the VERIFIER
- \* What VC is writing "person"

Complicated because  
a lot to consider but  
MUST be simple to user.

\* Simple screens  
w/ ~~PERMANENT~~ ~~PERMANENT~~ \*  
for all parties

~~~~~>

education

- onboarding & explain features
- explicit tell them only on my phone

peer to peer. — not going anywhere
BUT people don't get
this.

3) Designing for Trust

- Trust is persistent issue
 - Build moral consistency in the overall world experience and start gaining confidence of users w/ smaller ~~stages~~ use cases
-

* Simplify the verification.

START Simple

↳ not banking or health care

4) Making the product accessible

→ blind/low vision (V)

- screen readers

↳ may read out PII??

* QR codes are difficult
for visual impaired.

Other methods should be
explored

* magnify - needs to be
responsive

- can't scan

" bluetooth interaction "

Intermediate screen to educate user

→ Trust registers
are key.....

↳ Bluetooth low energy

user is always scanning

repeated interactions

- auto request / saving

BAR all the time

* longstanding connection
presentation request *

protocol auto request.

"4200 characters in QR code"

~~Agency~~ presenting QR

1st it was a QR code
in the wallet

How flipping to vouchers having
the QR code so

Ka Ping Ye

10 Principles
for key interaction design

Securing interaction design.

- easy way
- implication

1. What are some other UX issues that are important to consider?
2. How can we overcome some of the accessibility/inclusivity challenges?
3. What are some new ideas that we can test w/ digital wallet users?

* Kyle Robinson - Hypotheses

↳ Demo - Energy & Minds

How are we teaching the value
of the credential?

What does the user already do
→ mental model

- Person ID
- Driver's license

low internet / rural.

↳ durable... need a back up

Inform users analog - verifications aren't saving?

DIDComm-terop - Veramo, Aviary Tech, roots.id

Session Convener: [Nick Reynolds](#), Brian Richter

Notes-taker(s): [Italo Borssatto](#)

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

[DIDComm v2 Specification](#)

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

Even with a good spec, testing DIDComm interoperability is hard because parties need to be compatible in the DID methods and transport layer adopted in the tests. Usually each team implements their own DID methods and interoperability tests end up not being common, but during the IIW35 we found some attendees who share common profiles in their solutions.

The interoperability test was executed only between Veramo, Aviary and RootID teams.

During the preparation of the interoperability test some attendees suggested that:

- Having a grant to test interoperability between the projects would be nice.
- Having a docker container that mounts the scenario for a DIDComm interoperability test would also be nice. DIF could be the organizer and maintainer?

The setup for the interoperability test where:

- HTTP as transport layer
- did:web as DID method

The DIDs used in the test:

- VERAMO: did:web: iiw-demo.herokuapp.com
- AVIARY: did:web:aviary.pub
- ROOTS.ID: did:web:...

Veramo implemented an earlier DIDComm specification version and Aviary the latest one, what brought some delay in the test.

What can we do to improve DIDComm interoperability tests:

- A hosted docker container
 - DIF should host?
 - Http endpoint "SendMeDIDComm"
 - Parameters:
 - Anoncrypt
 - Authcrypt
 - None
 - Type of key, only to start:
 - x255/9 2020
 - TrustPing test

This will be discussed in the next DIDComm User Group meeting



Standard Wallet Backup Container

Session Convener: (Telegram)Sam Curren & Lane???

Notes-taker(s): Scott Phillips (Trinsic), Dmitri Zagidulin (MIT/DCC)

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

Intro

- Starting with: Orie's Universal Wallet Interop Spec (Wallet Export Container)
- Conversation has progressed since then <https://w3c-ccg.github.io/universal-wallet-interop-spec/#locked-wallet>

Where should the spec live??

DIF Wallet Security WG

Bundle

Regardless, of encryption envelope, what are we actually exporting? (What goes into the bundle?)

If we're using .tar archive, we can put multiple files into the export. For example, see Open Office File Format. (OpenXML Specification)

Compression

Encryption

- Out of the box Zip encryption - not good
 - Reasonable start: .tag.gz archives
 - see <https://github.com/w3c-ccg/universal-wallet-interop-spec/issues/108>
 - What are we zipping? That is, what is the cryptographic envelope?
 - Recommend: JWE
 - Issue: password(/passphrase)-encrypt it or not?
 - if yes, you should use Argon2 (instead of PBKDF2 or SCrypt) "key stretching algorithm" (which takes a password (which you're hopefully storing in a password manager) and iterates/ hashes it a bunch, and creates a symmetric key suitable for encryption).
 - Ideally, we want the key mgmt steps to mesh with the human instructions (see Tilly hat "put your warranty into the top drawer on the left)).
-
- Software doesn't do it as much with the rise of cloud storage, but backup and restore is still valuable
 - We need to have a good technical solution, but it can't bother the user or it won't be adopted.
 - Jobs For the Future is focusing on wallet interoperability for backup and restore
 - Backup is about data structures, and storage of the private keys
 - When I think about all the data in a wallet, I have 3 things
 - Backup should be bundled
 - Should be compressed (convenience and storage)
 - Should be encrypted for security
 - I would love a nerd to be able to take this, and with the encryption key: decrypt, uncompress, unbundle with standard tooling
 - It would be nice if encrypted zip files were worth it, but they aren't.
 - Common tool usage would be useful for nerds, but not for normal people.
 - .tar.gz would be a good option, but there isn't a good encryption.
 - Encrypt after compression, since good encryption won't have repeating information (and thus won't compress at all)
 - There are non-trivial interactions between encryption and differential backups
 - If you can avoid pass-key encryption, and rely on other key management, that's ideal.
 - The weakest link is the user.
 - In the future, it would be ideal to have MIM key-splitting (eg to shard the key out to the old lady's kids)
 - In the short term, maybe generate a passphrase, print it out, and store it in the fireproof safe.
 - Encrypt notes:
 - AES GCM256 (#108 UWspec)
 - Argon2 - key stretching
 - If you don't immediately share the key via DIDs, you still have the problem of what key can people remember.
 - More focus on the keys being part of the process. (ex, tilly hat warranty in bottom left dresser drawer)
 - Better to allow agility and then tell people to not use certain options.
 - Use JWE: JSON Web Encryption as the envelope

Use Argon2 instead of PBKDF2

- What's the process of involving Ubikey in this workflow?
 - Punt on this, let's talk to ubikey people.
 - Standard practice is generate symmetric key, encrypt with HSM (Ubikey). Then encrypt the bulk data with the symmetric key in software
- The other option that will be valuable for muggles:
 - Store in the device key-store.
 - Rather not directly involve biometrics

Bundle Contents

1. Manifest file with metadata about what is in the container
 1. You can have more forward compatibility, and more ability to evolve the spec quickly.
 2. Allow for continuation files?
 3. Identify standard ways of designating special files (dids, vcs, etc)
 4. CESR: Composable Event Streaming Representation
 5. Let's just assume JSON for now
 6. How to handle files we don't understand - custom file information
 7. Office OpenXML spec ([rels.xml](#) links to other formats)
 8. We should use text-based, human-readable format so that it is at least partially self-documenting
- Open Wallet Foundation is only doing implementations, not specs and standards.

your agent, given a pico

Session Convener: Bruce Conrad

Notes-taker(s): Bruce Conrad

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

Slide deck: <https://bruceatbyu.com/s/IIWXXXV>

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

A reprise of session 6 I, in which we gave away control to some picos.

SESSION #12

What the hell is holder binding? In W3C VCDM/VCs

Session Convener: Paul B.

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

Dear Web5/SSI Founder... (mistakes founders make in this space)

Session Convener: Timothy Ruff

Notes-taker(s): Ankur Banerjee

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

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

1. Focus on the size of the pie, not the size of the slice
 1. Example: a company Digital Trust Ventures invested in had a CEO that had issues with giving away 51% equity. In a few years, walked away with 8 figures.
 2. When Amazon bought Whole Foods, their stock price went up so much that the purchase was essentially free.
 3. Uber 10x'd the size of the "taxi" market.
2. When billionaires invest in things, they often want full control
3. Doing Evernym as a broad identity platform was a mistake, would do it differently if now. But, perhaps wouldn't be in this room.
4. **Don't give up. Persist.**
 1. SSI and Web5 doesn't have an adoption problem. It has obstacles.
 2. Read about [Shackleton's adventure](#), it's inspiring.

Healing Authority Wounds

Session Convener: Kaliya and Surya

Notes-taker(s): Kaliya

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

Healing Authority Wounds - 1 day workshop will happen in 2023.

We went around and heard from people briefly about why they came to the session.

- Healing in self - and how hard it is to try and solve a tech problem when users react from a traumatized place
- Organizations deal with authority wounds/issues
- Effective framework for healing authority wound - why decentralized ID exists - influence community no necessarily triggering.
- Questions that arose include - What are we as a community, we have authority over what we are as human beings - what would transform?
- I trusted the Federal Government with my information as an employee - but then the information was breached (in OPM hack). Trust Authority to investigate and prosecute.
- Complex PTSD in a range of contexts, personal life, work, standards processes - working in the educational community - what does it look like to work to prevent trauma from happening - because when it is present one stops learning
- Trauma is draining talent pool.

Kaliya shared some of what was inspired the idea of the workshop.

Came out of a conversation with Jorge Lopez after Kaliya presented about unconferences - that happened at DWeb Camp. He shared about his own experience being part of a leadership team leading a community/project the [Economic Space Agency](#) that melted down on reflection part of this was due to Authority Wounds.

Surya Kramer was also at DWeb Camp and is a process facilitator and somatic experience design expert. The three of us had a great set of dialogues about how to collaborate together on putting on a workshop about Healing Authority Wounds.

This session at IIW was our first putting forward of this idea within a technical community.

Here are some sketches of some of the topics we discussed in the.

Social DNA and the capacity for leadership

Awareness out of marginalize

Structures of Agreement - and how to signal to folks who are not navigating well.

Engagement in a group process - not seen and not tracked

Leadership needs to model these things of good structure of agreement for example to ask forgiveness, when modeled - something cracks open.

We talked about architecture discussion

Level of confidence - and degree of authority.

The role of Authority and the gap between projection and perception

The Paradigm or expectation of who people are.

Privacy is not understanding

Authority and Relationships go bad.

Behavior authority in each of us

This is where there is an opportunity for real dialogue.

Trust & Respect - what is missing? - collective agreement

Filter out destructive ways of dealing with each other.

Emotional intelligence of managers.

There is some opportunity to understand root causes of these issues - a Bi-lateral failure of empath can lead to degradation.

Awareness prevents steps into authority when needed to but didn't have a good model for how it would work.

We can't become the thing we don't have.

Cultures of Accountability are needed to support and defend against polarization.

We need more options and perspectives including seeing conflict as a doorway to new information and options.

The Obstacle is the way.

Mediation is emotional work.

Health leadership is key

Caring to Care

In authority role to create openness

Training to bring it into the center.

Protocols for engagement in particular listening.

Groups that exist - never going to be in group

How to create the ability to call people in conversation

Create council neutral environment to call people into accountability

Create a social grid of intention.

Sit with the difficult - where is my trauma attached in 'dark matter'

Un spoken and discomfort not uncomfortable talking about how they are.

Rebooting did:ethr

Session Convener: Lauritz Leifermann, Dennis von der Bey, Philipp Bolte

Notes-taker(s): Philipp Bolte, [Italo Borssatto](#)

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

did method, ethereum, did:ethr, rebooting

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

Original notes: <https://hackmd.io/x15fSXiqQESsI9cZxCuKtQ>

Current problems:

- Diverging smart contract versions
- Smart contract development and deployment life cycle
- No upgradability (migration is hard)
- Replay attack vulnerability (no nonce tracking on addDelegateSigned)
 - Non-standard meta txn hashing (no usage of EIP-712)
- Unused delegate mapping
- Specification governance
- Missing assertionMethod for resolvers
- Hard link between controller key material and assertion method
- No audit
- Not maintained
- Going through the problems:
 - Since the deployment of did:ethr, the DID Core spec has changed → is the current version of did:ethr following the spec? → we don't know but probably not
 - We need to find a funding model for how to include the community + a governance model around it
 - Did:pkh is competition we have to compete with → even though its not spec compliant (no support for service endpoints, key rotation, ...)
 - Should we do a working group and talk to the Ethereum Foundation? → Might be helpful because another company has indicated interest in supporting changin did:ethr
 - On chain upgradability brings securities risks
- Ideas:
 - Maybe we should rename did:ethr → did:eth
 - did:ens and did:ethr could be the same thing in the future
 - Governance:
 - Two aspects: who controls the spec and the contract
 - We don't need/ want tokens
 - Funding: Maybe proposal to ENS foundation/ Ethereum foundation → also a big marketing tool
 - Maybe put the code into a DIF working group for distributing governance → maybe it's too big?

- DID DAO could be a central place for multiple smart contracts containing different SSI tools (revocation, did management, ...)
- We don't need a DAO on day 1
- If governance fails this trust in the DID registry fails → not rely on one smart contract maybe → there is an EIP that allows subscriptions between different smart contracts
- [ethr-did-dao channel in Veramo discord](#) is a good place for discussion on that
- The updated version has to be cheap/ not pricey to use
 - We could benefit from a Sidetree option?
 - Maybe usage of Anychain → cheap option that can turn into an optimistic rollup
- **Ethereum DID WG**
 - Schedule a call where we all attend every 2 weeks, Thursday 12pm ET/ 6pm CET → we may rotate the time
 - Done by the Veramo team in their Discord
 - Meetings should be recorded and put into

Attendees for Ethereum DID WG:

| Name | E-Mail |
|---------------------------------|------------------------------|
| Hersh Patel | hersh.patel@trinsic.id |
| Ajay Jadhav | ajay@ayanworks.com |
| Philipp Bolte | philipp@bolte.id |
| Dennis von der Bey | dennis@vonderbey.eu |
| Lauritz Leifermann | laudileif@gmail.com |
| Otto Mora | omora@polygon.technology |
| Dale Olds | olds@vmware.com |
| Stephan Baur | stephan.x.baur@kp.org |
| Doug King | dwking@gmail.com |
| Keith Kowal | keith.kowal@sworldslabs.com |
| Italo Borssatto | italo.borssatto@mesh.xyz |
| Reinard Lazuardi Kuwandy | reinard.l.kuwandy@gdplabs.id |
| Nick Reynolds | nick.reynolds@mesh.xyz |
| Haydar Majeed | haydar@privatize.io |

Self-sovereign human-based identity for the next billion. 800K users today.

Session Convener: Remco + Paolo

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

YOUR greatest standardization regret!

Session Convener: Andrew Hughes

Notes-taker(s): Notes were deliberately not taken.

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

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

We had a great mix of new and experienced standards committee participants. There were great stories of things that seemed like good ideas at the time but turned out to be not so great once they hit reality.

Interesting insights into some specific debates from 10-15 years ago that resulted in spec features that people continue to use (or abuse) today.

Grateful for everyone who came and shared their stories!

Dazzle Office Hours

Session Convener: Johannes Ernst

Notes-taker(s): Johannes Ernst

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

<https://dazzle.town/>

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

We held the weekly Dazzle community office hours at IIW with remote participation.

Discussed various questions about Dazzle, technology, product and strategy. Showed some software (similar to the demos in Demo hour this week) and some wireframes for future rooms in the Data Palace. Also discussed some semantic models that we are using.

Practical applications and considerations of programmable VCs

Session Convener: Howard

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

Can DAO / NFT be used for Open Source Ecosystem

Session Convener: Mike Schwartz

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:

Mike Schwartz presented an overview of his NSF POSE proposal which can be found at <https://gluu.co/pose2> which proposes to use a DAO, NFT's and Tokens in a Web 3 ecosystem to better incentivize an open source ecosystem.

Lively discussion ensued.

Slides are here: <https://gluu.co/ato-web3-2022>

* POSE = Pathways to Open Source Ecosystems

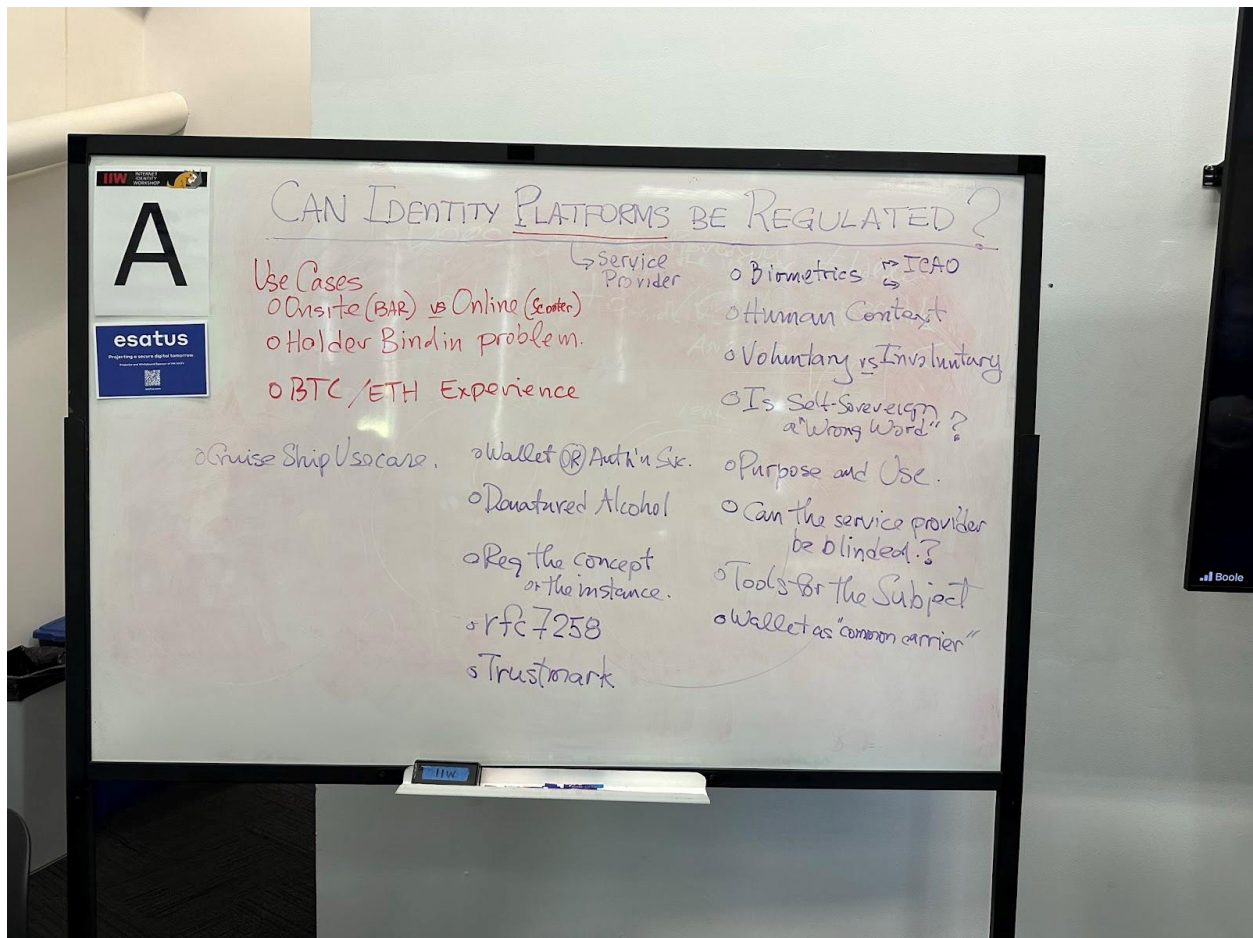
SESSION #13

Can Digital Identity Platforms be Regulated?

Session Convener: Adrian Gropper, Ken G.

Notes-taker(s):

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



Self-Sovereign Dapps

Session Convener: Sam Gbafa

Notes-taker(s): Elissa Maercklein

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

Self-Sovereign Dapps:

- The goal is to bring SSI tooling into Web3, where people already have public/private key pairs
 - A Dapp is a “web3” application or software that interacts with a smart contract or blockchain in some way - this is a very loose, fluid definition
 - Sign-In with Ethereum - a way to sign into an application using your Ethereum-based account with authentication
 - Authentication vs Authorization
 - Authentication: Hi, this is me!
 - Authorization: Yes, you can have some permissions (informed consent!)
 - ReCap extends SIWE to include authorizations
 - Provision access to self-hosted data or verifiable credentials
 - i.e. new web3 Instagram: Provision access to settings, to photos, to friends list
- How can we extend beyond just signing in?
 - Applications we use - Uber, Twitter, etc. - they control the identifier and can remove/delete your account if they want to
 - SSX Library - Self-Sovereign Anything: use SIWE to establish a session for an app instead of a username and password
 - How do you now have VCs with the key?
 - **Rebase**: self-issue credentials, i.e. sign a statement proving you are the owner of a Twitter account, post tweet & witness verifies, Rebase issues a Verifiable Credential. User for a Dapp now can have this VC in their data store and give access to Dapp for the data store
 - **Kepler**: store credentials in a self-hosted data vault, provision access to only that folder
 - This helps to limit cost of compliance without a need to store potentially high-risk data, like healthcare data, while empowering individuals to store and maintain this data themselves
 - Also enables revocation by sending to a node that then distributes further
 - **SSX** gives simple API to allow Dapp developers to interact with these libraries
 - Users show up with key and can do everything
- How would I limit interaction in a smart contract to require proof from a VC before interacting?
 - Topic is an active area of research
 - Paper released last month that shared how a smart contract could produce verifiable credentials
- EIP under review to have same key-pair issue encryption keys, as well
- [Issuing Verifiable Credentials with Smart Contracts Talk](#)

Web5 Ontology work group. Let's discuss authentic data, relationships and disclosure levels.

Session Convener: Jim M. Timothy R. Bry B.

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

Bank On It! Identity in Financial Services

Session Convener: Tony Jin

Notes-taker(s): Tony Jin, <other>

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

- Canada & bank consortium: <https://securekey.com/>
- Early Warning Systems → Zelle & Authentify

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

- What are the main drivers for ID in financial services?
 - Option 1: it all comes down to cost → efficiencies, fraud
 - Option 2: customers have a lot of pain of repeat entry, really annoying thing for the customer
 - Option 3: might be driven by policies from government
 - Mostly conforming to open banking or to
 - Customer types: some are just baseline compliant, others take advantage of the requirement to modernize
 - Option 4: mitigating risk and non-repudiation
 - Are you you, can you rely on that from an audit perspective
 - Confirming identity of good actors and preventing the usage by a bad actor
- What is digital ID adoption in other countries
 - Singapore Singpass (covered in prior info session)
 - Sweden → BankID, hosted by the banks themselves, can be used outside of banks
 - Bank consortium runs the systems, relying parties are paying to use it
- Why do we need addresses for AML?
 - A legacy system from when we used to send physical bank statements
 - Also now regulatorily required as to not exclude certain consumers who don't use emails / phone numbers
 - Its a broken system → now people move around so much

- Underserved groups without clear identity & history that limit access to financial services
 - Homeless, nonprofits exist to help
 - New immigrants → for instance Canada has rental housing programs for new immigrants
- Maybe regulators need to educate / add more nuance based on risk profile, different levels of assurance required
 - Challenges around regulator risk appetite → banks are fearful of overstepping and being fined, also challenges around technical implementation
 - Could be a challenge around redlining and excluding certain socio-economic groups
- Mexico example: certain levels of bank accounts with certain transaction limits can be created with limited KYC, have not seen in the US
- Simplify a lot of things if you can have a digital credential that can replace wet signatures → what's the financial community around VCs?
 - Hypothesis: driven primarily by regulators on what banks are allowed to do
- Credit Unions & Co-Ops are good examples for early GTM
- Technology question: what risk & ID solutions are being used to secure transactions?
 - In the US, Canada, etc. Merchant is not regulated, its up to them to determine their risk level on if they want to use solutions such as 3D Secure (expensive)
 - For e-commerce merchants, this becomes a tradeoff of risk (chargebacks), and conversion of sales
 - In Canada, very stringent PCI regulation protects cardholder information. Merchants are very afraid so very quick to adopt these technologies to protect their consumer and their brands and avoid fines
- Open source space: banks actually want to come to the table to discuss and participate rather than just talk with vendors to have things done
- Traditional banks are important to meet needs of consumers → started to meet a specific need of consumers and then expand to broader use cases
 - E.g., China: AliPay started as an escrow system, and then became a widespread payment system. Now can transact almost entirely without cash
 - E.g., Tencent is building a payment system for the gaming ecosystem
 - In the US everyone wants to hold onto the payment rails because its lucrative, hence slower innovation & adoption of new pieces
 - Is the limited adoption for better digital payments due to identity & fraud/risk concerns or is it due to regulatory & market capture by incumbents?
 - E.g., India has UPI payment systems based on Aadhaar, being used across the entire country. Originally was driven by more efficient government disbursements
 - E.g., Costa Rica central bank has created this interchange system with settlement and low dollar value payments can be sent for free, instantly
 - Phone numbers are tied to banks accounts that create accountability / KYC
- Alipay uses progressive levels of KYC
 - Anyone can send payments using a basic phone link
 - Requires additional KYC to receive payments e.g., as a merchant

Modular Blockchain Designs + ZK Rollups (Why blockchain will play important role in the future of SSI)

Session Convener: [Rouven Heck](#)

Notes-taker(s): [Italo Borssatto](#)

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

Ethereum "modular blockchains" concept where basically blockchain solutions solve each of this problems separately:

- Execution
 - Running smart contracts
- Data availability
 - Storing the smart contracts results
- Settlement
 - Guaranteeing consensus

Economic incentive to run a node. Sidetree doesn't offer this incentive as well.

Is identity a "double spend" problem? Theoratically, yes! To guarantee the last state.

In an end user centric solution we need a decentralized infra-structure to guarantee user data protection.

Clarification. When we talk about blockchain, what are we talking about? General model of a replicated mutable ledger. Not blockchain that stores distinct ledgers. A monolithic blockchain.

The idea in "modular blockchain" is that execution, data availability and settlement will end up being implemented by distinct modules in the blockchain solution.

So, we'll be able to receive proofs from an execution, store them in a separate network and use a settlement module to check if the results are accepted.

The proof production is quite heavy, but now it is possible to create recursive proofs, where several proofs are combined and the settlement verification comes in constant time execution.

There are options where storage can be made by the user and only proofs are kept available publicly.

Independent incentivized backend which guarantees settlement.

Blockchain's initial idea guarantees that anyone can run the blockchain from start to finish and see that the result is right.

Mathematical execution proofs (ZKP) guarantee the latest state just by checking a proof, without the need to run the whole blockchain transactions to get to the last state.

Settlement layer won't accept new blocks if execution is not correct.

The proofs are all stored in the settlement module. Not sure if middle states can be recovered. Using an L1 as reference it's possible.

Execution can be done locally and settlement can guarantee, by the proof, that the execution was correct.

Parts of a DID document could be checked without publishing the whole DID document.

A censorship resistance can be achieved with ZK technology.

In the identity space we can have data which are not public, which is very important for PII protection, but you can still prove some claims.

Nobody has developed a ZK DID method. There are around 6 teams working in modular blockchain solutions and in some months building solution on that will probably be much easier.

Tezos ecosystem is moving to modular blockchain. Salastria is focusing on data availability.

We should start discussing using each piece of these new modular blockchain solutions to build new identity solutions using them. Discussing what each solution could bring as a benefit to these ecosystems would be nice.

Not relying on tools like Infura and being able to trust and verify VCs in your mobile device for example, would be possible with ZK proofs.

This is not an exclusivity of the Ethereum ecosystem. We are talking about layer 2 solutions in any other ecosystem. Users would be able to choose the settlement solution to be adopted.

The choice of blockchain modules will happen according to the use case you want to cover.

Let's talk about the byway. (Not the information highway)

Session Convener: Joyce + Doc

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

Don't Use DIDs use DID URLs

Session Convener: Joe Andrieu

Notes-taker(s): Ed Harris

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

- <https://diddirectory.com/cosmos>

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

- Detailed implementation of this approach may be viewed at <https://diddirectory.com/cosmos>

LABEL--> SUBJECT, Pointing to the control asset in the VDR not real worlds things, need ID to point to Offchain things, physical parcel, have hash to doc that describes it

Ii. Dids AND NFTS

- NFT IS ON CHAIN, USE REF TO NFT,

III. Need did to point to nfts,

- Context of given nft, ref things that are not control asset ie /owner, describes who the owner is
- Example, of standard
 - Did:ex:abc
 - Did:ex:abc#owner
 - Did:ex:abc/image.png
 - Label is DID, generate a did document based on the the current subject/owner,
 - Diddirectoary.com/cosmos (Live url)
 - Best example is in the DID cosmos, find spec for any DID you hear about
 - Update on Diddirectory
 - Mirrors w3c registry pinged every minture, echos registry
 - Email contact, can auth. In did directory and take control, can put complex landing page with images, bullets and links, go here and find the method instead of needle in the haystack to find the links
 - Conversation, ferwer did mejtods
 - Learnings, supper awsome to have independent soverin name spaces, whant interop sapces
 - Example
 1. Did:ford for everhthing FORD controls
 2. Future, millions of DID moethods
 - Cosmos is a usage pattern, initially though it would be a family
 - My subject is the control asset, the did key is pointing to the ????
 - Jus use dids to point ot the thing
 1. Counter
 1. vdr between subject and label, how do you speak about Verifiable Data Registry (where state is measured ie BTC, ETH, etc)
 - We took diff approach and get layering

- Client wants to store Did document in IPFS, anchored on chain, discovery on chain , BCR has this pattern (joe), replacement or augmentation, got through the anchor to get to the doc
- ? Can I use did URN , alternative did:ipnfs instead of IPFS (Johnnie did this --Joe) cyryp bound pointers can change with consistent IPFS
- ? Subject iuteefl is the VDR
 1. Is it possible, without subject being the VDR itself?
 1. Je, had this question doing cosmos, ujust use the ref did# (did hashtag, did doc can have verifidation relationships, verify VC from owner from the crypto that is owner, as separate), use DID, run into ambiguity, with naming, using the spec can now handle this issue in did sctructure url instead of (did spec over 3 years)
- ?best practiceices for someone new into this space
 1. Somewhere to collect this is useful, , need best practice patterns
 2. Implementation guide is the best now, cant change after december
 3. Next thing is group control over the listings, now it is email bound, need org to use and own it (did: auth, need authntneticate archi anchored to public ????)
- ?Tying dids to nfts,
 1. Problem, no universal identifier, this interops for the chains
 2. Make it a url and it is a universal identifier (did cosmos work leverages some of the CAP 19)
 1. Did url pattern for NFT to have its own namespace bound to the unique NFT
- List
 1. 4 ways tolink resource
 1. Put info in did doc
 2. URL with Hash, when you get back can verify, privacy compliant
 3. Not give URL, just give #, selling house, not giving info until legit buyer with agent, can see lien report for CC and termite etc
 4. Most privacy perserrving
 - Hash Graph, do not know how many resources there are #graph
 - If put properties directly in DID doc, no way to have privacy version that is equivalent, they will hard code to the property
- ? What is the rest of the DID doc
 1. Did cosmos work
 1. SDK, strip cosmos, to to hub and look for the next part,
 - Exis:.....how to reach router on the cosmos hub
 - Structured by modules, here is how you talk to the right module
 - Complex nfts
 - Green electric production with evidence of approval from UN, cert, audit of facility, all bundleed into complex nft all

- in NFT module, route to the object with Business Logic echo back to the module
 - 2. No code NFT Module, meet pattern allowed them to be minted
- Limited spec?
 - 1. Thought son iot???
 - 1. Walk around the endpoints, point to different services, good chunk can be done with services, mental model shift, is it downloadable resource or mental model
 - 2. Canonical, way to do it, json v json/ld - Joe Anser (missed questions)
 - Some folks prefer registry, this is not good in decentralized world, crime against identity
 - Did urls are the undiscovered rest of the iceberg in dids, friend left Mr Reed
- ?can did rep multiple subjects, url name space rep multiple subjects
 - 2 questions
 - 1. Today did is expected to point to one thing subject, could be a group all americans
 - 2. New arch, single did can have infinite number of refs in namespace, did resource # and did ?method
 - 3. In this pattern
 - 1. Label is did
 - 2. Subject is VDR control asset (did ion), multiple decentralized systems (resolve the did by the VDR)
 - 3. Each did resp a single nft, yes
- Questions, a lot of data in resolution of did???
 - Carbon credit stuff, data is in vcs, did model is today
 - Project, certification, audit/auditor, energy/smart meter, all VCs, with pointer using this method, VC can be in the Did doc or url in DID pointing to the VC...
 - Many use cases, overlapping the DID doc., point of view
 - If not nfts, then would not come at it this way
 - Have the VC this is an nft, we wanted to bind what the NFT is closest to the control asset as possible
 - ?did url use, don't specify the path in specs, question,
 - Joe, unfortunate spec
 - Query, path, fragment parts is the pattern (keys in did doc is snatar, using did query is emergent) - still figuring it out
 - In the spec that these are different things
- Resource, for more that you did with cosmos
 - Url, diddirectory.com/cosmos (echo w3c reg with help)
 -

Further Exploration of DID and VC Data Architecture with Category Theory

Session Convener: Brent Shambaugh

Notes-taker(s): Brent Shambaugh

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

<https://www.categoricaldata.net/>

<https://github.com/bshambaugh/Explorations-of-Category-Theory-for-Self-Sovereign-Identity>

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

Some person asked: Is there a Category for RDF? I answered that I thought that Benjamin Braatz Thesis defined this.

Some person suggested that Brent should look at Graph Database for Category Theory by Robert Roseboro.

F. William Law ... Category of.. (((?)))

Category Theory for Federated Semantic AI

Know some equivalence ... logically Equivalent

Transfer scope to another...

Look at TLA+ ==> Do you know about proof. Amazon Proofs for Distributed Systems.

What is possible with asynchronous programming & Pi Calculus?

Schedule Meeting with Ryan Wisnesky: [<https://www.wisnesky.net/>] , explore links

DID Don't explain it. Have users experience it!

Session Convener: Bryan

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:dns - Current version and ideas for improvements

Session Convener: [Markus Sabadello](#), [Tomislav Markovski](#)

Notes-taker(s): Ankur Banerjee

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

1. [did:dns specification](#) - this is the main documentation on this project.
2. [Universal Resolver](#) (check out the did:web examples)

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

1. Existing DID methods
 1. Ledger-based, e.g., Indy, ION, cheqd
 2. Ledgerless ones like did:key
 3. Many people now just use did:web instead where the file is published at `.well-known/did.json` e.g., [did:web:iiw-demo.herokuapp.com](#)
2. Current version of did:dns
 1. Eliminates the need to have a web server, just a DNS record needed. On the flip side, it requires access to domain control.
 2. Uses record type URI, which is not very common.
 3. Current examples use did:key, which can be specified in a compressed form and expanded to a default DIDDoc.
 4. Another idea is using TXT records. Different providers have different limits
3. Future ideas
 1. Look at what [ENS](#) is doing since they are using DNS-like resolution. Other examples are [Unstoppable Domains](#) and [Porkbun](#).

Use [SRV records](#) for service endpoints? This is currently used for SIP, XMPP etc other types of services so the usage is well understood. SRV records also have

SESSION #14

Authentic Web++

Session Convener: Sam Smith, Neil Thomson

Notes-taker(s): Phil Fearheller, Neil Thomson

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

- Authenticity
 - GLEIF
 - [Digital Identity: It's all about Authenticity](#)
- The cheap pseudonymity problem
 - [The Social Cost of Cheap Pseudonyms \(paper:Freidman, Resnick\)](#)
- Reputation

Sam Smith (see [KERI Resources site](#) for KERI, ACDC, Reputation)

- YouTube
 - [Reputation and Two Sided Networks \(Video\)](#)
- [Open Reputation Framework](#)
- [Open Reputation](#)
- [Authentic Data - Simple \(in Principle\)](#)

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

Note: This is an edited, blended version of Phil Fearheller and Neil Thomson's notes

Sam Smith "The internet is broken (not because we don't understand each other, but) because we can't trust each other. If we want to exchange value, we need to trust - the only trust is verifiable ownership of each other's cryptonym."

Goals (of the Authentic Web):

- Secure traceability of data to its source
- Authentic Web = Trust on Steroids
- Death of Spam

Basis for authenticity (of an Entity)

- Type 1 Secure attribution to a cryptonym
- Type 2 Linkage (for the cryptonym) to a verifiable entity (person, legal organization, thing/device)

Observation:

- Type 1 is the “reputation” case, where attribution, mutual attestation, endorsement, etc. to the cryptonym by third parties, which is not dependent on a “trust anchor” for their attribution
- Type 2 is the “trust anchor” case where a entity providing attestation is doing so from an authoritative position, under accreditation by regulation, to a trust anchor (e.g., GLEIF/vLEIs) and the ToIP Issuer, Holder, Verifier trust model
- Data authenticity - verifiable data - “Authentic provenance chain” connection of data to it’s source

Type 1 is all about:

- Control of the identifier (controlling the keys)
- Secure attribution (authentic provenance chaining to the entity providing the reputation/attribution).

Most of this IIW session discusses Type 1 - the use of reputation (as opposed to VCs, Issuers).

Observation

- The non-digital world uses a mix of accredited credentials and reputation (e.g. academic, professional credentials; personal & professional reputation)
- Failure use case - the very recent Twitter “Blue Check Mark” fiasco, where Twitter clearly did not vet the users claiming a name/identity and most certainly not through secure attribution and proof of ownership of and identifying information.

Solving the *Cheap Pseudonymity* problem:

- “Cheap pseudonyms (as identifiers) introduces opportunities to misbehave without paying reputational consequences

Solving the

Some solutions to the “cheap pseudonym” problem:

- Proof of Work (POW)
- Proof of Stake (POS)
- Reputation

All of these have a “cost” to acquire, which (particularly reputation) should be increasingly expensive to walk away from if you abandon a cryptonym. In other words, a compromised reputation should see that reputation collapse or be severely impacted (in a non-linear manner).

In many cases, there can be an “imbalance of power” between the entities providing and receiving attestation

- Opening a Bank account - is cheap for the bank, but expensive for the person
 - Bank has all the power, you have little
 - Bank can act as a reference to reputation for your bank identifier
 - If you give a poor reputation to the bank, you are but one in thousands of customers influencing the bank’s reputation

“Don’t trust a pseudonym any more than the value of their reputation” (against that pseudonym)

Reputation - value/metric of behavior within a context which enables future (and type) of interaction. Past behavior (for which reputation is based) is assumed to be a predictor of future behavior

Reputation Portability (the walled garden problem)

- Facebook - while there is pressure in the EU to allow FB users to extract and move their data, FB is highly unlikely to allow you to extract relationships (and reputation) to transfer to other social media.
- Amazon (shopping site) when they added the ability to rate reviews on a product, they made the reputation of reviews expensive. But the problem is that Amazon owns that reputation and you can't take it with you.

What is also of interest is “reflexive” reputation in that Amazon also allowed the raters (of a product or service) able to rate other raters.

Trust Anchors

Trusted entities that bestow reputation on pseudonyms. GLEIF with the LEI is an example of a Trust Anchor.

Reputation - Behavior based contextual predictor of future behavior

Transitive Trust - When reputation in one context can be used as a predictor of behavior in another context.

Verifiable Credentials... borrowing one entity's reputation (e.g., GLEIF and loaning it to another entity (digital letters of reference)

VC is a type of reference

- Reputation by reference (GLEIF -> Issuers -> (legal entities) Organization - Role - Person (assigned to the Role))

Next Step(s) - Creating a Manifesto

Items for the Manifesto:

- What is the community of practice
- Understanding reputation is contextual and we need a mechanism to formalize that
- Reputation is reflexive
- Reputation requires secure attribution - details
- Reputation is contextual - need to formalize
- How to define ways for self-organization of reputation that is all top down and versionable.
- Mixing “authoritative” and “reflexive” reputation

What's the DIF(F)? Decentralized Identity Foundation Explained

Session Convener: Chris Kelly

Notes-taker(s): -

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

[Link to Slides](#)

[DIF Website](#) - a great place to start

[DIF Org FAQ](#)

[DIF Grants information](#)

[DIF Public Calendar](#)

[DIF Blog](#)

[DIF Meeting Recording Archive](#)

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

The Decentralized Identity Foundation (DIF) is a member-led, not-for-profit organization focused on building foundational technology elements, and working alongside other partner organizations, to deliver an open, standards-based, accessible, and inclusive identity ecosystem.

Our members include a wide cross-section of industry, from large corporate enterprises to individual contributors along with liaison agreements with Governments, Educational institutions, researchers, and associated industry bodies.

Founded in 2017, our mission is to advance the interests of the decentralized identity community, including performing research and development to advance “pre-competitive” technical foundations towards established interoperable, global standards.

DIF is proud to have supported development of two central standards of the decentralized identity industry, the lower-level specifications Verifiable Credentials Data Model and the Decentralized Identifier specification, which are both iterated on, and hosted at the Worldwide Web Consortium (W3C). The Foundation is home to a lively and open ecosystem of software companies aligning on everything from product design and UX down to the translation engines and connective tissue to integrate Verifiable Credentials and DIDs into today’s software systems.

The Decentralized Identity Foundation is proud to fulfill a unique role in the digital identity ecosystem by providing an inclusive, transparent community and IPR framework, to expand upon these open-source specifications and deliver other foundational elements which are key to growth, functionality and sustainability of decentralized identity donations, continuation of work, longevity. All work carried out at DIF is available to the wider community under free, open-source licenses: for more information, [see DIF FAQ](#) -

Trans Identity

Session Convener: Nicole Roy

Notes-taker(s): Nicole, Dmitry

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

Steve Yegge's Google platforms rant:

<https://gist.github.com/nckroy/d5d65046fb4fbcf645693a80e32a6989>

Falsehoods programmers believe about names:

<https://www.kalzumeus.com/2010/06/17/falsehoods-programmers-believe-about-names/>

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

Assumptions programmers make about names

Steve Yegge's google platforms rant - accessibility

Optionality of data

Not limiting input artificially

Enabling use of elastic data models that can change along with society

Intentionality about addressing "Data model debt"

Jurisdictional conflict about legal documents (or not) needed for changing certain data elements

Use of SSI technologies to support identity in transition

Pub/sub mechanisms for distribution of identity change data to relying parties, a la IETF secevent

"Stop collecting that data"

Give people choices about "no" options on things like gender marker - don't assume gender is something a person even expresses or identifies with

Verifiable Voting: Using VCs, VPs, + ZAPs to solve cryptographic voting

Session Convener: Sam Gbafa

Notes-taker(s): Elissa Maercklein

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

- **Examples of Capabilities:**

- <https://w3c-ccg.github.io/zcap-spec/>

- <https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/41892.pdf>

- [USVoteFoundation.org research report](https://www.usvote.foundation/research-report)

- [MACI 1.0](#) and report from Vitalik on [Minimal anti-collusion infrastructure](#) [here](#)

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

Goal: Hypothesize voting systems that are cryptographically backed

- **Architecture:**
 - Issuer can issue a VC saying to a Holder saying they are a registered voter
 - Holder can submit vote + VC in a Ballot VP to cast their vote to a Tally
 - Ballot VP properties: prove you are the holder of the VC, and that it contains a vote, should be included in the Tally
 - Tally (could be smart contract or program)
 - Implement an accumulator
 - Holder can always verify that their vote is in an accumulator (you can't see who they voted for, just that the vote is included)
 - Privacy preserving, verifiable
- **Questions:**
 - **How do we trust that the Tally only includes valid votes?**
 - Store hash of presentations that could show everyone who voted
 - Governance policy that if X people made a claim, require resubmit for secondary verification
 - **Is the accumulator self-certifying?**
 - Depends on type of accumulator
 - Merkle tree to verify vote exists in tree, not necessarily who the vote is by/for
 - **How could we facilitate delegatable voting or conditional voting?**
 - Cache at a certain point but executed later
 - See next question on capability, not credentials (Z-caps have delegation built in)
 - **What if you're issued a capability, not a credential? The two should not be conflated**
 - Removes concerns about what is hashed here & can expose some metadata about what is contained within
 - Credential exists to make attestations (facts) compared to capability of actually taking the action
 - Can result in mis-delegated authorizations in larger scale, complex systems
 - Could facilitate the ability to change the vote if needed
 - Z-caps have delegation built into the architecture
 - **What if you also receive a proof while voting?**
 - Can selectively disclose that you voted without sharing who you voted for
 - Could potentially accumulate off of the proof
 - Required for a recount if results are questioned, people can't change their vote after the fact
 - Needs to be bound with the voting action, otherwise proof issuer could just issue more proofs and recount would be different than initial results
 - Acts functionally as a receipt for voting
 - People who delegate might want to confirm the person who they delegated to did, in fact, cast a vote
 - **How do we avoid side-channel re-correlation?**
 - You'd essentially have to use standard practices for obfuscating identity, i.e. hide internet address, so on
- **Use Cases:**
 - Probably not an American national digital voting system: [USVoteFoundation.org research report](https://www.usvote.org/research-report) about the viability of an End-to-End verifiable voting system and found it's not feasible

- Could be: HOA voting, student body elections, PTA elections, DAO governance
- **Capabilities:**
 - Some examples of object capabilities
 - <https://w3c-ccg.github.io/zcap-spec/>
 - <https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/41892.pdf>

What did we learn from NSTIC + What does government need to know to re-establish/re-charge identity ecosystem.

Session Convener: Kaliya and Ken Gantt

Notes-taker(s): Travis Edwards

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

[NSTIC Report](#)

[DHS Office of Biometric Identity Management](#)

[Biometric.Gov](#)

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

This session is 3 of 3 designed to inform, discuss, and gather feedback on the topic of identity ecosystems and varying roles of government, industry, and the public. This session was co-hosted with Kaliya who was involved directly with NSTIC process in 2010.

NSTIC or NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE Overview

Kaliya outlined the experiences dealing with NSTIC circa 2010. General consensus was this was important activity, that had a “good concept but failed launch”.

Of note ... “National” and “Identity” in NSTIC title were placed as far apart as possible in the title to not be confused with an national identity program or project.

NSTIC = NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE

Noted concerns from participants circa 2010 included;

1. lack of shared understanding, 2) too many self interests, 3) there were more discussions on how to setup board of advisors and leadership of group than discussions about current status of the issue, 4) lack of access, 5) lack of shared understandings and terminology, 6) lack of diversity representation in attendees

Loop that never got resolved related to creation of a trust framework. Why is the government asking the public to do this...Gov creates identities and then asks public to take on risk and liability. Government was not issuing digital anything so its public risk. How do to get from analog to digital

identity - vision at time was that the private sector would do identity proofing and guarantee identities in some new system and this trust framework would help it interoperate. They got really recursive fast...Government put out a strategy document then asked the community how it should run, electing a steering committee, and ended up convening amazing gatherings but facilitated them poorly.

Government “talked at the private sector” a lot...

Governance workshop in Hilton basement with 300 people. There were no introductions so we left not knowing who was in the room.

Only the bigs in industry could afford to be there...

Second Speaker -

NSTIC was a document. We are going to go to the moon but no framework for how it was going to happen. They spun up the Identity Ecosystem Steering Group with public/private/government collaboration. Great idea.

NSTIC and IDSG activities were good activities supported by President Obama.

They wanted it to be self organizing but you had 300 people with little niche of identity and there was no concept of decentralized identity at that time. Biometrics folks, access identity management (AIM) folks, and civil society folks with too many groups without common language.

Good 4-5 years of effort, smart people in room realized terminology was all over the place.

Now we have technology to build upon which allows for contextual centric identity to be put in play without rip and replace of old identity access management platforms.

If going to moon? There was no shared definition to explain “are we going to land on moon, orbit, sending probe or astronaut, whose moon, what is a moon?” We brought together folks who build landing gear, pressure suits, rocket motors and said build a rocket. **No clear goal or understanding.**

Everyone talked about their piece of identity. **Too many self interested folks who caused intellectual capital to leave.** Too many cooks in the kitchen as well.

Vision was there, defined aspects of what you do were not there. There was expectation for a disparate community to create that which was great aspiration but there was too much difference in goals.

There was an urgency to make the thing...focus on deadlines...but they did not take time to go over terminology and create understanding with privacy and AIM, or biometrics and IT folks. Not enough on group development and shared understanding.

A lot of time was spent on governance of the organization, which ended up being spin cycles and wasted time since there was no shared understanding. 6-12 months to form an organization and we did not know what we were talking about.

Third Speaker - Adrian - Severed on the management committee, bureaucracy dominated in all aspects, there were no skunk work teams going over small areas to be pushed, the structure of it limited creativity during the entire process. If you want desired outcome, do not introduce structure too early or at least iterate it. Do not build governance for tomorrow without doing it for today.

What was the purpose of the group or desired endstate? "Technology, policy sandwich" was a trust framework. It should have been an accountability framework.

Under What Authority Did the Government Come Up With This?

The Constitution does not grant authority for X, and if X is not explicitly outlined is reserved for States to handle.

RealID is really a trust framework. Reframing as such would be helpful.

Why attempt to tackle this again?

Ken Gantt asks four questions about public/private partnership concept similar to NSTIC,

Initial thoughts based on feedback, IIW experience, was to ensure future initiatives look closely at 1) inclusive nature 2) awareness and education aspects

Designing a 1st Year General Studies Curriculum for "Introduction to Digital Identity"

Session Convener: John Wunderlich

Notes-taker(s): John Wunderlich

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

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

Curriculum:

Course Objective: To equip students to be effective digital citizens and consumers, based on using their digital identities and act in their own best interests.

- Phil - many students will graduate into jobs and careers that involve processes and interactions that depend on digital identity
- Doc - two kinds of knowledge, tacit and explicit
 - Most people understand human interactions tacitly
 - Digital world in explicit
- This course helps students live effective digital lives.
- "Artificial proximity through digital identity"
- There is no such thing as digital intuition

> this course won't work without undergraduate contribution to the design course

Suggested Course topics

1. The nature of identity
14. Privacy, Authenticity, and Confidentiality
15. Policy
16. Regulation & Law
17. Standards

15. Secrets, Confidences, and the magic of cryptography
2. Defining digital identity
3. Problems of digital identity
4. The laws of digital identity
5. Relationships and digital identity
6. Privacy and digital identity
7. Trust and identity
8. Psychology and digital identity
 - What are the default human interactions that work in person but are bad experiences on line?
 - Forgetfulness and Forgiveness
 - Identity online is permanent and shared, not bounded
 - Retraining cultural reflexes
13. Real world impacts on you of the uses and abuses of digital identity
16. Authentication
17. Federation

Reading list

- Erickson's Identity, Youth, and Crisis
- Phil Windley Learning Digital Identity
- Sandra Petronio Boundaries of Privacy
- boyd's The secret life of networked teens

Let's Plan a Hackathon

Session Convener: Brian Richter

Notes-taker(s): Brian

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

<https://app.mural.co/t/aviarytech6399/m/aviarytech6399/1668717598676/4fdd16886d0b5fec51f6b3d2920d627e21844899?sender=u376da0e2d436cfbb30285927>

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

We made great progress trying to put an event together. Planning in the mural link above. Will continue planning offline. Let me know if you are interested in joining the planning committee!

brian@aviary.tech

DACH lunch.

Session Convener: Andre

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

Ideas for Community Building in the SSI space. / ?

Session Convener: ?

Notes-taker(s):

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

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

NO NOTES SUBMITTED

SESSION #15

Trust Over IP Interoperability Framework

Session Convener: Drummon Reid, Judith Fleenor, Allan Thomson

Notes-taker(s): Neil Thomson

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

The ToIP Tech Arch Spec can be found [here in PDF and GitHub MD](#)

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

Trust over IP's mandate includes providing interoperability certification testing as part of its mandate. The rationale is quite simply that adoption and successful deployment, and a sense of "just works" is critical to SSI and ToIP's full stack architecture acceptance by governments, corporations and users.

ToIP is following the lead of organizations like the WIFI-Alliance, which created a cross-organization certification group, organized and financed by Wireless manufacturers and supporting technologies to define full wireless stack certification across a wide variety of use cases, context and device types (access points, office building, airports and per device user access, for the entire wireless ecosystem).

This was done by defining device and software component profiles and use cases which formed the base for the interop test cases. As a result the WIFI Alliance sticker on products was assurance that "it just works" and was seen as successfully promoting early and confident adoption by the entire spectrum of customers.

Another example is the Video Cassette Recorder market (of many years ago). Sony BetaMax and the VHS consortium were the two standards. Sony only attracted a small number of vendors to support BetaMax vs the rest of the industry supporting VHS. Sony had the better product, but VHS won, due to greater adoption by VHS by both the machine suppliers and the supply of recorded material.

ToIP needs to do the same thing to know that SSI "just works". This needs the organizations developing SSI at all levels to become the support for building ToIPs interop certification group, including funding and donation of time and expertise. For supporting organizations, this ensures that they are at the forefront of driving the interop requirements and test cases.

Based on industry experience, ToIP has determined that delivery of full interoperability certification will be 18 to 24 months and needs to begin now. This will avoid the problem the Software Technology and Cyber Security (STCC) industry experienced where they did not initially commit to an interop certification approach and discovered only in early deployment to a customer using equipment from two vendors that each vendor had different interpretations in the implementation details, which was both expensive, lowered credibility and set back acceptance until an interop certification test suite was created.

Questions and Feedback

Does this mean picking winners and losers in the current implementations of, say, verifiable credentials such as anon creds?

No, this is about creating a single interpretation of the technical specifications, down to the test case level. This provides unambiguous definition for not only existing VCs, but also for all future VC development, creating a level playing field for all SSI technology development organizations.

Certification is also about the entire technology stack of which VCs are only part. The goal is overall SSI system certification, not just SSI components. Note that DIF (the Digital Identity Foundation) only wanted to specify, develop and certify components (e.g., secure store) vs. entire SSI systems.

How will interoperability cover different environments and uses of SSI?

This will be part of the work of developing the interop suite. While there will be a base set of interoperability requirements, there will also have to be specific environment, device, server, etc. certification suites, plus advanced suites for optional or advanced behavior. It will be up to the ToIP marketplace and ToIP members to define the use/test cases to be included, so participation in building ToIP interoperability certification suite is in the interest of all SSI developers.

The alternative is to let the largest vendors dominate the industry through their ability to deliver a wide range of SSI technologies such that they can provide organizations with a complete single vendor solution. This would be analogous to AT&T's dominance of telecom in the US.

Questions to the room:

1. should TOIP develop an interoperability certification framework and delivery it?

Answer: All but one person said yes.

- One dissenting opinion was: why commit now? There may be newer, better, better alternatives to the ToIP stack in the near future.
- Another pointed to ToIP certifying the existing, most popular Verifiable Credentials (e.g., Anon Creds) the way they operate today as the standards.

2. Is there some other group or existing organization where this should happen?

There were no suggested alternative organizations

Final Comment (from a participant): I have seen demos of some components and full demonstrations the SSI stack here at IIW. It is very hard to understand whether they will be interoperable, particularly in a multi-supplier application or environment (without a vendor neutral interop certification suite)?

DIDs as first-class citizens in the blockchain world. A showcase.

Session Convener: Antonio Antonino

Notes-taker(s): -

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

KILT blockchain node code: <https://github.com/KILTprotocol/kilt-node>

KILT SDK: <https://github.com/KILTprotocol/sdk-js>

KILT DID method spec: <https://github.com/KILTprotocol/spec-kilt-did>

KILT whitepaper: <https://www.kilt.io/wp-content/uploads/2020/01/KILT-White-Paper-v2020-Jan-15.pdf>

KILT docs: <https://docs.kilt.io/>

BBS+ + Predicate Proofs

Session Convener: Dan Yamamoto

Notes-taker(s):

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

- Verifiable credentials
- BBS+ signatures
- Predicate proofs
- Range proofs
- JSON-LD

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

Quick demonstration of JSON-LD BBS+ signatures with selective disclosure and predicate proofs,

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

We can generate a range proof to indicate “maximumAttendeeCapacity”: { “range”: [100, 30000] }` for example, to prove the maximum attendee capacity is in a range of 100-30000.

The key point is “termwise encoding” from JSON-LD data to a 1-dimensional array of integers (input of BBS+ core algorithms) for realizing predicate proofs with LDP-BBS .

Currently, range proofs only support a integer range proof; do not support split range proofs, decimal or float number range proofs at the moment

Related GitHub repositories are:

- [zkp-ld/zkp-ld-playground](#)
- [zkp-ld/jsonld-bbs-signatures](#)
- [zkp-ld/bbs-signatures](#)

- zkp-ld/bls12381-key-pair
- zkp-ld/bbs
- zkp-ld/bulletproofs_amcl

Three of them are forked from @mattrglobal, and two of them are forked from Hyperledger urisa.

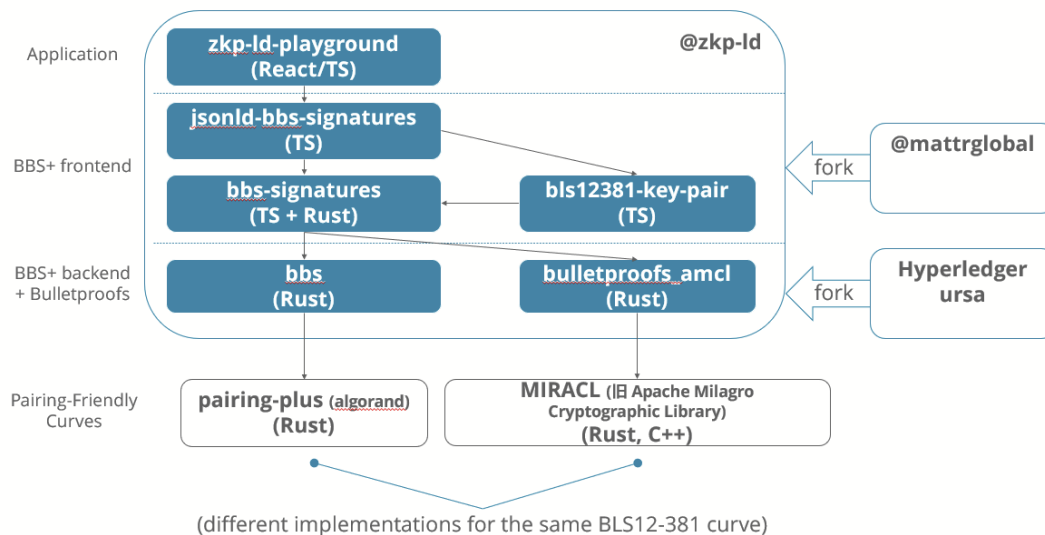
There are not sufficient documentation at the moment, but a conference paper might be useful to get the idea: https://sako-lab.jp/download.php?article=ssr2022_proceedings_dan.pdf / <https://ssr2022.com/slides/FormalisingLinkedDataBasedVerifiableCredentials.pdf>

“Holder-binding” feature has not been implemented yet.

Are there any alternatives to BBS+?

-> possibly includes Pointcheval-Sanders signatures and Sanders redactable signatures. Sanders also published Lattice-based signatures with ZKP that might be used to implement post-quantum VCs in the future.

Implementation Details



Verifiable Credential Rendering (Hints)

Session Convener: Dmitri Zagidulin, Charles Lehner, Ben Goering

Notes-taker(s): Charles Lehner

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

Verifiable Credentials, Rendering, Templates, Cascading Stylesheets, User-agent, issuer, overriding, consistency

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

<https://lehnerstudios.com/2022/11/17/iw35session15b-vc-rendering-notes.txt>

End Surveillance Capitalism

Session Convener: Chris Heuer

Notes-taker(s): Chris Heuer

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

#endsurveillancecapitalism

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

Session Audio/Transcript: <https://otter.ai/u/2fBzzFluVETAhLqhcgeMNB8egGs>

Submit a Change.org Draft Petition for Consideration below or if you'd prefer, using this simple form <https://forms.gle/K677XNPhvsVoxga18>

Conversation with Clive Smith on Movements and his experience/thoughts on how to move them... <https://otter.ai/u/x13XEmqSJFgLvhSPvpGeTm8Bp0>

ESC - End Surveillance Capitalism

CHANGE.ORG

- **Submission 1:** End Surveillance Capitalism: People aren't just being exploited for exploitative corporate profits, they, and our whole society are being harmed. It's time to end the efforts to make trillions of dollars of profit off of our data, our rights, and our very lives.

An initiative of the Customer Commons and the Internet Identity Workshop.

Trust Alliance New Zealand

Session Convener: Trust Alliance New Zealand

Notes-taker(s): Elina Cadouri

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

<https://internetcomputer.org>

Intros

Kyle Peacock from Dfinity

Elina Cadouri from Dock - Tooling and infrastructure for SSI/DIDs/VCs

Reuben, Benri - Enterprise Solutions for travel industry

Sam Curan, Indicio

John, JLinx Labs - protocols and products for decentralized data exchange

Paul D, GS1 US - supply chain

Kevin Corter, Toby data - data aggregation

Jonny Striber, lawyer interested in DAOs, conflict resolution

Chris Claridge & Klaeri Schelhowe, Trust Alliance New Zealand

Agenda

1. Introduction of Trust Alliance NZ
2. Overview of the Problem Statement
3. Proposal "Federated Farmers Wallet"
4. Discussion
5. Next Steps

Farm Data Sovereignty Organization

- Farmers should be able to capture and share data
 - Farm enterprises/organizations (not farmers) identity
- Non-profit industry consortium
- Building out NZ's digital infrastructure (not a platform)
- Enable data capture, protection, sharing

TANZ is an enabler for NZ's food and fiber industry to change from selling based on brand promise to brand proof

- Provide digital proof both domestically and internationally
- Not trust marking themselves, want to enable the tools
- Looking to be in the background to enable the protocols

Shared the current alliance

- Federated Farmers, government agencies, universities, GS1 NZ, tractor supplier, Technology companies, DATACOM, supermarkets, fertilizer companies, regional councils, food auditor, banks/lenders, health and safety providers
- These brands will connect these protocols for the tools
- How is it funded? Membership fee, non-profit organization is able to apply for government funding

- Running for about 3 years, part of the time was undercover and then learning from the members via discovery workshops
 - Initially felt like the industry wasn't ready, so they worked on use cases, definitions, protocols, etc.
 - Felt like identity was the starting point and looked into decentralized identity

Use Cases:

1. Identity
2. Location (who is the farm, where are they)
3. Critical control, transactions, events

New Zealand doesn't have a farm database, ID system, etc., instead they have regional councils who operate their own systems

Farm is the source of truth that is used across the value chain because they have all of the data about the farms

- E.g. the farm may need to share compliance, if it is in a VC format then it is easier to share
- The bank can prove that the customer is a good customer
- Market access - as non-Americans, non-US, non-Chinese it makes it difficult to sell to these markets
- They're the 9th largest producer of french fries and need to export to different systems

Wallet - how it will work

Data input > farmer's device > data output

Need support from the farming lobbying association

They're looking for 3 or 4 solutions, they need to represent several options to the government

Start VCs

1. Membership of federated farmers (union, represents 90% of the farm economic output)
2. Authentication for polling/voting (non anonymous) by the farm enterprise
 1. Current voting is paper based
 2. Happens frequently
 3. They're looking to provide the VCs for voting, but not to facilitate the voting
3. Holding credentials on farm like paddock boundaries
 1. No framework for farm data, don't know where the farm is
 2. Definitions of a farm change based on region
 3. Farms can be self-issued

July 6th is the farm summit

- They have a mandate to do this from the farm community

Voting is the initial use case for the application

Wallet

- Mobile app or browser extension to access the cryptographic identity
- Verb needed: voting, tracking for the supply chain process
- Farmers don't like computers, prefer mobile
- Might need to have both a phone and web experience

Dfinity - decentralized platform, can be stored

LEI - legally global identifier

Farmers have GLN numbers for the business - GS1 is building descriptions for farms

Operates like a DAO

There are existing apps, but federated farmers doesn't have an app

Does it make sense to store valuable data on the farmer's phones?

Make sure it works offline

Network is already formed with incentives to participate

Rollout

- Starting internally with the farmers union, then a smaller group, then all of the farmers over 2 years

Anoncreds 2.0

Session Convener: Ankur Banerjee

Notes-taker(s):

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

<https://wallet.cheqd.io>

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

- Authentication mechanism is Kepler wallet

DID : Keri A DID method resolver reference implementation that probably sucks.

Session Convener: Phil Fearheller

Notes-taker(s): Kevin Griffin

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

Slides:

https://docs.google.com/presentation/d/1sA1YydkSjlUs0I_j2_cG8QqNrO0Mf0oIHlGFwPTfUA/edit?usp=sharing

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

Running commentary:

Attempt to allow DIDs and KERI to communicate

URL should be encoded.

OOBI should not be part of the did as the witness AID can change

did:keri:AID?oobi=URLESCAPED

Could use a DHT for initial discovery, all the information you need to verify the source is from the requester.

You just need to know how to introduce each other.

Eventually the concept of a super watcher, every AID they have seen they could know about and you could attempt to find an OOBI in the did:keri there.

did:keri is a type of did:url as it contains a path.

`kli did generate --name cha1 --alias cha1`

generates a did:keri

rename to did:url

`kli did`

Why are you doing this.

Because we can embed an ACDC in a didcomm message, and we'd hand it off to Aries Handler

In did resolution you can add an option to the 'resolution options' like a HTTP Header, those options would be included

in the didcomm message.

have both did generate command and
did generate url command

suggest make url option as --url

```
`kli did generate`  
`kli did generate --url`
```

more commands...

```
`dkr resolve --name cha1 --alias cha1 --did <did:keri>`  
to generate diddoc
```

after resolution you can use diddoc metadata (if you don't trust your resolver) to fetch the key state for yourself to compare to what you have and what was sent to you.

For KERI multisig you need an array for publicKeyMultibase public keys.

someone in CCG working on similar multisig
or introduce new CESRVerificationKey2022
or introduce new KERIMultisigVerification2022

If single sig use use original publicKeyMultibase as it is familiar.

Service types, Phil just made them up.

KERI doesn't store service endpoints in the KEL, uses BADA RUN,
they're stored in KERI's local datastore, signed at rest.

Problems to solve:

- 1: make did:keri a did:url, parameterize the oobi and url encode it
- 2: yes we can define new service end points
- 3: define other key types, yes
- 4: Aries plugin would be nice
- 5: everyone stayed quiet, weak sauce
- 6: Markus would prefer a docker container of the did:keri resolver

The State of Hyperledger Aries and how to make a wallet in 4 hours

Session Convener: Stephen Curran, Kyle Robinson, Government of British Columbia
Notes-taker(s):

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

- Presentation [Slides](#)
- Hyperledger Aries [Project](#) / [Wiki](#)
- [Hyperledger Aries](#) Repositories
- [Aries Bifold](#) Open Source React Native Wallet
- [BC Gov Wallet](#) Repostory and [information page](#)
- [AnonCreds Specification](#)
- The BC Gov open source [Traction](#) Issuer/Verifier Enterprise Agency

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

What is Hyperledger Aries?

- Protocols
- Open Source Framework Implementations
- Applications
- Interoperability Profiles
- Test Suite
- A Wallet

Demo presented of the BC Gov Wallet, a deployment of the Aries Bifold wallet, a 100% open source wallet with a powerful build pipeline that allows us to publish a completely customized wallet for the BC Government that is 90% Aries Bifold. When the BC Gov Wallet team (and others developing Bifold-based wallets) adds capabilities to the wallet, 90% of the work is done in the shared Aries Bifold repository, benefiting everyone. The demo included a presentation of the Traction Enterprise Issuer/Verifier agency.

Does Web5/SSI have an adoption problem?

Session Convener: Timothy Ruff
Notes-taker(s):

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

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

NO NOTES SUBMITTED

Notes in this book can also be found online at
https://iiw.idcommons.net/IIW_35_Session_Notes



Jessica Tacka she/her/Mx. @JessicaTacka · Nov 18

What an experience at #IIW. I have to finish processing and decompress before I review the notes to narrow down my key takeaways. Thank you @idworkshop organizers and attendees for a wild ride!



Speed Demo Hour / Wednesday Nov 15 / Danube TECH



SPEED DEMO HOUR
SPONSORED BY

DANUBE
TECH GMBH 

| TABLE | Demo Description |
|-------|---|
| #1 | 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. |
| #2 | RootsId: The RootsId team (Rodolfo Miranda, Lance Wallace, Esteban Garcia and Alex Andrei) URL: https://rootsid.com/ & https://github.com/roots-id/rootswallet We will show the 2 Roots ID wallets that communicates with a mediator using DIDCOMM v2 protocols to send messages, issue and validate credentials. Looking forward to meeting everyone! |
| #3 | Gluu: Agama Developer Studio: Michael Schwartz URL: https://docs.jans.io/head/admin/developer/agama/ Agama is a programming language for web flows. With the Jans Auth Server, you can use Agama to define all sorts of interesting flows, e.g. registration, adaptive authentication, identity proofing. Available for free at the Linux Foundation Janssen Project: https://jans.io |
| #4 | Mee Agent: Paul Trevithick URL: https://meeproject.org Mee is a nonprofit, open-source project developing a free, personal software agent that represents you and your interests online. When it shares your data with service provider's apps and sites, it does so under the terms of a privacy-enhancing Human Information License. We'll demo a prototype of this agent running on iOS. We'll show how it can create a digital connection (beyond mere signin/signup) with a Mee-compatible website from a cold start (i.e. when the user has no agent installed). |

| | |
|------------|---|
| #5 | adnovum.com Aries 2.0 Android Wallet Prototype: Michel Sahli URL: https://www.adnovum.com/blog/this-is-my-gr-code-how-ssi-could-revolutionize-real-world-identification Presentation of an Aries 2.0 Android wallet prototype, which was developed during my master thesis to analyze the current issues with the verification of digital identities in the physical world and how we could enhance it using Aries 2.0. adnovum.com |
| #6 | Sphery - CARO B2B Platform: Lauritz Leifermann, Dennis von der Bey, Philipp Bolte URL: https://www.carovc CARO is a B2B platform for the US pharma market to get DSCSA-compliant by connecting SSI-technologies with already established systems. We will be presenting an actual real-world SSI product, our learnings, open-source contributions, and the technologies we had to invent on the road to production. This includes a novel revocation method and an industry-backed trusted issuer list. |
| #7 | Dazzle / Dazzle Labs and Dazzle DAO: Johannes Ernst, Indie Computing Corp URL: https://dazzle.town/ What if you had all your personal data in a single place that you control? All your posts from Facebook, your orders from Amazon, maybe even your Tweets! And that no unaccountable vendor has ultimate control over? |
| #8 | Update on Blinky Project (Explorations with I.o.T): Brent Shambaugh URL: https://github.com/bshambaugh/BlinkyProject/ Description: Explorations with an ESP32 with a Cryptographic Co-Processor for Providing a Signer for the Ceramic Network and Possible Future Directions |
| #9 | TAG LLC presenting Digital System Design (Dry Systems) & Naturally forming Systems (Wet Systems), an exercise in evaluating differences between human realms of presence in both environments: Jeff Orgel NO URL: The materials will be displayed at the table. The human animal is built to exist in a set of limited environments which are naturally formed. The Digital Realm is completely structured/unnatural in every respect. |
| #10 | Digital Identity (ADI) Association - Commercial implementation of spec DTX® Identity Cloud: Jason Burnett - Digital Trust Networks URL: https://adiassociation.org/technology/ The DTX® Identity Cloud demo will show managing employees of an external workforce, using the ADI Association's ADIA identity specification. DTX® is the first implementation of the open specification developed by the ADI Association. |
| #11 | esatus AG & Lindner Group: Sebastian Weidenbach, Franziska Meilhammer, Andre Kudra URL: https://ingo-id.com/ https://esatus.com/index.html%3Fp=8009&lang=en.html We demonstrate Lindner's "inGo" with which verifiable credentials are used in production for compliant physical access to construction sites. Credentials remove paperwork from this harsh environment and ensure only eligible persons are on-site. inGo is enabled by esatus' SOWL. |
| #12 | GLEIF (gleif.org): Phil Fearheller and Kevin Griffin URL: https://www.gleif.org/en/about/governance/annual-report With 2021 inline XBRL publication of it's annual report, GLEIF demonstrates the first use of a verifiable Legal Entity Identifier (vLEI) to sign an annual report. |
| #13 | Center Identity /Location-based key recovery: Matthew Vogel URL: https://centeridentity.com Current methods for key recovery are difficult, but we will demonstrate how easily a private key can be recovered with the visual memory of an end user. This makes user-centric identity feasible as passwords become obsolete in light of our new approach to securing digital assets! |
| #14 | Microsoft, Ping Identity, Workday, IBM, Avast, SpruceID: Kristina Yasuda, Jennifer Schreiber, Andrew Hughes, Oliver Terbu URL: https://identity.foundation/jwt-vc-presentation-profile/ Interoperable presentation of Verifiable Credentials between Wallets and Verifier built by different providers |
| #15 | Identity.com: Martin Riedel, Andrew Bertin URL: https://www.identity.com/ We demonstrate one of our SSI technology stacks on the Solana Blockchain, consisting of did:sol as a DID method, Cryptid as a on-chain wallet abstraction using did:sol, and the Gateway Protocol that defines a governance framework around issuing pseudonymous tokens associated with a previous (off-chain) verification |
| #16 | Open Source Governance Editor: Mike Ebert URL: https://indicio.tech/governance-editor (in case you follow this and find it broken, this is a placeholder and we will have a page up shortly) Indicio has been working with the DIF to create a specification for trust lists and machine readable, decentralized ecosystem governance. We've created a governance file editor and governance interpreting code to show |

| | |
|------------|---|
| | a sample implementation of the spec. |
| #17 | The Abacus Authorization Engine: Jacob Seibach URL: To learn more about The Abacus, please read the Master's Thesis on the subject: https://scholarsarchive.byu.edu/etd/9221/ The Abacus Authorization Engine will be demonstrated to show various policies, the simplicity of invoking the engine, and the efficiency of the system. It will also show the simplicity of allowing the business owners to set policies for their domains. |
| #18 | Veramo - an open-source framework for Decentralized Identities & Verifiable credentials: Consensus Mesh Identity Team (R&D Unit) Simonas Karužas, Nick Reynolds Italo Borssatto URL: https://veramo.io/ In decentralized identity solutions, we need to prioritize interoperability and cross-platform support in order to serve the widest possible audience. Meeting these requirements can be costly. Veramo is an agnostic, modular solution that will surely save your team a lot of time. |
| #19 | Bundesdruckerei GmbH , Remote Wallet Attestation for mobile SSI Wallet Security: Paul Bastian URL: https://nextcloud.idunion.org/s/3zaz93rf3qtqJK3 The Demo shows an early version of a remote wallet attestation service that offers an issuer validated information about the wallet authenticity and hardware-backed keys. In the demo we show the Lissi Wallet contacting the Bundesdruckerei Attestation Service, which issues the wallet attestation as a VC. |
| #20 | Trinsic /OkeyDoke.io -Issuing, viewing and verifying a credential in a familiar e-commerce interface: Tomislav Markovski, Hersh Patel, JP George URL: https://dashboard.trinsic.id/ OkeyDoke.io is an ecommerce store that wants to offer discounts to artichoke farmers who have been certified by a trusted licensing entity. Come and see how the farmer interacts with a chat bot to apply for a licensing credential which is then issued to a cloud wallet tied to their email to show a discount on the artichoke seeds to the farmer |





👤 @danielabarbosa · Nov 15

...

Opening circle 35th [#IIW](#) @idworkshop - full house - lot's of new faces, old friends & even an airline pilot ✈️ and opera singer 🎵 @Hyperledger & @linuxfoundation is a proud supporter of this global identity community. Thank you all for showing up and moving this work forward.



↻ 3

❤️ 12



Chris Streeks @cStreeks · Nov 17

...

Had an absolute blast at [#IIW](#) this week! Great seeing familiar faces! Thank you @nobantu for the invite! 🙏



💬 1



❤️ 1



[Show this thread](#)

Diversity and Inclusion Scholarships / SpruceID



Thank You to Our Diversity & Inclusion Scholarship Sponsor [SpruceID](#)

Through this sponsorship we offered both complimentary tickets and travel reimbursement to 4 new attendees to IIW.

From our sponsor:

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.

We would also like to thank [Women in Identity](#) @WomeninID who helped get the word out and increased our reach in terms of possible recipients.



Women's Breakfast / Thank You to Sponsors Randa & JFF



Jessica Tacka she/her/Mx. @JessicaTacka · Nov 16

Radical Women's breakfast at [#IIW](#) 🙌🙌🙌 @idworkshop
[@TransmuteNews](#)



IIWXXXV #35 Photo Albums by Doc Searls

Check out Doc's FABULOUS candid photos of IIWXXXV @dsearls

Day One:

<https://www.flickr.com/photos/docsearls/albums/72177720304426235>

Day Two:

<https://www.flickr.com/photos/docsearls/albums/72177720304429940>

Day Three:

<https://www.flickr.com/photos/docsearls/albums/72177720304431417>

Stay Connected with the Community Over Time - Blog Posts from Community Members

A Community Resource

Each week Kaliya, Identity Woman and Informiner publish a round of the week's news from the industry. It is called **Identosphere - Sovereign Identity Updates (weekly newsletter)**

You can find it here: <https://newsletter.identosphere.net/>

As a follow up to the session 'Let's Bring Blogging Back' an IIW Blog aggregator has been created here: <https://identosphere.net>

If you want your blog to be included please email Kaliya: kaliya@identitywoman.net

A BlogPod was created at IIW - Link to IIW Slack -

<https://iiw.slack.com/archives/C013KKU7ZA4>

If you have trouble getting in, email Kaliya@identitywoman.net with BlogPod in the Subject.

Planet Identity Revived ~ @identitywoman & @InfoMiner cleared out & updated Planet Identity (see links below) you can support the work here:

<https://www.patreon.com/user?u=35769676>

IIW Community Personal Blog's shared via: <https://identosphere.net/blogcatcher/>

IIW Community dot.org's in the IIW Space: <https://identosphere.net/blogcatcher/orgsfeed/>

Hope to See you April 18, 19, 10, 2023

IIWXXXVI / The 36th Internet Identity Workshop

REGISTRATION OPEN IN JANUARY 2023



Heidi Nobantu Saul 🐝🦋 @nobantu · Nov 17

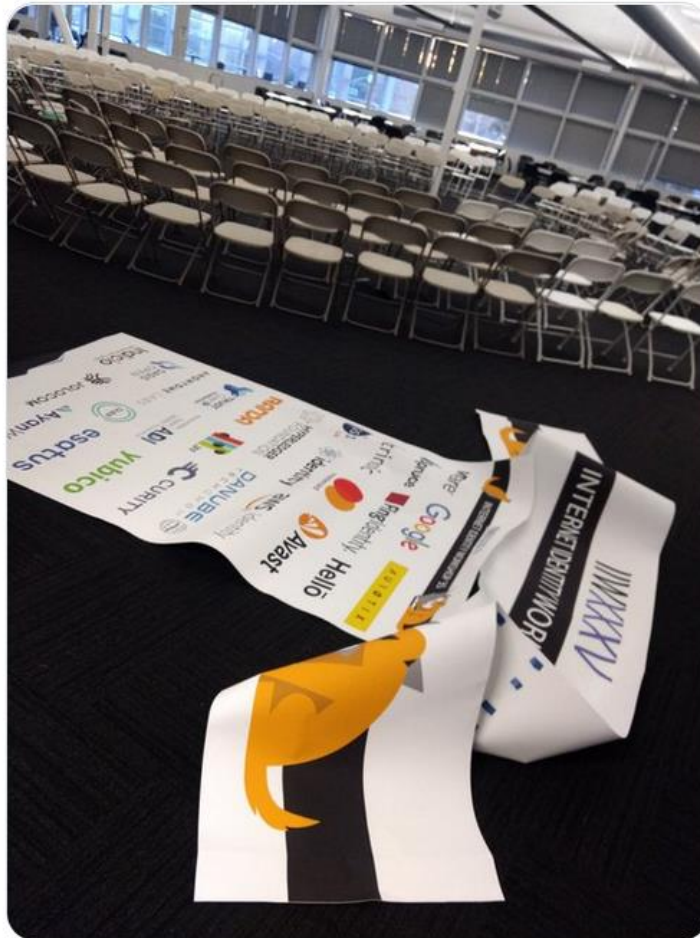
IIWXXXV is a wrap!

The largest @idworkshop to date ~

160 Sessions called and Convened

See you in April 2023

#iiw #openspacetecology



3

13



www.InternetIdentityWorkshop.com