

IIWXXXVI



INTERNET IDENTITY WORKSHOP 36



April 18-20, 2023

Book of Proceedings

www.internetidentityworkshop.com

April 18 - 20, 2023

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

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

Collected & Compiled by HEIDI N. SAUL

Thank You! Documentation Center & Book of Proceedings

Sponsors: AyanWorks & an Anonymous Sponsor



Contents

Thank You! Documentation Center & Book of Proceedings Sponsors: AyanWorks & an Anonymous Sponsor	1
About IIW	6
Graphic Recording of Day 1 - By a First Time Attendee	7
Thank You to our Sponsors!	8
IIWXXXVI Daily Schedule.....	9
IIW36 Agenda Creation = Schedule of Workshop Sessions	11
Tuesday April 18, 2023 ~ Day 1.....	11
Wednesday April 19, 2023 ~ Day 2	13
Thursday April 20, 2023 - Day 3	15
Notes Day 1 / Tuesday April 18 / Sessions 1 - 5	18
SESSION #1	18
eIDAS 201- Revision of the upcoming European Identity and Trust Framework	18
OAuth 101- IIW 101 Introduction Session	18
Web 7.0 vs. Web 5	20
Your CORE Identity: YOU are a Child of God	20
Forking VCs depending on Subject Identifier into Biometric or DID	21
Apple's Platform SSO: Leading the Way to Zero Trust on macOS.....	22
Mistakes were made...Product Manager confessions.....	24
Identity Ecosystem Picking Up Where NSTIC Left Off... Who, What, How, Why it's All Here Ready to Re- Establish! / ID Guy	27
Polyversal Coordination Stack for PLANETARY Self-Governance	27
vLEI Update	30
Large Language Models (LLMs) for Human Flourishing and Human Accountability	31
Government-Issued Digital Credentials White Paper	33
Assurance Levels or Assurance Details?	36
SESSION #2	37
OpenID 4 Verifiable Credentials OID4VC	37
Introduction to OpenID Connect	37
What is Web 7.0?	37
Trust Registries	38
Biometrics and Blockchain Signatures: Identifying pitfalls.....	40
Regi-TRUST: A Network of Network Model for Discovering and Validating Trusted Ecosystems	40

Federated Auth Network	41
Intro to KERI.....	41
KERI + ACDC 201 Accelerated Developer Introduction	42
Credential Migration + A Universal Credential Migration Format.....	42
Identity Multiplexing for Everyone.....	45
Solving Setup for - Federation, Provisioning, Session Security, Account Security	45
SESSION #3	46
Organizational Identity & Credentials.....	46
UMA 101 - Introduction to User Managed Access	50
ABC's of Writing DIDs with Universal Registrar (and how it's different from Universal Resolver).....	50
Let's Create a Decentralized Community Partner Language.....	51
Is Presentation Exchange the right query language for identity credentials?	52
Identity in the Fediverse	78
Expanding Language - Humans Think - Chatbots Process - How does that augment or disrupt communication intentions	79
Interoperable Trust Registries with DID-Linked Resources	83
Protecting Identity With WebAuthn	84
Introduction (and roasting) to the DCDR Framework (Data-Centric Digital Rights).....	85
McNamee Inspired Method to Crowd Source Congressional Policy and for Managing Politicians?	85
SESSION #4	87
NIST SP 800-63.4 Digital Identity Guidelines	87
FIDO Basics	89
Selective Disclosure with SD-JWTs 101.....	92
Decentralized Identity Foundation (DIF) Update	93
Energy + Mines Digital Trust B2B/G2B From Pilot to Production / Kyle Robinson (Bc Gov)..	99
DWeb Camp	99
Anonymous Reputation - What's the State of the Art?.....	110
Enhancing Your Participation in Tech-Related Public Consultations & UN Digital Compact seeking Feedback Session	113
“Good ID...” Is it time for a new framework?.....	114
Next Version of Sovereign Identity: Sovereign Individual System	114
Introducing Wikido, A Massively Multiplayer Joint Venture	114
SESSION #5	115
SPAC = Secure Privacy Authenticity Confidentiality - Tradespace Strongest A+C+P.....	115
Modified ESSR	116
SSI 101	144
Privacy as Alignment of Expectations	144
How can DNS help enable Digital Trust!	145
Where are my product peeps in the house?	147
30 days from Web5: A preview of the stack and Developer Preview release next month ..	148
IDtech & Why it's the key to SSI adoption / Riley Hughes.....	150
Credential Format Comparison	150
Identity & Internet the 17th Critical Infrastructure	153
Visuals of SSI	155
UX of Diia (a Ukrainian Government App)	156
Inter-Trust Domain Protocol - Can DIDs, AID, and OpenID Talk to Each Other?	156
When Browsers, Wallets, & Federation Overlap	158
Notes Day 2 / Wednesday April 19 / Sessions 6 - 10	162

SESSION #6	162
KERI for DUMMIES & Non Technical People	162
Open wallet Foundation “101”	162
Good Biometrics vs. Chain of Custody in the VC Context	185
Detachable Federation Authorities	185
Access Control Use Cases.....	187
Jurisdiction: The Missing Layer in the Identity Stack	190
What’s New with Hyperledger Indy.....	191
KERI and ACDC 201 - Developer Introduction	193
SESSION #7	194
So you want to be a QVI . . . (Qualified vLEI Issuer)	194
Wallet Attestation - Device Binding, Holder Binding, Attested Issuance, Demo E2E w/OpenID, Regulations	194
Digital Trust in the Age of ChatGPT	195
Advanced Topics in DID Resolution	214
A Digital Wallet Market Study	215
The Current State of WEBAUTHN	215
PICOS, Lora WAN, & theSSIOT	217
Use Cases and Storytelling	217
SSA.....	218
KERI 301 KELs, TELs, & ACDCs outside of KERIpy	220
SESSION #8	221
Why Can’t I Trust Who’s Calling or Texting Me? AND what KERI, ACDC, and vLEIs Can Do About That	221
We’re SABOTAGING SSI’s Chances of Success	221
Key & Trust Management revisited	223
Indemnification: Identity Risk Management as a Service.....	224
State Government Use Cases... and if there is time, The secret to state procurement	225
Meta Trust Registry - Interoperability of Trusted Ecosystems / Lucy & Savita.....	225
Using Humor and Visual Communication to gain Trust.....	226
Red Teaming Digital Identities... And Why You Need It!	227
ACRs : Authentication Context Class Reference	228
Talk Session Identity in Ethereum / Jane	231
Singpass: sign up with 1000 RPs	231
SESSION #9	232
Query Language for VCs (Presentation Exchange?) Part 2.....	232
Verifiable Credential Revocation in 2023, and What Might Be Next	232
Linux Foundation - Digital Trust Initiatives: DIF, Hyperledger, Open Wallet, TOIP +++	233
YOUR DID Method Sucks - Change My View	233
Privacy Enhancing Mobile Credentials (PEMC).....	234
Why Open Linked Trust.....	236
Joys & Miseries of Structured Data - Analyzing the Life Cycle of Authentic Data /	237
AuthZ and SSI: Architecture for using an external authorization engine in an SSI ecosystem	238
Security Encryption Authorization GUNdb peer2peer graph - access control for distributed storage and compute	239
Want to make revenue with Identity? Quit talking about Identity	240
Public Private Partnerships - What’s needed for success? Identity Ecosystem or Archipelago	246
SESSION #10	248

OpenID 4 Verifiable Credential Issuance (was DID4VC 101)	248
SPAC #2 = Secure Privacy Authenticity Confidentiality - Tradespace Strongest A+C+P	248
AI Why We Need DID's NOW	248
Identity Collaboration *SDG* Untangling Chains of Society (SDG) Supply Chain, Portability, Interoperability, Value Chain, Trust Chain / Lubna D	249
Internet Data Usage Control System - JLINK / John Wunderlich	249
Human Rights Affirming Government Identity AND FSLTT @IIWXXXVI Fed, State, Local, Tribe, Ter - We are here from Gov, we should talk	249
Expanding The Language = Techorata Informed and reflected on by the = Desiderata - Joyful, Contemplative & Serious	253
OAuth 1st Party Native App Authentication / George Fletcher	257
VC's in the Supply Chain: GS1 Verifiable Credentials	257
½ AI breaks ID things/cyber security and ½ How VCs/DIDs trust Registries Fixes things AI Breaks	261
Notes Day 3 / Thursday April 20 / Sessions 11 - 15	264
SESSION #11	264
INTEROP Profile with SD-JWT + OpenID4VC	264
Using What We've Got - Pure Identity plays probably aren't the answer	290
KERI + ACDC 201 Part II	295
Web 7.0 Trust Registry FrameWork - TrustReg Documents (DID Documents)	295
Aries Bifold - What is new?	295
The Rubric Podcast	298
What the heck is a hash	298
AnonCreds AMA	300
Rubber, Meet Road - The Common Actor Model (CAM)	302
SSI Deployment Challenges / Phil Fearheller w/GLEIF	302
Government-issued Digital Credentials and the Privacy Landscape (is there anything else you want to tell me?) - repeat of session on Day 1	302
SESSION #12	304
Making Credentials Beautiful with OCA (Overlays Capture Architecture)	304
AI (ML, etc) and SSI: Post-Scarcity Utopia vs Hellscape?	305
Credential Trust Establishment	308
Interoperability: What does it look like to a user? What baby steps can we take to get there? & Interoperability - What's Hot? What's Not?	309
Blockchain and Biometric Signatures	311
Dazzle Office Hours/Intro Get Your Personal Data Back!	311
Creating A Decision Matrix Around Credential Exchange Protocols	312
Deep-dive on creds.xyz (a decentralized social reputation system for Web 3 Communities & DAOs)	313
Dynamic Pitch Modulation and Satiric Prose	314
KERI IPR??? If it doesn't get cleaned up it's going to hurt	314
Fun with DIDComm (sub) Protocols	317
SESSION #13	320
WebAPI/Quylanguage to VC's (again)	320
Your Identity is NOT Self-Sovereign	320
Binding Identity to Publicly-Visible Content	324
AUTOREP - an autonomous decentralised reputation scheme	324
JSON Web Proofs - Status and Progress	324
Delegatable Verifiable Credentials	325
What did I DO? I pointed an NFT to a Verifiable Credential!!!	342

Exploring how to engage more w/ Washington DC - What are hurdles to adoption?	343
Session #14	347
The Great Migration: DiDs and VCs are perfected! The face a world full of Active Directory.	
How Do We Make it Easy to Switch?	347
Verifiable Credential rendering method or VC ‘render Method’ vc rendering a display	348
Where will the Generative AI/ML in my Wallet Come From?	349
OWF Project Ideas.....	350
Web 15.2: Shiny Toy or Pit of Despair.....	368
Yo-ID A reusable IDV network, as simple as possible.....	369
Principled Peacemakers ~ A Real Identity Demo	370
PERCEPTIONS - Let’s talk about those related to identity...But more importantly, what is the Gov’t doing with my biometric data? (Inquiring minds want to know)	370
Did:eth + did:ens Update and Call To Action.....	370
SESSION #15	371
SPAC #3 = Secure Privacy Authenticity Confidentiality - Tradespace Strongest A+C+P	371
What AI will never do or be.....	371
Bridging Protocols	372
Browser APIs and Intent Handlers (for wallets)	375
Digital ID/SSI Researchers/Scholars masters/PHD Student Network? What do we do to start/support this? How do we create annotated Bibliography?.....	376
Calling All EDs - What Can We Do Together? / Jean Q and John	377
Hyperledger Identity SIG Launch.....	377
GLOBAL Assured Identity Network (GAIN) Update - VCs interop profile - Interoperability /Network or Network	378
Speed Demo Hour / Wednesday April 19.....	392
Diversity and Inclusion Scholarships - Spruce ID & tbd	395
Some IIW Experience Tweets	396
Blog Posts About IIWXXXVI	399
Stay Connected with the Community Over Time - Blog Posts from Community Members	400
Doc Searls - Candid Photo Galley from IIWXXXVI	401
Hope to See you October 10, 11 and 12, 2023	402
Inspired by IIW™ Regionally Focused Open Space unConference’s.....	403

About IIW

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

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

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

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

The event is now in its 19th year and is Co-produced by Phil Windley, Heidi Nobantu Saul and Kaliya Young. IIWXXXVII (#37) will be **October 10, 11 and 12, 2023**

.



Phil Windley @windley · Apr 24

...

Last week's #IIW was great with many high intensity discussions of identity by people from across the globe.

technometria.com/p/internet-ide...



2

6

22

1,177



Graphic Recording of Day 1 - By a First Time Attendee



Illustration by Chance McGee - Although not officially a technologist Chance is an expert animator and the work he does can amplify and bring SSI to more people. [Studies](#) have shown that live drawings during presentations have the ability to dramatically increase engagement and retention in audience members. He's interested in and excited about SSI and Decentralized ID and could do great things to help the community. [Connect with Chance on LinkedIn:](#)

From Chance: This is more of an impromptu graphic recording based on my limited knowledge. In the future, if I were to sit down with you or your team, we could come up with a series of info graphics and/or animations that could help communicate various complex topics.

Thank You to our Sponsors!



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

Upcoming IIW Events

IIWXXXVII #37

October 10, 11, & 12, 2023

In Person Mountainview, CA

<https://internetidentityworkshop.com/>

IIWXXXVI Daily Schedule

IIWXXXVI 36 Day Schedule

TUESDAY, April 18 / Doors Open at 8:00			
Doors Open at 8:00 AM for Registration Barista! - Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme Donuts - Fruit - String Cheese etc.			
Barista! And Continental Breakfast	8:00 - 9:00	Lunch	1:00 - 2:00
Welcome Introduction	9:00 -10:00	Session 3	2:00 - 3:00
Opening Circle / Agenda Creation	10:00 - 11:00	Session 4	3:00 - 4:00
Session 1	11:00 - 12:00	Session 5	4:00 - 5:00
Session 2	12:00 - 1:00	Closing Circle	5:00 - 5:45
Welcome Reception & Dinner 6:00			
<u>Off the Rails Brewery</u> 111 S Murphy Avenue Sunnyvale, CA 94086 (408) 773-9500			

WEDNESDAY, April 19 / Doors Open at 8:00			
Barista! - Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme Donuts - Fruit - String Cheese etc.			
IIW Women's Breakfast Roundtable's	7:45 - 9:00	Lunch	12:30 - 1:30
Opening Circle / Agenda Creation (SHARP)	8:45 - 9:30	Speed Demo Hour	1:30 - 2:30
Session 1	9:30 - 10:30	Session 4	2:30 - 3:30
Session 2	10:30 - 11:30	Session 5	3:30 - 4:30
Session 3	11:30 - 12:30	Closing Circle	4:30 - 5:30
Conference Reception & Dinner			
Back A Yard Caribbean BBQ (w/v&v options) - Here at CHM!			

THURSDAY, April 20 / Doors Open at 8:00

Barista! - Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme Donuts - Fruit - String Cheese etc.

Opening Circle / Agenda Creation (SHARP)	8:45 - 9:30	Session 4/Working Lunch	12:30 - 2:00
Session 1	9:30 -10:30	Session 5	2:00 - 3:00
Session 2	10:30 - 11:30	Closing Circle	3:00 - 4:00
Session 3	11:30 - 12:30	IIWXXXVII Oct 10, 11 and 12, 2023	

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

<https://dasbierhauz.com/>



Drummond Reed @drummondreed · Apr 18

...

Replies to [@idworkshop](#)

Amazing that we are now at [#IIW](#) 36. That's 18 years of solving Internet Identity. Strangely enough, I think we're getting close. [#DigitalWallets](#) and credentials are arriving fast. Watch this space...



2

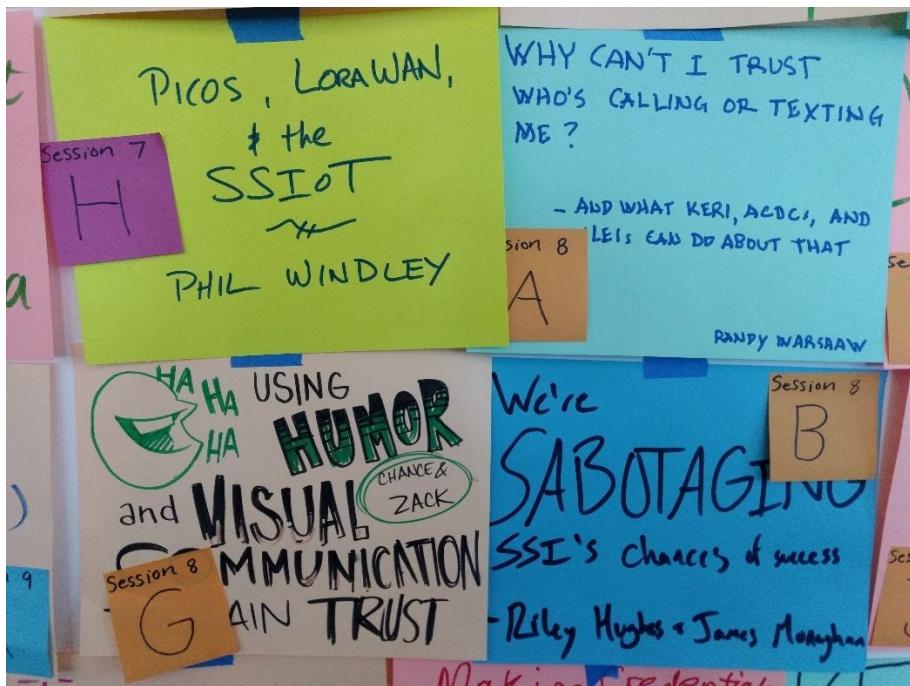
11

8

144

↑

IIW36 Agenda Creation = Schedule of Workshop Sessions



159 distinct Sessions were called and held over 3 Days

We received notes, slide decks, links to presentations and photos of whiteboard work for 122 of these sessions.

Tuesday April 18, 2023 ~ Day 1

Session 1

- 1A/ eIDAS 2.0- Revision of the upcoming European Identity and Trust Framework / Paul Bastian
- 1B/ OAuth 101: Introduction Session / Vittorio Bertocci
- 1C/ Web 7.0 vs. Web 5 / Michael Herman
- 1D/ Your CORE Identity: You are a Child of God / Jacob S
- 1E/ NO SESSION
- 1F/ Forking VC's Depending on Subject Identifiers into Biometrics or DIDs / Adrian Gropper
- 1G/ Apple's Platform SSO: Leading the Way to Zero Trust on Macos / Dipti Shiralkar
- 1H/ Mistakes were made... Product Manager Confessional / James Monaghan
- 1I/ Identity Ecosystem Picking Up Where NSTIC Left Off... Who, What, How, Why it's All Here Ready to Re-Establish! / ID Guy (Kenneth Gantt)
- 1J/ Polyversal Coordination Stack for PLANETARY Self-Governance / Day W
- 1K/ vLEI Update - GLEIF / Karla McKenna
- 1L/ Large Language Models for Human Flourishing and Human Accountability / Dave Sanford
- 1M/ Govt-Issued Digital Credentials & the Privacy Landscape (Is there anything you want to tell me) / Heather Flanagan
- 1N/ Assurance Levels or Assurance Details? Mark Haine

Session 2

- 2A/ OpenID 4 Verifiable Credentials OID4VC 101 / Tobias, Torsten, Kristina
- 2B/ Intro to OpenID Connect - an IIW 101 Session / Mike Jones
- 2C/ What is Web 7.0? / Michael Herman
- 2D/ Trust Registries / Nicole Roy and Dmitri Zagidulin

- 2E/ Biometrics & Blockchain Signatures / Troy Samuels
2F/ Regi-TRUST: A Network of Network Model for Discovering and Validating Trusted Ecosystems / Lucy Yang and Savita Farooqui
2G/ Federated Auth Network / Day Watebury
2H/ Introduction to KERI / Nuttawut Kongsuwan & Phil Fearheller
2I/ NO SESSION
2J/ KERI + ACDC 201 Accelerated Developer Introduction / Kent Bull
2K/ NO SESSION
2L/ Credential Migration + A Universal Credential Migration Format / Nick Steele
2M/ Identity Multiplexing for Everyone / Travis Wellman
2N/ Solving Setup for: Federation, Provisioning, Session Security, Account Security/Atul T

Session 3

- 3A/ Organizational Identity & Credentials / Timothy Ruff (DTV) & Phil Fearheller (Gleif)
3B/ UMA 101 User Managed Access - an IIW 101 Session / Steve V
3C/ ABC's of Writing DIDs with Universal Registrar (and how it's different from universal Resolver) / 3D/ Ankur Banerjee (Cheqd) & Markus Sabadello (DanubeTech)
3D/ Where Public Data Streams? How can we share, discover and compare signed data from different sources? / Golda
3E/ Let's Create a Decentralized Community Pattern Language / Randy Farmer
3F/ Is Presentation Exchange the right query language for identity credentials? / Dirk B & Tim C & Sam G
3G/ Identity In/For The Fediverse / Johannes Ernst
3H/ Expanding Language - Humans Think - Chatbots Process - How does that augment or disrupt communication intentions / Jeff Orgle
3I/ Interoperable Trust Registries with DID - Linked Resources (DRL's) / Alex Tweeddale (cheqd) & Andor Kesselman (Benri.io)
3J/ NO SESSION
3K/ NO SESSION
3L/ Protecting Identity With WebAuthn / Matthew Miller
3M/ Introduction (and roasting) to the DCDR Framework (Data-Centric Digital Rights) Jean & John
3N/ McNameo Inspired Method to Crowd Source Congressional Policy / Britt B & Phil Windley

Session 4

- 4A/ NIST SP 800-63.4 Digital Identity Guidelines / Justin R
4B/ Fido 101 AKA Passkey - An IIW 101 Session / John Bradley
4C/ Selective Disclosure * SD-JWT 101 / Kristina Yasuda & Brian Campbell
4D/ Decentralized Identity Foundation (DIF) Update / Clare Nelson
4E/ Energy + Mines Digital Trust B2B/G2B From Pilot to Production / Kyle Robinson (Bc Gov)
4F/ DWeb Camp / Doc Serals
4G/ Governance and Accountability of Decentralized Identity and Verifiable Credentials / Scott Perry
4H/ Anonymous Reputation - What's the State of the Art? / James Monaghan
4I/ Enhancing Your Participation in Tech-Related Public Consultations & UN Digital Compact seeking Feedback Session / Kaliya & Jean
4J/ NO SESSION
4K/ "Good ID..." Is it time for a new framework? / Ethan V ID2020

- 4L/ Next Version Self Sovereign ID - Sovereign Individual System / Ying Liu
4M/ NO SESSION
4N/ Introducing WiKido - A massive multiplayer joint venture workshop 1 of 3 Legal Mechanics of NAO / Jonny Stryder & Bry Benson

Session 5

- 5A/ SPAC = Secure Privacy Authenticity Confidentiality - Tradespace Strongest A+C+P / Sam Smith
5B/ IIW 101 Session - Intro to Self-Sovereign Identity / Limari DIF & Stephen Curran (BCGov)
5C/ Privacy as Alignment of Expectations / Joe Andrieu
5D/ How can DNS help enable Digital Trust! / Marhieu Glaude
5E/ Where are my product peeps in the house? / Bonnie Yau
5F/ 30 days from Web5 - A preview of the stack and Developer Preview release next month / Daniel Buchner
5G/ IDtech & Why it's the key to SSI adoption / Riley Hughes
5H/ Credential Format Comparison / Paul Bastian & Andre Kudra
5I/ Identity + Internet the 17th Sector of Critical Infrastructure - Let's Talk About Why... Bringing the US to a Halt! / The ID Guy (Kenneth Gantt)
5J/ NO SESSION
5K/ Visuals of SSI / Zack Jones
5L/ UX of Diia (a Ukrainian Government App) / Francisco Corella
5M/ Inter - Trust Domain Protocol “Can DiD’s , AID & OpenID talk to Each Other? / Wenjing Chu
5N/ When Browsers, Wallets, & Federation Overlap / Heather Flanagan

Wednesday April 19, 2023 ~ Day 2

Session 6

- 6A/ KERI for DUMMIES & Non-Technical People / Timothy Ruff
6B/ Open wallet Foundation “101” / Daniel Goldscheider
6C/ Good Biometrics vs Chain-Of-Custody in VC Context / Adrian Gropper
6D/ NO SESSION
6E/ NO SESSION
6F/ Detachable Federation Authorities / Justin Richer
6G/ Access Control Use Cases / Alan Karp
6H/ Jurisdiction 101 - The Missing Layer in the Identity Stack -Workshop 2 of 3 /Bry Benson (Wikido)
6I/ NO SESSION
6J/ NO SESSION
6K/ NO SESSION
6L/ What’s NEW with HYPERLEDGER INDY / Char Howland
6M/ KERI and ACDC Developer Introduction / Kent Bull
6N/ NO SESSION

Session 7

- 7A/ So you want to be a QVI... (Qualified vLEI Issuer) / Karla McKenna GLEIF
7B/ Wallet Attestation - Device Binding, Holder Binding, Attested Issuance, Demo E2E w/OpenID, Regulations / Paul Bastion
7C/ Digital Trust in the Age of Chat GPT / Wenjing Chu
7D/ Advanced Topics in DID Resolution / Markus Sabadello & Ankur Banerjee
7E/ NO SESSION

7F/ A Digital Wallet Market Study / Lucy Yang and Kaliya Young
7G/ The Current State of WEBAUTHN / Nick Steele + Matt Miller
7H/ PICOS, Lora WAN, & the SSIOT / Phil Windley
7I/ NO SESSION
7J/ NO SESSION
7K/ Use Cases + Storytelling / Zack Jones
7L/ SSA - New Endpoint to Issue: Software - Statement - Assertions: JWT for OAuth Client Reg / Mike Schwartz
7M/ KERI 301: KELS, TELS & ACDCs outside KeriPy/ Jason Colburne
7N/ NO SESSION

Session 8

8A/ Why Can't I Trust Who's Calling or Texting Me? AND what KERI, ACDC, and vLEIs Can Do About That / Randy Warshaw
8B/ We're SABOTAGING SSI's Chances of Success / Riley Hughes + James Monaghan
8C/ Key & Trust Management? Key Resolution - Trust Lists = Discussion / Comparison / Paul and Christian
8D/ INDEMNIFICATION Identity Risk Management as a Service / Carlos Korten
8E/ State Government Use Cases... and if there is time, The secret to state procurement / Mike Leavy
8F/ Meta Trust Registry - Interoperability of Trusted Ecosystems / Lucy Yang & Savita Farooqui
8G/ Using HUMOR (ha ha ha) and Visual Communication To Gain TRUST / Chance and Zack
8H/ Red Teaming Digital Identities... And Why You Need It! / Tiffany Maoney
8I/ Authentication Context Class References - Where and How to express and convey Authentication Policy / Pam Dingle & Dale Olds
8J/ Talk Session Identity in Ethereum / Jane
8K/ NO SESSION
8L/ NO SESSION
8M/ How to Onboard 1000 Relying Parties (RPs) - a Singapore Case Study / TY & Gayle w/ Assurity Trusted Solutions
8N/ NO SESSION

Session 9

9A/ Query Language for VCs (Presentation Exchange?) Part 2 / Sam Smith
9B/ Verifiable Credential Revocation, 2023 + What might be next? / Stephen Curran
9C/ Linux Foundation - Digital Trust Initiatives: DIF, Hyperledger, Open Wallet, TOIP +++ / Daniela Barbosa
9D/ YOUR DID Method Sucks - Change My View / Gabe Cohen, TBD
9E/ NO SESSION
9F/ Privacy Enhancing Mobile Credentials (PEMC) / John Wunderlich (Kantara)
9G/ Why Open Linked Trust - Open = permissionless to add (and also discoverable claim sources) Linked = can link claim to a common subject or another claim / Golda Velez
9H/ Joys & Miseries of Structured Data - Analyzing the Life Cycle of Authentic Data / Jean Queralt & John
9I/ Auth Z and SSI - Architecture for using an external authorization engine in an SSI ecosystem / Jacob Siebach and Mike Ebert
9J/ Security Encryption Authorization GUNdb peer2peer graph - access control for distributed storage and compute / Colten Jackson
9K/ NO SESSION

- 9L/ Want to make Revenue with Identity? Then Stop talking about Identity! ID DOES NOT = \$ / Rebekah Johnson
9M/ Identity Approach - Public Private Partnerships - What's needed for success? Identity Ecosystem or Archipelago = Let's Talk / ID Guy - Kenneth Gantt
9N/ NO SESSION

Session 10

- 10A/ OpenID 4 Verifiable Credential Issuance (was DID4VC 101) / Tobias L
10B/ SPAC #2 Privacy! Secure Privacy + Confidentiality / Sam Smith
10C/ AI Why We Need DID's NOW / David Yap
10D/ NO SESSION
10E/ Identity Collaboration *SDG* Untangling Chains of Society (SDG) Supply Chain, Portability, Interoperability, Value Chain, Trust Chain / Lubna D
10F/ Internet Data Usage Control System - JLINK / John Wunderlich
10G/ Human Rights Affirming Government Identity AND FSLTT @IIWXXXVI Fed, State, Local, Tribe, Ter - We are here from Gov, we should talk... / Mark H & Elizabeth Garber
10H/ Expanding The Language = Techorata Informed and reflected on by the = Desiderata - Joyful, Contemplative & Serious / Jeff Orgel
10I/ OAuth 1st Party Native App Authentication / George Fletcher
10J/ NO SESSION
10K/ NO SESSION
10L/ VC's in the Supply Chain: GS1 Verifiable Credentials / no name
10M/ ½ AI breaks ID things/cyber security and ½ How VCs/DIDs trust Registries Fixes things / Kaliya Young
10N/ NO SESSION

Thursday April 20, 2023 - Day 3

- 11A/ INTEROP Profile with SD-JWT + OpenID4VC / Paul Bastian & Torsten L
11B/ Using What We've Got - Pure Identity plays probably aren't the answer... / Matthew Miller
11C/ KERI + ACDC 201 Part II / Kent Bull
11D/ NO SESSION
11E/ NO SESSION
11F/ Web 7.0 Trust Registry Framework - TrustReg Documents (DID Documents) / Michael Herman
11G/ BC Wallet and ARIES BIFOLD - What is New? Credential Branding - Mobile Verifier - MORE / Clecio BC.Gov
11H/ The RUBRIC Podcast / Erica Connell
11I/ What the Hell is a HASH? (Crypto for Scaredy Cats) / Joshua Coffey
11J/ NO SESSION
11K/ ANONCREDS AUA / Berend Sliedrecht
11L/ Rubber, Meet Road - The Common Actor Model (CAM) / Chris Kula
11M/ SSI Deployment Challenges / Phil Fearheller w/GLEIF
11N/ Government Issued Digital Credentials & the Privacy Landscape (Is there anything ELSE you want to tell me?) / Heather Flanagan

Session 12

- 12A/ Making Credentials Beautiful with OCA / Stephen Curran

- 12B/ AI and SSI - post security vc. Hellscape - AI is here, moving fast - Our community is uniquely positioned to mitigate harm- - ID, Wallets, PDS's are Key / Dmitri Z., Joyce Searls, Davin
- 12C/ Credential Trust Establishment / Mike Ebert
- 12D/ Interoperability: What does it look like to answer? What baby steps can we take to get there? & 12E Interoperability - What's Hot? What's Not? / Bonnie Yau & Timo Glastra
- 12E/ Blockchain Biometric Signatures II / Troy
- 12F/ Dazzle Office Hours/Intro Get Your Personal Data Back! / Johannes E
- 12G/ Creating A Decision Matrix Around Credential Exchange Protocols / Marrieu G
- 12H/ NO SESSION
- 12I/ Deep-dive on creds.xyz (a decentralized social reputation system for WEB 3 Communities & DAOs) / Ankur Banerjee
- 12J/ NO SESSION
- 12K/ Dynamic Pitch Modulation and Satiric Prose / Jacob Siebach
- 12L/ Thursday Hot Topic! KERI IPR??? If it doesn't get cleaned up it's going to hurt / Kaliya
- 12M/ Fun With DIDComm (sub) Protocols / Nick Reynolds
- 12N/ NO SESSION

Session 13

- 13A/ WebAPI/Quylanguage to VC's (again) / Torsten L
- 13B/ Your Identity IS NOT Self-Sovereign / Justin R
- 13C/ A Working Session: Binding Identity to Publicly Visible Content / Eric S
- 13D/ NO SESSION
- 13E/ NO SESSION
- 13F/ AUTOREP an autonomous decentralized reputation scheme / Johannes
- 13G/ NO SESSION
- 13H/ Json Web Proofs - Status and Progress / Dan (?)
- 13I/ Delegatable Verifiable Credentials / Phil Windley, Alan Karp, Sam Smith
- 13J/ What did I DO? I pointed an NFT to a Verifiable Credential!!! / Mahesh Balan
- 13K/ NO SESSION
- 13L/ Exploring how to engage more w/ Washington DC - What are hurdles to adoption? Kaliya & Rebekka
- 13M/ NO SESSION
- 13N/ NO SESSION

Session 14

- 14A/ The GREAT Migration! DiDs & VCs are done! They face a world full of Active Directory. How do we make it painless to switch? Josh G
- 14B/ VC 'render Method' vc rendering a display / Dmitri Z
- 14C/ Where Will the Generative AI/ML in my Wallet Come From? / Adrian Gropper
- 14D/ NO SESSION
- 14E/ NO SESSION
- 14F/ Open Wallet Foundation = OWF Project Ideas / Torsten L
- 14G/ WEB 15.2 - Shiny Toy or Pit of Despair? John W & Justin R
- 14H/ Yo-ID A reusable IDV network, as simple as possible / James Monaghan
- 14I/ Principled Peacemakers ~ A Real Identity Demo / Johnny Bry
- 14J/ NO SESSION
- 14K/ NO SESSION
- 14L/ NO SESSION

14M/ PERCEPTIONS - Let's talk about those related to identity...But more importantly, what is the Gov't doing with my biometric data? (Inquiring minds want to know) ID GUY - (Kenneth Gantt)

14N/ Did:eth +did:ens Update and CTA / Nick Reynolds

Session 15

15A/ SPAC #3 Secure Privacy Authenticity Confidentiality Privacy - Final Chapter / Sam Smith

15B/ What AI Will Never Be. / Doc Searls

15C/ NO SESSION

15D/ Bridging Protocols / Charles (Charlie) E. L

15E/ NO SESSION

15F/ Browser APIs and Intent Handlers (for wallets) / with Adain (?)

15G/ Digital ID/SSI Researchers/Scholars masters/PHD Student Network? What do we do to start/support this? How do we create annotated Bibliography? Kaliya

15H/ Calling All EDs - What Can We Do Together? / Jean and John

15I/ NO SESSION

15J/ NO SESSION

15K/ NO SESSION

15L/ Hyperledger Identity SIG Launch / Char Howland & Hart Montgomery

15M/ NO SESSION

15N/ GLOBAL Assured Identity Network (GAIN) Update - VCs interop profile - Interoperability /Network or Network / Gail H, Elizabeth G, Dima P, Mark H, Torsten L



Phil Windley ✅ @windley · Apr 20 · 🎙

...

Recording a podcast about decentralized identifiers (DIDs) at #iiw with @IdentityWoman, @dsearls, @JoeAndrieu, & @emsconnell



1

5

19

627

↑

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

SESSION #1

eIDAS 201- Revision of the upcoming European Identity and Trust Framework

Session Convener: Paul Bastion

Session Notes Taker(s):

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

eIDAS 2.0 Large Scale pilots:

- <https://www.dc4eu.eu/>
- <https://eudiwalletconsortium.org/>
- <https://www.nobidconsortium.com/>

<https://www.digital-identity-wallet.eu>

OAuth 101- IIW 101 Introduction Session

Session Convener: Vittorio B

Session Notes Taker(s):

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

API Authentication / Key Credentials / Right of Data Privacy value.

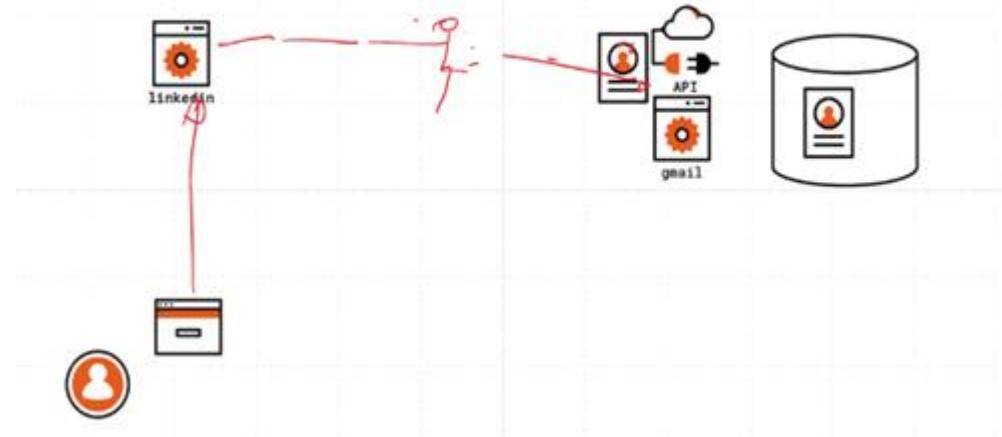
Non permissive adjunct to anyone can do anything with the data credentials.

NOTES FROM IIW #33 Session led by Vittorio - nothing new submitted since then

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

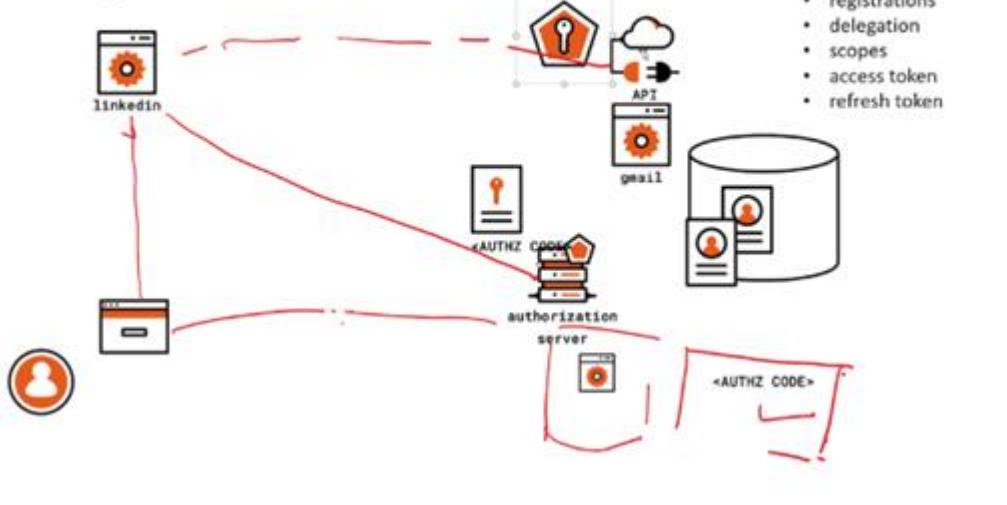
Accessing Resources Across Apps: Brute Force



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 sends 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 sends <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 of OAuth to provide identity federation

Web 7.0 vs. Web 5

Session Convener: Michael Herman

Session Notes Taker(s): ?

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

Web 7.0 is the way to go parsing the advocacy of Web 5.0 transition

Caution on it ~ at Mid-Tier.

Your CORE Identity: YOU are a Child of God

Session Convener: Jacob Siebach

Session Notes Taker(s): Jacob Siebach

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

There is a God in Heaven, and His Son is Jesus Christ.

Each of us is a Child of that God, and He loves us.

“Self-sovereign identity is about being souls in the world.” ~Doc Searls

Each of us contains the seed of the divine.

The idea of *identity* is different than the technology that enables us to do things in our modern world. All modern tech should support the *soul* of the person, and THAT should not be forgotten.

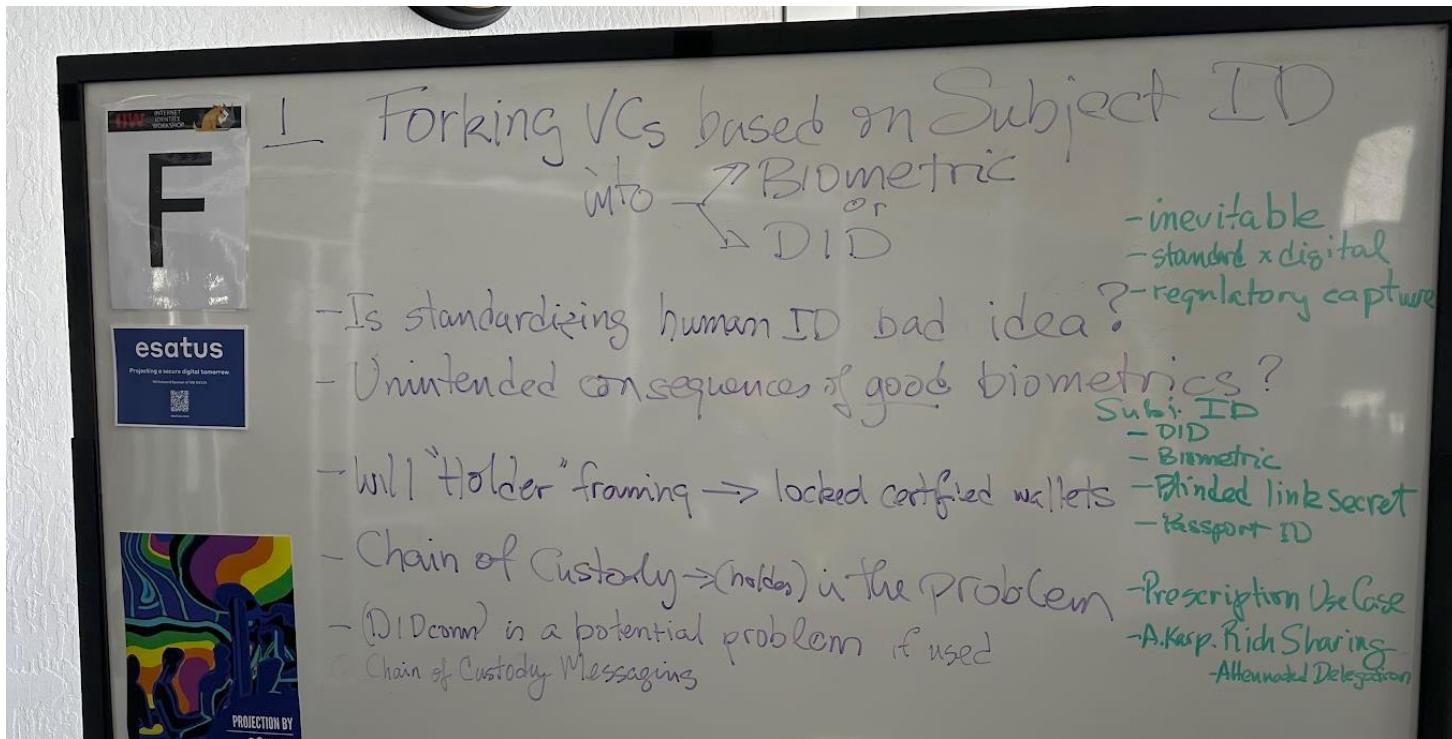
To learn more, visit <https://www.churchofjesuschrist.org/comeuntochrist> and download the Book of Mormon app from The Church of Jesus Christ of Latter-day Saints.

Forking VCs depending on Subject Identifier into Biometric or DID

Session Convener: Adrian Gropper

Session Notes Taker(s): Adrian Gropper

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



Apple's Platform SSO: Leading the Way to Zero Trust on macOS

Session Convener: Dipti Shiralkar

Session Notes Taker(s): Matthew Miller (Cisco)

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

- Apple has integrated authentication using an org's credentials while logging into your actual macOS device
- Challenge: centralized management of authentication, tying "central ID 'user1'" to "endpoint ID 'localUser1'"
- Requires use of MDM to manage identities, device login was only managed by local OS
- What macOS Platform SSO is tackling:
 - Password sync: local account password always synced with organization password
 - SSO: Provide password when logging in, subsequent authentication challenges use info from desktop sign-in
- SSO Steps
 - Registration
 - Registers the keys with the IdP
 - Happens out of band
 - Authentication
 - Completely implemented in macOS
- Requirements
 - Compatible IdP
 - Device needs to be managed by MDM
 - MDM profile is very specific, "SSO Extension Profile" (SSOe)
 - A compatible IdP-provided authenticator that implements the extension, to broker the authenticated session with the IdP after desktop login
- Q: What is the significance of this technique?
 - Number one challenge in the macOS world is central management of identity. No Active Directory in macOS
 - In practice macOS devices have local device accounts created that don't map to centralized IdP identities
 - Second aspect is that end users only need to know a single password, the one to log into their computer. From that point on subsequent authentication challenges in browsers, etc... can instead use the authentication session established after desktop login.
- **Q: What about going passwordless?**
 - macOS requires the password on reboot, like iOS does after reboot, before Touch ID can be used on subsequent authentications. Consider this the "P0" of this support, so true passwordless support might come later. PSSO supports either password or secure enclave as authentication method. With secure enclave PSSO uses key stored on secure enclave instead of password to authenticate with IDP. But this method does not support password sync.

- **Registration**
 - SSO extension running on macOS
 - Keywords (note taker's naivete): "PSSO", "AppSSO"
 - IdP provides an "authenticator" that implements the SSO extension
 - Admin deploys SSO extension profile from MDM
 - First time user logs into device, OS shows system notification telling you to register for platform SSO
 - Notification clicks Register, OS passes users off to IdP authenticator (SSO extension)
 - SSOe requests keys from OS(PSSO): SignKey and EncryptKey
 - OS generates keypairs, returns public keys to extension
 - Extension registers public keys back to IdP server
 - It's on the IdP to figure out how to secure the API request to pass back public keys
 - IdP stores public keys
 - OS prompts typical Touch ID/system password authorization modal
 - SSOE saves login configurations back to OS with typical OpenID URLs for callbacks and IDP username etc
- **Authentication**
 - Agent is out of the picture now, the OS will directly talk with the IdP via provided URLs
 - User enters password
 - OS takes password, makes call to token endpoint with JWT-bearer grant-type
 - Inner JWT has username and password
 - macOS will do some checks (e.g. .well-known) to make sure IdP is securely accessible
 - IdP responds with a JWE (encrypted JWT)
 - **Q: What happens if the endpoint device is offline?**
 - Apple does not block endpoint login so you can still use your computer
 - IdP simply does authentication like usual (e.g. in the browser) when the device comes back online and tries to access a protected system
 - OS calls /key endpoint to validate idtoken
 - Syncs local password with IdP
 - User goes to browser
 - Browser is redirected according to values provided in profile deployed via MDM
 - **Redirect URL**
 - PSSO only works with Redirect (type) SSO extension MDM profile
 - User is redirected to Redirect URL, Apple validates bundle ID configured via MDM profile and hands off request by call back to ssoe plugin deployed by IDP.. if PSSO enabled, this callback would have token as parameter
 - **Q: Where is SSO flow supported?**
 - Only works in Safari and native apps at the moment
 - **Q: How does the IdP establish the authenticated session e.g. in the browser?**
 - IdP needs to know to step up with MFA/etc...
 - **Q: Where is the "Zero Trust" in all of this?**

- This is leading to Zero Trust because it's desirable to establish device identity and device trust
- Trying to approach this from the "zero touch enrollment" angle

Mistakes were made...Product Manager confessions

Session Convener: James Monaghan

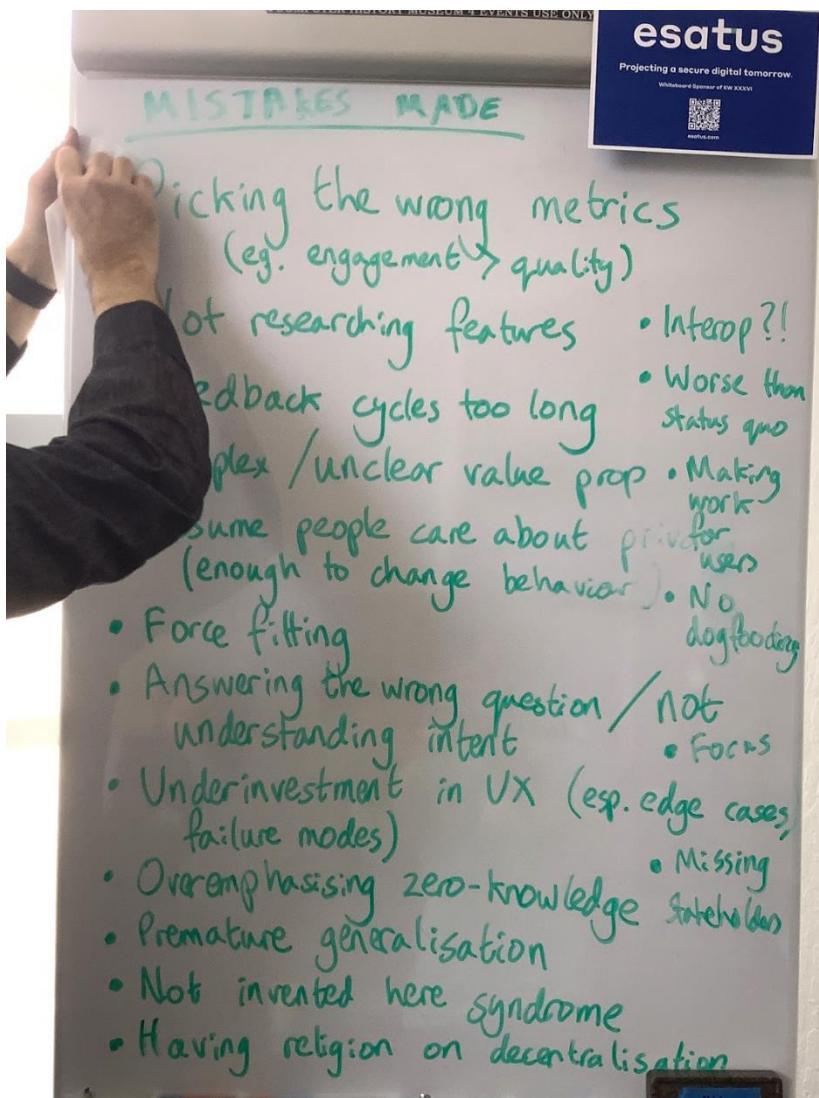
Session Notes Taker(s): Timo Glastra, Ankur Banerjee

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

- PMs not incentivized to research features
- Picking the wrong metrics
 - Engagement goes up, but quality of content goes down, and the community is collapsing. (engagement > quality)
- Feedback cycles too long
- Gamification bad influence
- SSI has a complex / unclear value proposition
- Assume people care about privacy
 - People don't care about privacy as much as we think they do
 - Preaching privacy is like preaching abstinence to teenagers
 - VPN has done it right: You can watch Netflix from US, not privacy
 - People don't want to give up convenience.
 - People actually like personalised ads (when they are not creepy)
- Force fitting
 - Think about what users care about, not features that are under the hood. How transparent do you want to be?
- Answering the wrong questions
 - Good Health Pass. 140 pages roadmap. It went nowhere, as it was answering the wrong question.
 - Question it answered: How do we build the most privacy preserving health passes
 - Question it should have answered: How do we restart travel and tourism in time for the season?
 - The user doesn't care about the answer to the question. The decision must be implicit in the UI/UX, rather than an explicit answer to the question.
- Not enough UX research / underinvestment in UX
 - especially edge cases, E.g. what if your phone dies? Or if there isn't good internet connectivity? This is true for even an event like IIW.
 - Lot of these tech stacks only work on mobile.

- Lot of SSI space does not work in the browser
 - People want portable data. UX of SSI doesn't always work
 - Duck duck go gives a scoring based on TOS Did not read for websites
 - Too much focus on zero knowledge, e.g., a e-commerce company DOES need to know your name and address to deliver packages
- Wrong messaging
 - Saying the user will be the only holding the data (it's wrong, as you will share it)
 - Nobody cares about the terms of service, they all click accept
- Premature abstractions, overgeneralization
 - Building the one platform that is capable of everything
 - Products are a bunch of legos. End result: you can communicate between wallets, but that doesn't solve the customer's problem
- Adding features you think the user might want, instead of waiting for users to provide feedback in what they need
- Not invented here, focusing on the infrastructure too much
 - Not reusing what's already available, reinventing the wheel
- Thinking decentralization matters / religion
 - It's only useful if it achieves a purpose
- Optimizing for the wrong things (e.g. interoperability)
 - Too much focus on interoperability. It's not what customers need
 - The most interoperable are apple / google wallet, you can create a compliant wallet item from any system.
 - Who cares about interoperability? End users? Architects? Governments?
 - web browsers are interoperable, and who cares?
 - Interop is worthwhile as there's no reason to use these technologies if we don't have interop. Everyone can create a proprietary implementation
 - Can't have portability without it, however having interoperability doesn't necessarily give you portability.
- SSI solutions are worse than status quo (Web 2)
 - It's slower, harder to work with, need to know a lot, more complex
 - We're not even meeting the needs of developers
 - As a user the key management with wallets etc.. is way too complex
 - None of the features you have with e.g. banking (undo, recover, etc..) we don't have any of these in SSI
- Too much focus on consent
 - It will become something like a cookie consent, e.g., people will just auto-accept or hide banners like with EU GDPR cookie law
 - E.g. with scanning QRs. Consent to the connection, consent to the credential
- Focus on data over capability
- We should be innovating on what we want to be best in the world at, and not anything else.
 - We should not invent a new database, or a database query language
- lot of focus on signing, verification, infrastructure
 - but what does it mean for the user
 - too much focus on how computers exchange information, rather than humans

- What can we do?
 - Bring in the stakeholder often and early.
 - Why is this so hard?
 - Because it's expensive, people don't want to spend the money to do it
 - Too many people building the infrastructure that is hard to use
 - Is the product the infrastructure
 - Lack of dogfooding
 - Less into the technical details
 - Missing stakeholders
 - e.g. with identity you're often nowhere without the government



Identity Ecosystem Picking Up Where NSTIC Left Off... Who, What, How, Why it's All Here Ready to Re-Establish! / ID Guy

Session Convener: Kenneth Gantt

Session Notes Taker(s): Travis Edwards

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

NSTIC - National Strategy for Trusted Identities in Cyberspace

[NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE](#)

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

No Other Notes submitted

Polyversal Coordination Stack for PLANETARY Self-Governance

Session Convener: Day W

Session Notes Taker(s): Joe Andrieu

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

https://en.wikipedia.org/wiki/The_Starfish_and_the_Spider

<https://80000hours.org/podcast/episodes/audrey-tang-what-we-can-learn-from-taiwan/>

https://en.wikipedia.org/wiki/Audrey_Tang

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

What do we need in a framework for planetary governance.

Question: what does governance mean in this case?

IIW is a great example. Open Space allows people to self-govern.

Governance is the whole set of tools and approaches to managing activities.

Thought: what if we had laws through global voting wouldn't that require a registry?

What about Worldcoin?

Similar challenge. Can we avoid the global database?

For voting, you don't need an eternally unique personhood. You just need to prove *for a particular election* that the voter is eligible for that vote.

Comment: how do we make and enforce rules (as a social interface, regardless of technology)

What are the patterns we need to create?

What are the outcomes we can test to understand if we succeed?

Planetary flourishing as a metric?

What are the pro-social patterns to replicate?

Start with self-organization. Necessarily the groups are smaller?
(at least at the start)

If we start with a pattern that, when set loose replicates itself.

Note: "The Starfish and the Spider" https://en.wikipedia.org/wiki/The_Starfish_and_the_Spider

One thing many people do, is procreate. Then individual groups, as groups, should duplicate.
Which allows for iteration & evolution.

Important to identify the intersection between the group and its function. United Way versus Social Club. The point is the mission.

The kind of goals that we actual have, cannot be accomplished by large hierarchical organizations.
Disagreement on that. It's just harder for them to change. Harder to get consensus, easier in small group to take actions.

Scaling with centrality is easy. So how do we scale without centrality? That's hard.

If we solve the small part, the rest will grow.

Thought: temporality in governance (constitution, law, regulation, policy)
These separations matter.

It's not just about

We often think of governance as the voting or fairness of participation.

But we also need to look at the whole process of sense-making that precedes that vote.

Must include disinformation, propaganda, coercion, enfranchisement, framing, etc.

We can't all invest in understanding everything.

What we all have in common, is an ingrained sense of fairness. Toddlers understand the fair distribution of apple.

As an individual (pre-historic) person, you could feed yourself. But if you needed to get the mammoth, then you needed to make sure you get a piece of the kill.

I don't think we need to vote, we need to poll. At its limit, polling is voting.

If you've self-selected into a topic, become an expert.

I like the notion of a free commons where any idea can be advocated and those ideas that get support build social awareness and eventually change.

Example: Polis is <https://pol.is/home>

Polis is a real-time system for gathering, analyzing and understanding what large groups of people think in their own words

Pictures of agreement (tadpole diagram)

Reference to other work

<https://80000hours.org/podcast/episodes/audrey-tang-what-we-can-learn-from-taiwan/>

https://en.wikipedia.org/wiki/Audrey_Tang

Indigenous conception of law: like a jaw. The upper jaw is immutable, always true. The bottom jaw is adjustable, about what we are focused on.

Thoughts for businesses: how do you structure to participate in benefit.

If you don't allow autonomy at the individual level, you won't have self-governance.

Leverage is greater in larger organizations.

What about the biggest stick? Force will be used. How do we handle that?

The goal is a platform that is coercion free.

When we say "healthy competition" ... that implies a safe framework within which we compete.

Can we move past rivalrous competition?

Antipatterns out there in ideas of eternal and immortal corporation.

The most troubling thing about AI...

UBI provided by taxing AI

That's hush money.

Where we are in time (AI):

In 2000 we have small models, small PCs, etc. We had lots of clients, trained it up and made it work. For each client they'd get something customized.

You don't see patents on AI some methods because you can't patent math. The main thing that OpenAI did was gather the data.

Efforts to enclose the commons.

Commons were built in a world of constrained resource.

vLEI Update

Session Convener: Karla McKenna

Session Notes Taker(s): Karla McKenna

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

www.gleif.org vLEI tab at top of landing page

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

Updates provided on:

The vLEI ecosystem and infrastructure went live in December 2022.

The Inception Event was held to create the Root of Trust for the LEI ecosystem and infrastructure.

GLEIF then was able to issue the first in production Qualified vLEI Issuer vLEI credential to the first QVI, Provenant.

GLEIF then contracted with Provenant to become GLEIF's QVI. Following the requirements and processes in the vLEI Ecosystem Governance Framework, Provenant then issued GLEIF the first in production Legal Entity vLEI credential, followed by the first vLEI role credential, an Official Organizational Role vLEI credential to GLEIF's CEO.

These credentials are listed in the vLEI section of GLEIF's LEI page on www.gleif.org.

All Legal Entity vLEIs and OOR vLEIs issued will be listed on the LEI page with subsequent revocations noted.

-Qualified vLEI Issuer Program

One qualified; 4 in the application phase; 5 in the evaluation stage.

Working closely with a group of organizations on the development of an SDK for QVIs.

vLEI Infrastructure

GLEIF Controller and GLEIF KERI Witness Network - live.

Design work is underway for Hyperledger Indy Ledger Anchored vLEIs

vLEI Ecosystem Governance Framework

v1.0 EGF was published on gleif.org in mid-December 2016 coinciding with the launch of the vLEI ecosystem and infrastructure.

An update of selected documents in the EGF was published in mid-April 2023

LEIs keeping pace with digital transformation

Use of LEIs is relevant as our world undergoes digital transformation

There is an opportunity for secure, verifiable organizational identity to be realized more cheaply, with certainty, by leveraging improvements in automated cryptographic verification - with *organizational credentials*, like the vLEI

Link to presentation:

https://td2ec2in4mv1euwest.teamdrive.net/bqpcsfcc/public/VnNI-vPK?k=vhKxs8djNoF0eL6R_Foyi-P-42eho312nZWgy8DBNEg

Large Language Models (LLMs) for Human Flourishing and Human Accountability

Session Convener: Dave Sanford

Session Notes Taker(s): Dave Sanford

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

We split the white board into 'Human Flourishing' and 'Human Accountability' halves and talked about both. Often risks and vulnerabilities of desired use cases to promote human flourishing led to mechanisms for human accountability or vulnerabilities associated with lack of human accountability - so the notes below do not reflect the order of discussion.

Human Flourishing

Before most session attendees arrived there was a short discussion of how AIs could support the creation of more effective and possibly individual Vendor Relations Management (VRM) functions. The problem with maintaining VRM functions is that (unlike vendors) most customers are not interested in safeguarding their interest longer than it takes for a transaction. Vendors are in it for the long haul which has led to vendor capture by many organizations that were created to act in the customer's interests.

AIs could maintain the longer term attention to customer's interests that humans often can't be bothered to.

The main discussion involved an AI supply chain where a large company created more generic LLMs that could be handed off (via sale or other means) to individual or organizational customers - for them to train for their individuals needs. They would be trained for specific purposes that only the individual or organization could know or implement.

I gave various examples in my partially successful attempts to use Quora's Poe service to create a fiction writing coach that understands various developmental editing approaches and criteria that are specific to my needs.

Attendees suggested that LLaMa and Alpaca may already be there, but Alpaca has been pulled back, but people can get on the waiting list.

There was discussion of how much or what feedback to the generic LLM maker would be valuable to the user if they could have visibility and control over what feedback was required.

Human Accountability

There was discussion of recent articles from Tristan Harris (Center for Humane Technology) pointing out the potential irresponsible or malicious uses of LLM technology.

Legally Enabled Self-Signed (LESS) identity is perhaps the strongest Decentralized ID framework for human accountability. LLM AIs (or any other kind) operating autonomously across the net could have DIDs, which could be queried to determine what human or organization was responsible for it. If it couldn't identify itself and/or identify who was responsible for it - the receiver could 'deny list' it.

There was a similar discussion for open source or other software licensing and version control - such that you should be able to trace code provenance back to a human.

There was a discussion of the need for regulation to either require or standardize good behavior or provenance back to a human, which seemed unenforceable and a preference for industry to take design and standards responsibilities in this area.

As a lower, but probably necessary standard (e.g. in totalitarian countries) there was a discussion of pseudonymous identity for humans - with the recognition that in this case all trust would be created over time using selective disclosure.

Finally, there was a discussion of the variability of jurisdictions to enforce or regulate these things based on legal differences including, but not limited to free speech and libel laws.

Government-Issued Digital Credentials White Paper

Session Convener: Heather Flanagan
Session Notes Taker(s): Nicole Roy

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

<https://openid.net/2023/04/05/open-for-comment-privacy-landscape-whitepaper/>

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

60+ page paper

First $\frac{1}{3}$ of paper - survey of what's happening

Reasonable sampling of what's going on now

What are the privacy implications of what's going on now?

Biggest gov issued digital cred: India

Most ubiquitous: Singapore

EU

Italy

US

Nigeria

Paper is currently open for comment! Please read and comment!

Middle $\frac{1}{3}$: analysis:

OECD privacy framework

NIST requirements

GDPR etc....

Heather wants the gov policymakers to have an understanding of what's going on around the world. Geopolitical barriers are permeable.

Want civil society / lobbyists / etc. to be informed

Also talking to the people writing the technical standards to try to get them to understand how their stuff is being used in the world today.

Involved a lot of interviews and listening sessions, etc.

Lot of researcher - peer-reviewed research. Citing sources.

Last $\frac{1}{3}$ of the paper - recommendations:

Bringing things back to the basics, would be really nice if people doing this stuff were securing their systems first. Data minimization has been a thing for a very, very long time. These are not provocative or new recommendations.

Advanced cryptography

Something that Heather struggled with: Recommendation that each relying party should be certified and registered according to what information they may collect. Registered with “the government” (generic). Lots of people in the group seem to also be concerned about this.

Is this because it’s a tech requirement, or a government requirement? With SSI the idea is that anyone should be able to verify.

The issue is perceived safety problems with people interrogating credentials for info they shouldn’t be collecting.

Selective disclosure - some parties allowed to retrieve certain info, etc. Gov. of Ukraine does this.

In Italy, relying parties do have to register with the gov for a small fee, in order to keep the system funded.

“We want to protect your privacy” - paternalistic, patriarchal and probably wrong. Autonomy and choice comes from the individual.

Reasonable disclosure levels - how much info, what type, boolean answers, etc. “Is this person over 21?” [Y, N]

Being paternalistic isn’t the answer, doing better UX so people know and understand what’s being asked for is the answer.

“How can governments demonstrate their compliance with requirements for privacy preservation” One idea is that the private sector should lead the way. The belief that verifiers need to be registered in order to consume gov credentials, that’s not the way it works in the physical world, don’t want that to be the way it works in the digital world, either. Hope that we can supply a UI component that interacts with the verifier, such that the verifier has to share how this data will be used, so the person can make an informed decision about sharing data with the verifier.

In US, room for something like the office of inspector general to audit as gap remediation? Difference between government issuing a credential, and gov regulating who is checking that credential.

Issuer should have no idea where the credential is used. Checking status / revocation check should also not be able to be observed by the issuer.

Need audits to make sure implementations of privacy-preserving standards are actually correctly and securely implemented.

Requiring certification of implementation for verifiers / RPs for secure implementations/deployments a la PCI-DSS is not a bad thing. Register these certifications in an open ledger. Also make public “this is the information that we collect for the purposes of x” (letting you in the bar, etc)

Huge diversity / depth of cultural differences w/r/t cultures trusting the government versus trusting commercial sector.

Do we just need a GDPR for the US? Yes.

Agreement that it's a UX problem, that is much better than a EULA or GDPR implementation.

Threat modeling the government important

How does this interface with PHI. Discussion about interplay with department of health and human services. Entities that can be subpoenaed and disclose data about what medical services a person is using. Something like an anoncred may be best. OIDC ID token not so much.

Tech can do whatever you design it to do. Policy/governance/trust layer is crucial.

Lack of trust for both public and private sector.

Non-profit, non-governmental sector, the orgs that in many cases do have more trust. Consumer union, consumer reports, IIHS, etc. Orgs or consortia that could be monitors/arbiters of this.

Missing layer: Out-of-band-governance that governs what the tech should do, and does.

Governments have an obligation to share the information of who is using and requesting the information. FOSS need to be at the core, and transparency is key. Any authority making a statement about data should be issuing a W3C VC. And we will need to be able to verify this information decades in the future.

Conversation comingles issuing and consuming the data. Issuing the data is a unilateral act, and it can be blind to how it is consumed. The provenance of the data can be solved cryptographically. There is a zero knowledge proof infrastructure that would support this. Issuance isn't the problem, consumption is the problem.

SSI talks about everything up to the point of verification, but that's not where any of the problems are. It's about what happens after that.

Assurance Levels or Assurance Details?

Session Convener: Mark H
Session Notes Taker(s):

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

No Notes Submitted

SESSION #2

OpenID 4 Verifiable Credentials OID4VC

Session Convener: Tobias, Torsten, Kristina

Session Notes Taker(s):

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

No Notes Submitted

Introduction to OpenID Connect

Session Convener: Mike Jones

Session Notes Taker(s): Mike Jones

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

OpenID Connect and related work, including OpenID Certification

The deck used the presentation is at http://self-issued.info/presentations/OpenID_Connect_Introduction_18-Apr-23.pptx and http://self-issued.info/presentations/OpenID_Connect_Introduction_18-Apr-23.pdf.

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

There were good questions about errata, implementing logout in the face of browser changes, the legal agreements enabling federation, and certification.

What is Web 7.0?

Session Convener: Michael Herman

Session Notes Taker(s):

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

No Notes Submitted

Trust Registries

Session Convener: Nicole Roy and Dmitri Zagidulin

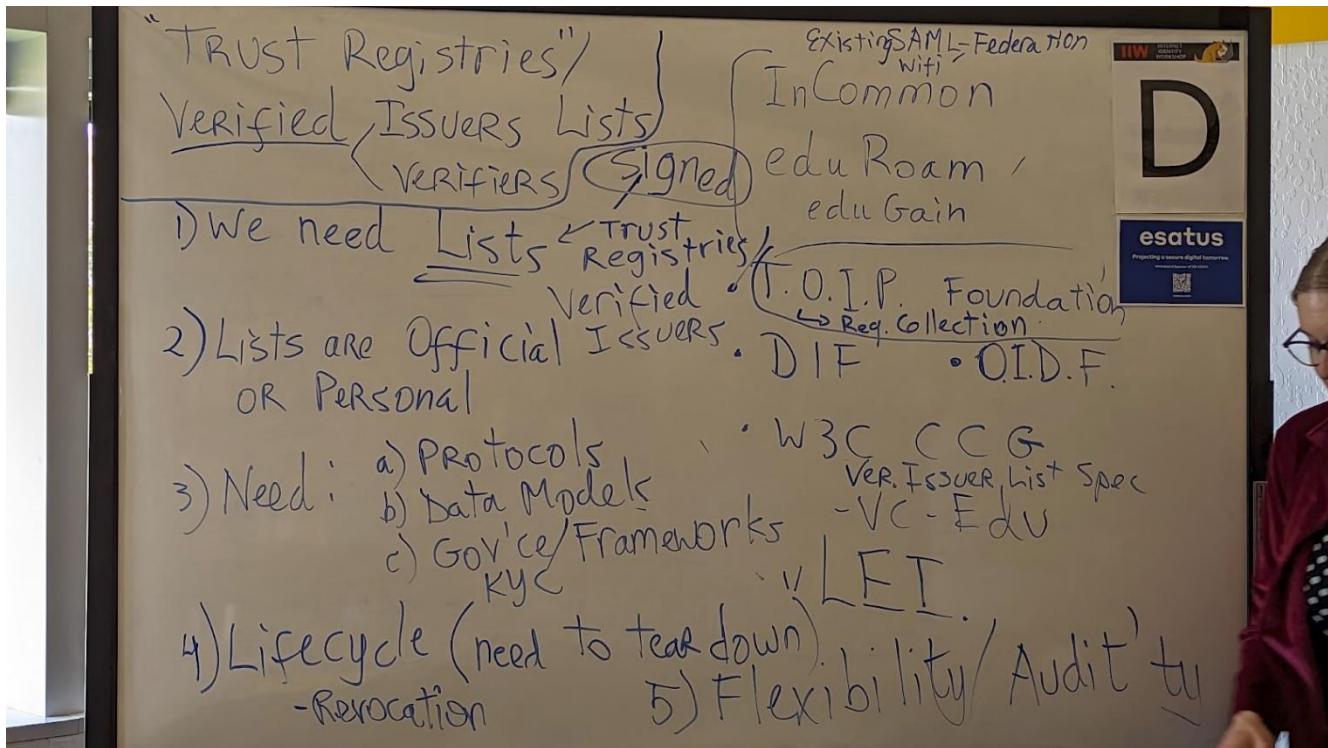
Session Notes Taker(s): Nick Reynolds

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

Trust Registries

- How to articulate multi party trust networks?
- InCommon Federation - 6000+ members?
 - Part of global mesh organization called eduGain / eduRoam
 - InCommon does organizational validation
 - InCommon issues “trust marks”
- We have VCs, but still need to trust the issuers. Need a trusted mapping.
- RWOT - Verified Issuer List / Verified Verifier List
- Trust Registry Data Model being incubated at W3C C&C CCG
- A Trust Registry is a list of identifiers (+ name/logo)
 - Can include Credential Type per issuer (but not necessarily)
- What is the need for this registry?
 - Identity Provider:
 - e.g. Penn State University
 - Relying Party:
 - e.g. Instrument system at CERN
 - CERN needs to KNOW that certain data comes from PSU
 - Governance processes already exist. Want to make sure the Trust Registry and those Governance processes are speaking the same language.
- Where are registries kept?
 - Anywhere.
 - Some on Distributed Ledgers
 - Some on specific servers
 - Others on user’s device
- TOIP Tech Stack Working Group for Glossaries working on a glossary for Trust Registry / Trust List terms
- DIF C&C CCG Trust Establishment Work Item
- What if an organization has multiple legal entities?
 - possible solution: OpenID Federation spec
- Trust Registry concept applies at massive organization level but can also be per-user (e.g. trusted contact list)
- Response to Possible Threats
 - Processes similar to how TLS operates
- CTAs:
 - Join ToIP / DIF WGs

- Use Cases:
 - Health providers that are trusted to issue Covid Tests
 - Professional Trades credentialing
 - Local Groups (e.g. pickup soccer)
 - Constrained Delegation (e.g. medical proxy)
 - Almost any DID use case



Biometrics and Blockchain Signatures: Identifying pitfalls.

Session Convener: Tchaikawsky "Troy" Samuels
Session Notes Taker(s): Troy

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:

Concerns:

Avoid using a centralized entity like (NEC) performing the biometric hash creation due to Govt corruption, and single point of failure that compromises all users. Employ decentralized identity management.

Unexpected directions it went into was using the biometrics to create a wallet.

There are pitfalls there. Does not help build trust between Govt and Blockchain pseudo anonymous identities.

NEXT Discussion topics:

Does open source biometric matching software exist?

What's the incentive to use if it is not mandatory? How can economic incentives be employed to help promote volunteer use? Similar to how driver licences are used to shop, create bank accounts, enter bars etc...

Discuss the privacy implications of moving forward and how this can be abused in a dystopian world?

How can this be used in place of government ID in day to day activities?

Regi-TRUST: A Network of Network Model for Discovering and Validating Trusted Ecosystems

Session Convener: Lucy and Savita
Session Notes Taker(s):

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

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

<https://www.sparkblue.org/Regi-TRUST>

Federated Auth Network

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

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

No Notes Submitted

Intro to KERI

Session Convener: Nuttawut Kongsuwan (Finema) and Philip Fearheller (GLEIF)
Session Notes Taker(s): Catherine Nabbala (Finema)

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

Link to the presentation: <https://bit.ly/keri-101>

Outline:

Theory

- Key Event Receipt Infrastructure (KERI)
- Autonomic Identifier (AID)
- Key Event Log (KEL)
- Key Event Receipt Log (KERL)

Demo

- KERI Command Line Interfaces (KLI)

Points discussed

- AIDs are Primary Roots of Trust in KERI
- There are 2 Levels of Authentication.
 - 1. Tying the control to some an unknown entity.
 - 2. Tying the controller to a known identifier
- The primary innovation is making the binding cryptographic
- Advantage: No exposure of Rotation keys so KERI keeps the keys in TPM so that the Rotation Key is not exposed.
- KERI has witnesses as well, similar to the Traditional Contract signing. Key Event Receipt is a key event with one or more signatures from witnesses/validators.
- During exchange of keys, one party will be the controller and the other will be the validator.
- Witnesses don't rotate their key pairs. Only the controllers do. Witness list is rotatable.

- KERI in a nutshell
 - Key -asymmetric key cryptography
 - Event -a series of key events that are related to the management of public keys and identifiers, including key rotations
 - Receipt- signed receipts from witnesses of key events that provide an additional threshold structure.
 - Infrastructure- an open-source framework for building decentralized identity systems.

DEMO: What can you do with KERI

KERI + ACDC 201 Accelerated Developer Introduction

Session Convener: Kent Bull

Session Notes Taker(s):

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

No Notes Submitted

Credential Migration + A Universal Credential Migration Format

Session Convener: Nick Steele

Session 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:

- We've (presenter / Dashlane / 1Password?) begun working on a new scheme for credential migration and are interested in figuring out what a migration format could look like
 - Looks pretty similar to TLS in my mind
- There is no standardization for how password managers (and soon, credential wallets, which is what password managers have slowly been becoming) migrate data between each other
 - We want something that is not just a raw CSV

- Post-Lastpass breach, 1Password had a lot of users migrating over; in order to support that, it was an extremely manual process for 1Password
 - They output a CSV which 1Password had to marshal on their own and support users as they moved their credentials into their new wallet
- Question: What's the breakdown of users using 1Password for just passwords vs those using it for other types of credentials?
 - A large minority uses it for things outside of passwords (secure note storage, credit cards, addresses, etc)
 - 40%?
 - 1Password is simply an arbitrary secure storage provider
 - In Summer, 1Password will start supporting passkeys
- Question: Is providence and attestation w/r/t passkeys in-scope for 1Password?
 - There should be some way to say where a credential came from after it's migrated
 - EG, a passkey that migrates from 1Password to Dashlane should have some audit trail showing that the passkey came from 1Password eventually
 - Signature Count, Original Providence, would be something I want to know as a credential manager or potentially as an enterprise
 - Enterprises moving at scale from LastPass to 1Password
 - How do I do this in my datacenter where I use LastPass to provision CID secrets and I need to move them from LastPass to my new solution?
- **Proposed Credential Migration Scheme**
 - Today, you just export a CSV from your current provider (Dashlane etc) and upload it to the new provider, and the new provider has to figure out how to interpret it
 - Way this works is similar to TLS
 - Let's say user is trying to migrate from 1Password to Dashlane
 - Dashlane produces a public key; drag it into 1Password
 - 1Password creates a symmetric key that is then used to encrypt the vault data
 - 1Password hands back public key along with encrypted vault and additional metadata
 - Dashlane recreates encryption key using 1Password's public key and Dashlane's private key (ECDSA) and uses it to decrypt vault
 - This all happens locally, not over a network (ideally)
 - Flow is designed to require manual user involvement so it can't be automated
 - Want to factor in providence – if a user has both a personal vault and a business vault, given the business has providence over the credentials in the business vault, they shouldn't be migratable by the user
 - No middleware involved – needs to be a universally-understood format that anyone can produce and consume
 - 1Password can't migrate from smaller managers (eg some crypto wallets) because they have no idea how to deal with the export format
 - The onus is on the importer to marshal credentials that come through, which should be changed

- Having an interoperable format provides benefits beyond just import/export between password managers
 - Other services and functionality could be built on a standardized credential export format
- **Question:** Is 1Password intending to be a backup method for private keys or do they intend to enable usage of them?
 - The goal is to have 1Password now handle signing functions for wallets/deployment operations/RBAC/etc.
 - 1Password is more likely sooner than later going to be moving to being more of a cryptographic functionality provider for users
 - Users don't want big tech (Google/MSFT/etc) to control all their information
 - It is "absolutely" the goal to enable migration from Google/Apple/Microsoft wallets into 1Password
- **VDATA (Vault Data) format**
 - Some auth data around the key
 - Attestation attached to key
 - Was the user verified when they created the export?
 - Synced credential(???)
 - Key info and private key
 - Metadata
 - Providence
- **Question/Thought:** Why not have fundamental usage rules for credentials/passkeys/etc. built into the spec for the data formats?
 - EG, a passkey that dictates that it can't be migrated/exported
 - How would an enterprise admin specify "credentials can be transferred 1Password -> 1Password, but not 1Password -> Dashlane"?
 - Nick would rather be in a place where a policy exists locally on the user machine as opposed to on a policy server
 - Export shouldn't work just because we can't reach the policy server
 - Exporter/importer should adhere to these policies
- **Thought:** TCG is doing work on transferring credentials between TPMs, "which is freaking hard". You're walking into that territory.
 - The approach they took might be worth looking at
- **Question:** What's the business case for this? Elephant in the room: why would password management companies *want* to make it easy to leave their platform?
 - It's a two way street (if it's easy to export, it's easy to import)
 - Users expect to be able to export
 - Today, if I want to export, I produce a raw CSV with all credentials
 - If that CSV is compromised, I (1Password) am now implicated in this breach
- We are looking into trusted computing / homomorphic schemes
- **Question:** Would you consider a middle layer (such as a blockchain) to protect transmission between exporter and importer / to help attest to importer authenticity?
 - We're not ultimately concerned with who the importer is or why they want the data; more so that the user consents and wants it to occur

Identity Multiplexing for Everyone

Session Convener: Travis Wellman
Session Notes Taker(s):

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

No Notes Submitted

Solving Setup for - Federation, Provisioning, Session Security, Account Security

Session Convener: Atul T
Session Notes Taker(s):

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

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

No Notes Submitted

SESSION #3

Organizational Identity & Credentials

Session Convener: Timothy R (DTV) & Phil F (Gleif)

Session Notes Taker(s):

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

OPENID4VCs allow variety of choices in the VC Tech Stack

Verifiable Credentials (VC) is generic term, including but not limited to W3C VC, ISO 18013-5 (mDL), etc.

Since last IIW, the following happened

1. EU adopted OPENID4VC for the upcoming EUDI initiative

UX

OPENID4VP

- Query language to granularly specify what kind of credential Verifier wants. (use DIF Presentation Exchange 2.0)
- Verifiable Presentations are returned in a newly defined VP Token
- simple overall architecture e.g. device local communication when same device flow is used

Same Device (VP Token in redirect URI)

Cross Device FLOW (VP Token sent via HTTP POST)

OpenID for VP over BLE, NFC tap under consideration

cross device flow has security issue that phishing could happen

Transcript via [Whisper Transcription](#):

[Inaudible] >> If you look really closely in terms of, oh, the thing, what this response mode is really trying to get around is that the the AES or the IDP or whatever terminology you subscribe to from the next slide, maybe an AES, run an old scenario, is that the wallet might be a native application here, right.

So it doesn't have any backing endpoints to serve the response back to the client to verify.

So instead, the responsibility gets inward to the verifier and instead posts an endpoint that the client, that wallet can actually send a response to, it's redirect and then complex the redirect.

So, because obviously redirects are limited and they're kind of sized in response mode, sized in response you can actually send through them, this kind of resolves that limitation of, you know, carrying an artifact too large to go with the redirect.

- So you're saying that with this to work, the verifier must be an online service.

- Correct.

In this scenario, I must have a back-end address for one point to send results.

Okay, but you have another one that shows me where the bear fire is in the app.

Is your example a very common question.

Are you talking about the Bluetooth flow.

No, I'm talking.

You're talking about the.

The lights.

Yeah.

I've got two native apps, right.

I want to invoke them all to hit, right.

the app could invoke the wallet through a clean URL mechanism.

Right.

And then when it's done.

[Inaudible] - Right, so, I mean, fundamentally, we're creating request objects and response objects, and putting them into URLs because that's the system we have available to us with operating systems today.

They don't understand that we're trying to coordinate between multiple wallets, that we're trying to do best response protocols.

So the limitations are that these are query parameters, and they go to the server after about 16k a lot of servers or into other years will choke.

So doing the post helps there.

If you were doing app to app, you could use the existing private response mode.

VP Token is a container. Other related conversation

[Inaudible] >> It basically tells you how the query was set aside, right.

So the verifiers are going like trying to get like in a complicated query scenario, like I've been given back some credentials and it's unclear to me maybe how they satisfy the query I made.

- And we're not holding-- - Good preparation for this.

- Exactly.

- And then for example, if like the (mumbles) (mumbles) for both the enterprise and the response.

So is presentation and submission part of the presentation execution.

Yeah.

That's defined and then-- Sorry, no question.

So is presentation and execution only for acquiring, but also to surprise the response.

Yeah.

Sorry, I wasn't clear.

Yeah.

Do you think that was a good question.

[LAUGHTER] I'm very special about that.

Yeah, that's a good question.

Where will the enterprise happen.

No, no.

[INAUDIBLE] OK.

Can we hand it over to Anuradha for questions.

[INAUDIBLE] [Inaudible] So at the key token, since there's only one part of our presentation, and let's say it's a DJI, you'll have the two-programmed string, which is a WWE-type string.

If one string was just returning a DJI and handoff, you have the key token array, which is two strings, one is a DJI, and the second is a handoff.

Both are starting individually, the whole array is not coming.

I didn't know what part of the string he used to sign that.

[INAUDIBLE] Oh, that's coming.

So in this, I mean, do we assume that the subject has a date or not.

We assume that the credential, if it is happy that it is-- if it is a way to prove possession of the key that is near to do the credential, I mean, what the botasan will take any assumption of what the mechanism might be to be wrong about the key for the inside, why the magic of the key could be hit.

That is what we've actually had in the credential.

[INAUDIBLE] The only relationship we probably use in a protocol and the credential is [INAUDIBLE]
[INAUDIBLE] So we've got a non-singular request.

So what the security preservation says, this nonce needs to somehow turn up in that presentation.

Because that's the way you tie this presentation to the actual transaction.

So that needs to be a audience specification, and there should be a binding to the session that could be a challenge for Monster.

That's the only points that we have to connect to their presentation and the active contact.

Everything else here within that presentation is depending on what the specific credential format uses to make the preregional.

I just want to make sure I answer the question.

Yeah, I think you might miss something.

So in the sound of light in the VP's, you say, "Here's the different presentations I have and where the different data comes.

UMA 101 - Introduction to User Managed Access

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

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

- [Slides \(PDF\)](#)

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

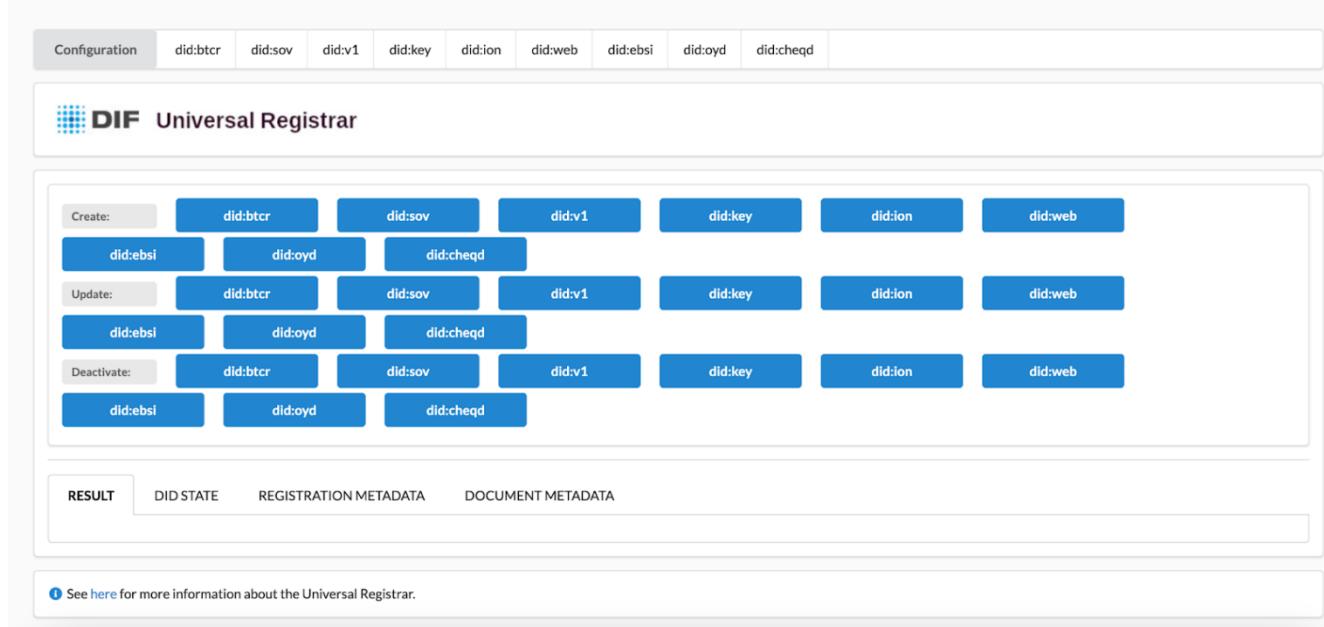
ABC's of Writing DIDs with Universal Registrar (and how it's different from Universal Resolver)

Session Convener: Ankur Banerjee, [Markus Sabadello](#)
Session Notes Taker(s): [Ankur Banerjee](#)

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

- [Universal Registrar / DID Registration DIF Specification](#)
- Universal Resolver example/demo endpoint: [uniregistrar.io](#)

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



The screenshot shows the Universal Registrar interface. At the top, there is a navigation bar with tabs: Configuration, did:btcr, did:sov, did:v1, did:key, did:ion, did:web, did:ebsi, did:oyd, did:cheqd. Below the navigation bar is a section titled "DIF Universal Registrar". This section contains a grid of buttons for performing various actions on DIDs. The grid is organized into rows and columns. The first row has buttons for Create: did:btcr, did:sov, did:v1, did:key, did:ion, did:web. The second row has buttons for did:ebsi, did:oyd, did:cheqd. The third row has buttons for Update: did:btcr, did:sov, did:v1, did:key, did:ion, did:web. The fourth row has buttons for did:ebsi, did:oyd, did:cheqd. The fifth row has buttons for Deactivate: did:btcr, did:sov, did:v1, did:key, did:ion, did:web. The sixth row has buttons for did:ebsi, did:oyd, did:cheqd. At the bottom of the interface, there are tabs for RESULT, DID STATE, REGISTRATION METADATA, and DOCUMENT METADATA. A note at the bottom left says: "See [here](#) for more information about the Universal Registrar."

- Universal Resolver makes *reading* DIDs easy
 - You don't *have* to send the requests to dev.uniresolver.io, you can run your own instance
 - Abstracts the complexity: e.g., `did:ion` needs to read from IPFS, `did:cheqd` needs to read from Cosmos, `did:ethr` needs to read from Ethereum. This is complex for developers, hence the Universal Resolver makes it easy to make reads happen
- Universal Registrar aims for the same but with *writing/updating DIDs*
 - This is significantly more complicated challenge, since there's unique formats/protocols for each DID method
 - E.g., for `did:ethr` an update requires signing and payment in ETH, whereas `did:cheqd` would need payment in a Cosmos token
 - Simple REST API for DID operations
- Why build a driver?
 - Support for other languages. E.g., cheqd developed a JavaScript SDK, but other people needed support in Python, Rust, Golang etc. Building and supporting SDKs in multiple languages is complex and expensive. Having a Universal Registrar makes it possible to support integrations with libraries in other languages.
 - Developers who want to build apps often have ability to sign messages (e.g. Ed25519) but don't know DIDs and/or specifics of the underlying ledger. This abstracts that complexity away.
- Example run through using `did:cheqd` to create a DID using a Universal DID Registrar driver:
 - Demo video: cheqd Demo - How to create a DID with JsonWebKey2020
- Another example taken was godidddy.com (DanubeTech's paid/hosted version of Universal Registrar)

Let's Create a Decentralized Community Partner Language

Session Convener: Randy Farmer

Session Notes Taker(s): Randy Farmer (whiteboard shots)

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

Follow up discussion will take place initially on <http://community.spritely.institute>. Use OCAPN2023 as the keyword to register.

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

Is Presentation Exchange the right query language for identity credentials?

Session Convener: Dirk B & Tim C & Sam G
Session Notes Taker(s): transcript of conversation

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

Tim: The background of query language of getting verifiable identity attributes

- DIF presentation exchange 2.0
- Advanced Syntax from OIDC

Requirements:

Agreement on one OPENID4VP to support multiple credential format (OIDC tokens, mdoc, VCs)

Q: should the response always be one credential, or could it be multiple credentials?

Q: should it be “bounded” or “unbounded” (not clear what that means, tbh - something about how expressive the query language is)

Q: should we support even more fine-grained selective disclosure, along the line of ZKPs?

Q: Should be easy to use for Verifier

Q: Predicative rp

Transcript via [Whisper Transcription](#):

[INAUDIBLE] components that come with the presentation.

And I would say one of the things-- if what you're saying is so, and Justin may join us later in the session, if he went through a previous session, then the request model around the protocol model called connect does exactly that.

In other words, it doesn't specify the state machine that might lead to an out-of-the-hand interaction in the case of issuance or in the case of verification.

But it starts off with this request of the authorization server that then results eventually in a verifiable credential or a token using issuing authorization or a token using issuing.

So yes, we do have a model of these pretty close to standard of how to do what you said.

Yeah, so that was kind of the background.

What we were hoping to talk about today is, presentation exchange, for better or worse, not trying to take anything on that, is kind of the developed query syntax of all these experiences, right, query language.

Thinking about, if you're familiar with like, bed-cm, but in a number of months.

(audience member laughs) Thinking about some of the other work streams that are significantly further along in terms of shipping and browsers, right, like bed-cm, which is designed to kind of enable the traditional federation model in a browser-mediated way.

How, what does a query language look like are things that are much more advanced, like requesting two different credentials from two different wallets without caring about the wallet or maybe you do care about the wallet.

So all of these different pieces that aren't in play with past keys and aren't in play with federation today.

They're just a much richer and more complex part.

So presentation exchange is super capable, but it's super complicated.

It's super hard to understand for a developer.

Not that web-off, and that's not simple either.

But maybe we can find something better in the middle.

I think there's a case to be made that more classic Federation use cases could do with some richness that they don't have today as well.

Daniel Fett and I have been talking for quite some time about building a richer expression language on top of OpenID Times request parameter.

I know he's not able to be here, but I know he's starting to think about trying to find a way that we can come up with a consistent expression language that could be used in this context in the context of OpenID Connect as well.

I think that would be super useful for it.

I make developers like that, I think, with the big finger.

- Definitely, you think you saw the slide here.

- What does it call it.

- Well, we're calling it Advanced Syntax for Claims in the OpenID Connect Community, but it's not really quite defined yet.

It's more about expressing quite complex constraints on the data that needs to be returned, which I think is broadly speaking what you're talking about too.

I think a useful thing to do as well is that we've got open ADK connects claim to press object, the advance syntax, we've got a couple of things that have been work partners in the credentials community group, we've got proposal on the mobile document request API and presentation exchange that at the very least for those interested in this topic we should try and collect as notes.

>> This reminds me of another one.

So I'm also part of a thing called the Google Interoperability Working Group and the Open Identity Exchange, which is coming at us from a kind of policy and user experience perspective.

And in the context of wallets with many, many credentials in, that community thinks that there needs to be a very rich way of expressing rules and passing them from one party to another to help the user pick the right credential.

It's much richer than type of credential or format credential.

It's down to specific features of the credential and how it is delivered, including some of the insurance processes that went on behind the casing activation.

Just to give a quick, so this is just to get back to the context.

This is the kind of [INAUDIBLE] where someone was asking for a document number 40 driving privileges in a very handout-specific manner.

And then what would the PD requests look like.

probably go to the presentation expense.

There's examples in there that do-- - What should I go to.

- Presentation exchange.

- Presentation exchange.

(audience member speaking off microphone) - Including one part in the other.

(audience member speaking off microphone) - Maybe we just want to go with some of these from both NPLs specifically, because it feels-- there's really good analogies for a very good application across all of these things, but not as well between inbox in open NPL or DB and precision exchange, for example, whereas this is likely becoming more from an NPL perspective.

So to compare, to have an equal comparison, then you could do a big one.

[INAUDIBLE] Just Google open ID for their conference.

Yeah, there's an Alex.

Yeah, and after that, I will show you a little bit of this.

Yeah.

[INAUDIBLE] (mumbling) - A three, on the right hand side you can scroll down.

[inaudible] [inaudible] [inaudible] [inaudible] [inaudible] [inaudible] [INAUDIBLE] More or less, yeah.

Yeah.

I mean, isn't this amazing.

Well, so-- Yeah.

One of the questions that I think, perhaps, we could pose to the group is, should the JavaScript API look like this.

And if so, I would like to hear from you all that you are satisfied by this, right.

Would you like to talk to somebody that you're happy with.

So it's a rather question, should it be that more, but also if not-- So this being open ID for BC.

No, but it should be a C-specific.

I think you're using many questions.

Is this a good enough starting place, because you can certainly make amendments to--
[INTERPOSING VOICES] I think there are two ways to integrate with first of all.

First of all, the example you gave is [INAUDIBLE] specific, the main difference.

I think the proposal you showed there could be also extended to be credentialled form a technology.

That's one that's one.

I would like to see how that's going to work for other credential formats.

I mean we only have an example for an end-up.

So that's one question, right.

If it is this really credential format or can it be used with different credential formats.

That's one question.

And then we would like to adopt that and there are some criticism with that approach.

But basically, it brought up where we are.

So it works, right.

Yeah, I think I think high level really if you take the two kind of efforts and for what they are.

Presentation exchange represents a highly expressive but also complex query language, right.

And the current state of the m.

request API is very limited but obviously simpler.

And so the question I think beyond reviewing syntaxes is actually to agree the requirements, right.

What query and scenarios do we actually want to support.

You know and and then how can we create an on-ramp where syntax for the simplest possible relying on requests are simple Keep it simple and simple, but you can graduate the syntax into Use cases that are sufficient to address the market or the requirements we've gone down on a guy Rather than like I know this is useful, but then it's also good to come back to those requirements, right.

Otherwise we're going to be chasing our tails In terms of integrating, I think perhaps if we had the requirements first, it would give us the evaluation tool to talk about the distinction between the two, right.

So perhaps just to start from where Apple and Google kind of proposed the browser API, at least as a baseline, perhaps, it's this realization that there aren't going to be more than one format to go into the future.

You know, we have certainly the nucleation for end box in these examples, partially because it's going to grow back whole.

But certainly, it should at least work with end box, let's say.

But also, it's very plausible, we believe, that color formats should also exist.

It's specifically very powerful for dentures.

I don't know if it's a hardware part, let's say, but ideally, we wouldn't have like 1,000 of our markets.

We would have like a handful of them.

It's more art design.

So let's say it could be proportional to the number of image formats on the web, perhaps.

Why is it relevant as a requirement.

I mean, if you're supporting two different formats, you already are prepared to accept three, two, four, five, six, seven, eight, and ten.

Not entirely, because if you have just a handful of formats, then you can hard-fold them.

You can go-hold them.

So for example, image formats.

But Web only has-- it's big, in the browsers, it takes JPEG, P, key, and when a new one becomes more.

It's not like you can put that on the whole browser and it will magically work.

It will roll up to the code.

So if you think of number of formats as something that is integratable, then you can hard-pull them.

If you think it's unbounded, then you have to make it fully accessible.

And that leads to different architectural forces.

I agree with that.

I mean, even if you're doing really hard bound, you can have extension points, further formats, right.

So the problem right now is-- So we're working on the assumption that it's only lasted-- in the future, it'll be purely a 10.

Yeah.

I think there's a question to ask, though, about the opacity or transparency of how much that needs to be well under structured ahead of time.

like how much in this or something coming down to it, experience in the prototyping you're doing in terms of how much interpretation, like what the native UI rendered by the browser is actually going to signal to the user in the credential selector, or wallet selector per se, right.

Is it gonna treat it relatively opaquely and just put that on.

Identifying the audience of the request, I guess, when you get a browser in the middle of it is, and how is that is pretty important as well.

- The policies have been, finally, the intuition is that a browser or an operating system would be able to tell that this is somewhat of a lightweight request for H-rating data, for example, versus-- - Why should the operating system know that this is a request for H-rating data.

Why should the operating system know that.

- So-- - The operating system should be able, I mean the operating system doesn't know what is really depicted in the picture.

The problem is that we need to be able to do it quite a lot.

But you can do it on the next meta level, right.

You need to know where you find the lines of the server.

I'm not hearing any of these changes.

Oh, yeah.

Sorry.

So, probably the goal is to be able to know enough of the faster booting.

and display a credential selector so they can use it to pick which one they want or use as a credential.

So a minimum of most of the things you need.

Anything else is sugar on top basically.

So maybe, what we're going to take, so what does the consent matter to give to actually give the college.

At the moment, if the professor is going to attend to a single wallet, then it's very easy.

When it attends the wallet, once the credentials have been picked, and the wallet can do whatever it needs to do, you actually exert consent on the user.

If you start talking about taking documents from off the once, then it sort of becomes open from the ex-con future.

How does the one-wheeler do that consent flow as now to the next one.

Have you taken a look at the platform and data privacy perspective.

There are terms like data control and there are obligations for some-- sorry.

Have you taken a look at the-- sorry.

I hope you accept my excuse.

So have you taken a look at the platform and data privacy perspective.

Because basically, what you're talking about content is bound to privacy, a war.

And if you're a data controller, for example, you're obliged to present a consent, for example.

So that might be a reason why, for example, the originating app displays the consent and does not indicate that to some other entity.

Just as a thought.

It's just popped up when you describe your idea.

So I was standing on the mobile icon, and I'm starting again.

[INAUDIBLE] And for a single result, it's very easy for us to have these examples.

Why we mount the node before something in the platform is if we want to dial up or dial down the new expression.

So if we get sites that are requesting a rigid mount information, we might put some extra or reserve the right to put some extra warning to mount some extra new expression.

At the moment we have no real plans to do that.

But it's at least being discussed.

The browser should be able to at least see the data and see what's being requested.

So it has the option of these to dial up the new actuation to meet at all times like introspection without really understanding what's going on.

Because in the end, it's really understretch, for example, the identity of a verifier.

You need to type into the trust framework of that verifier.

You need to understand how that verifier is going to be authenticated.

This is really complicated.

Why don't you just focus first on really understanding what's the nature of the request and what can be done.

That's what we have to do first.

We have to be focused on rooting against the right wallet and getting enough information to present it.

That's the only solution.

The other thing is just focus on the rider side, want to have this ability to at least reserve this right to put some new retraction in.

In a study site, we say that still we have to study input.

But it's sort of just-- we want to make sure we have the ability to do that.

So at least more than the users, there will be a certain set of sites who are asking for information.

And you can make sure that they're really giving away.

Because we don't really control the block.

We don't control the consent goes on and on and off.

And we don't know how to do it.

But we don't think they can do all the different systems that we want to do.

So one of those approach allows us to release a shot of something that stay from the same use of the data.

- Thank you.

- So I hope this is not a stupid question, but from the user experience perspective, this routing issue that we're talking about also includes either payment or stand protection, depending on how you wanna look at it.

So are we envisioning that the user is being asked for a payment authorization as well as information or that, so I'm just raising this issue because it's another aspect separate from just the data format or the data model for what's going on.

And can we decide that it has to be that payment is part of the, or a deposit or whatever you want to call it, it's part of the entire and the people that are black.

I don't know what he asked me that question.

I think it's too soon to tell.

Like the entire ecosystem has been secure at the moment, at least from my perspective.

I know that wallets specifically have wallets in the world.

They all are perceived as a container you put on anything hard as well as using instruments.

So it's plausible that we're going to this place right now.

But it's hard to say.

It's just too soon to tell.

I would perhaps start that question a little bit and you were a neat folks.

Do you expect being in history to be exchanged this way too.

Or where's that.

It has to be part of it.

- Well, after the case, the midtown deeper involves two separate relevance.

And so all the option that's the other you're involved in going to enrollment in the process.

I guess it's the law that we're serving.

- Oh, I-- I think that's sort of the role that we're going to live in a world with multiple wallets.

I think that's a huge challenge.

Maybe not each construction unit.

Yeah, thanks.

The thing that I also wanted to kind of call out here for the differing perspectives, at least what I understand in the Mobile Document Request API in terms of a team right now is, OpenID for VP is very much like the request is wallet centric, whereas I understand Mobile Document Request API is more credential centric, at least when the selective amount comes up, right.

So you can still have a multi-critical query, but to your point, Lee, that does have a lot of implications and massive trade-offs around how the UI is gonna be driven on that and when it comes up to wallet.

As you start getting into, depending on what scenarios you want to support in terms of complicated credential queries, what's going to be the consequence on that.

Like if I have a one-off and all sort of scenario for these credentials, like is the credential selector supposed to be telling me which applications can wholly satisfy it.

Yes, just for comparison then between the trusted domain with the I don't mean to say that in a very contrast kind of way in the sense that we certainly didn't spend a same amount of time to do that.

So I don't mean to say that the choice that we made was better than what we did.

But right now as it's written, it's a selector of just giving me one credential out of these many options.

To fulfill the entire request.

There's no provision for giving any, you know, two out of five.

So I give you a set of options and you have to basically pick one that you think satisfies one of the options as the response, right.

So many possible options for one credential, one credential in response that satisfies one of them.

So if I had to compare, I think we have a discussion that looks a little bit like the field descriptors.

- Simple descriptors with no submission requirements.
- It'll have one equivalent to submission requirements.
- Right, and you also have, just, sorry to tree onto that, any syntax, 'cause obviously you've got a request syntax, right, but as we were talking about in the Open-Open-ITB, the big session, as you

get more graduated queries and complexity, it becomes less and less clear how the queries will satisfy.

So, you know, the one of, sometimes, like, sometimes it's straight, like it's a doc type, right.

And the simplest possible query that's generated in the case, okay cool, they obviously gave me a driver's license rather than a PIMP ID card.

As soon as I get into groupings or anything like that, they don't have any way to relate the query syntax back to the query syntax.

Basically the verifier is just like-- In fact your original question is a question of requirements.

- Exactly, what requirements.

- If you're running that requirements so far with heavens ourselves, but maybe it's part of maturity in heavens, not fair enough on requirements.

- There's one good example in the ISO spec actually, ISO 180310-5, probably familiar.

there's the age over N claim that can be requested.

And there's this nearest, what do they call it.

Nearest age theory where they have defined basically like 10, 15, 20 different rules.

What claim you actually have in case you don't have the most accurate claim to reply.

And stuff like that, I think it can get really messy or complicated.

Then you would need something like what Tobias just mentioned, where you tell the verifier, the relying party, how the wallet intended to respond to the request, or satisfy the request.

So the comment of, I don't know what's going to be, but the way to test this parameter's value is also not present.

It's just whether the parameter is-- whether the attribute is a bit more-- If you go back to the example, then they would force the Wallace to have a parameter in m because that's where we started.

So I think we can agree that we are looking for something that supports multiple credential formats.

Yeah.

I think what's open still is whether this is bounded or unbounded.

And we should take note of that.

And I think we should-- Huh.

What does bound mean.

I mean, some introduced that term.

So I guess it means you need-- there is a fixed set of formats.

And you know how those look like and how The syntax for requesting credentials of what forms look like.

Unbound means you have something to do with the process.

I mean, PE is built.

Daniel, correct me if I'm wrong to work with any kind of form, and just out of the box because it's quite universal.

So this is an example of unbound.

Would you agree.

Yeah.

OK.

I would call PE an unbounded or uncountable Okay, whereas, you can see that it's all that you can count on.

Now, we're in.

Does that make sense.

Yeah.

[LAUGHTER] One unbalanced in terms of we might have new ones.

If we don't close it off, we'll never have our new one in the future.

I mean, I assume that we want to.

But we can see the marginal costs.

Yeah, but it's-- Can we pay a marginal cost every time you introduce a new product type.

And I think if you assume there will be tens of them, then you pay.

I think we would be happy.

Let me take it back to the reality of image formats.

Like in browsers, you only have a JTAG encoder, a BND encoder, a BND API, and a hand puller.

That's why I call it a puller.

That's fine.

That's fine.

And I think it's reasonable to come back with that, because in the end you also need to have the support for that puller in the wallet.

Right.

I mean that.

So-- Yeah.

Sorry.

I mean, we do not need to decide that.

I think it's important to write down that question at the post of prompts.

And I think just to let me just finalize what I heard while listening to that conversation, is that the next question is whether a request is always satisfied by single credentials.

Although, we will support multiple credentials, and what combinations from input descriptors-- or like, another term, input descriptors, and what's output.

But those are the things we need to talk about, you need to make the signals with them.

- What more requirements do they use as a selected exposure.

Having the ability to see the question specific parts of the connection.

- Yeah, so claims-based requests, right.

Not just kind of credential-based, you wouldn't be able to talk and introduce, not like roll-out groups and then they'd be the only kind of grouping.

I think the question, just to come back to the image formats, right, which is why it's important to consider, is like, a browser needs to know the image format needs to render the image.

Right.

Now that's because presupposing the browser's role and needing to understand it, right.

And I think the question is bound versus unbounding as well is because if it becomes inherently known very clearly to the browser, then to your point, browsers can add more support.

But the ecosystem is dependent on browsers all marching in unison to add those formats, right.

And you can create a reputation.

So there's pros and cons to weighing up that trade-off.

>> I've been in it since a lot of the security about the usability impact.

There's a difference between supporting multiple credentials generically or having them supported by, let's say, one wallet.

So it's a, choose what's actually coordinating the lease of pre-printing the pre-wall and it's a very different requirement than saying this wallet can actually exert this complex burden.

>> Yeah, I will always go back to the hello UI.

There's a lot of new brand new cards so no UI will be, Has anyone brought in to tell us that they have a selector of name, for example, where you can have your name come from multiple sources.

So you ask for just name and email address, profile picture, each one of these attributes come from multiple sources.

So far, that hasn't been quite the hard requirement that we can support.

>> I think you were.

>> Okay, sorry.

There was the question about attributes.

It's one of those.

I don't think you can capture that one yet.

And-- - One more question.

- Are we gonna be able to-- - Select the two, split.

- Yeah, select the two, split.

This goes into partribute, but I think that's where you come from, actually.

- Is that a good question.

- No, no, no.

(mumbles) - So then I had a whole one from that, which is, could we be able to do this minimization beyond the attribute level.

So for example, I'm putting a query which says, I only wish to have a credential return to me if the residential state is California.

Because that's all I care about.

I don't want to know any of the data if they're not in California.

So that's an expression over a certain constraint over certain claims by state.

(audience member speaking off mic) - That's the great constraint.

Don't respond to me if you can't say it's not as high a value.

- Actually, that wasn't quite where I was trying to go.

Sorry for that.

(audience laughing) Another one that I've dealt with is being able to do or apply a function to a client and convert it into a different data bank.

So that doesn't work with-- - Well, I was going to be seeing comments about period for start.

- Maybe the case, but if we can put it down as an aspirational requirement, it might prove useful if we can solve it.

So rather than say, don't return me anything, you might want to convert the attribute into a Boolean to say, tell me if my presented information is true or not.

you're returning information if it's true and you're not learning anything new at this cost.

So would an example of that be like address verification where the relying party sends in an address and says is this the address does the person have this address and they get back a true or false.

Well that they don't get any any crypto graphically.

Yeah that works in the federated by many more.

Potentially there are zero knowledge ways of doing that.

And I suggest to enhance the query language once those options come up.

It's a different story.

Yeah.

I think it's better to at least ask the question.

No, I'm not saying the question is developed, but I mean we have-- from my perspective, requirements are absolutely essential.

OK.

So maybe we should organize the ones that we think are controversial.

[INAUDIBLE] I'll share my thoughts just on another set of metrics, which is back to the question I tried to ask at the start.

I think which was, are we trying to write a query like which is exclusively for VC, or are we going to try and build something which is reusable across other group models.

Well, that's answered in the first.

That's credential format, so that's critical.

So specifically, this from my perspective has to work natively on the many NDLs and inboxes and critical combinations in the first essence.

But that doesn't mean we can't write a language which could be used for other things.

Why should we do that.

Because then it would be easier for developers to express the same requirements because they are critical.

And specifically that means you are more generic and more complex.

Does it turn off.

Yes, it turns off.

Yeah, we are discussing the requirements, right.

Sorry, what.

And I'm opposing against your requirement.

I think it's less than-- Sorry, what other problems do you have in mind.

What can I do to connect.

By the advanced syntax request, for example.

But we're not using-- artifacts return in OpenID Connect 4.

ID tokens are different from artifacts defined in the three-party issue of another hard model.

Why are we mixing up the two.

Because we could create a quiddity [Inaudible] >> Yeah.

[Inaudible] >> I'm coming at it from a beautiful creative language perspective.

>> Okay, then the point is do you want, do we want to have a query language that can be used for all things then query very top 10.

>> Well, very good including the original right here.

Just plan the person text is what we're asking for basically.

>> Yeah, I don't understand the question.

But what do-- I think he's referring to the transport portables.

What PE refers to as envelopes, transport envelopes.

So I think what the requirement-- I'm not good enough on PE to-- Yeah, I think you mean the envelope of agnosticism in the sense that if you send the bytes-- currently, if you send the bytes of this PE over whatever did come, it doesn't matter.

It all functions the same way.

It was designed that way so that it wouldn't be bound to one particular one or the other, because we already have multiples, and we'll probably have more.

So I think that's it.

[Inaudible] >> Like so if you imagine a world where a developer requests an identity credential, any credential could be an open identity, an entity took an example search into VC, MDL.

>> Whatever comes next.

>> Yes, like it might address the open ID account because people verify that the open ID connect with my MDL for a group of A's may come from an MDL.

Right, so is that, that's the line.

(audience member speaking off microphone) - Yeah, I don't agree either.

are different, different cross models behind those, right.

And because there are different architectures, cross models between those, you can do different things.

In the ideal building world, it's not a problem because you are creating those things on the fly.

So you can put in that thing whatever you want.

In a typical decentralized VC model, you have something in your wallet that you can't change.

You can reduce it.

Perhaps if you have sophisticated cryptography, you can do something on top of that with CKP.

But you're limited in what you can do.

But the question is whether we want to really cover all those different things and why.

I mean, OpenID Connect has a perfect language.

It works.

It's deployed.

- Torsten, I think he's just talking about, I don't think he's talking about the credential, modifying credentials, I think he's talking about sending it, just sending it over the wire in one-- I understand that, Daniel.

- I understand that.
- Absolutely.
- So what's the harm in that.
- He's talking about both.

He's talking about having the same thing for ID tokens and lowercase for a lot of credentials and also being able to use that over multiple protocols.

I think there are both things happening and I personally object to both.

- I think the biggest tension here really for this kind of claim for Sintex, right, is like an ID token is like a general payment conveyor of what a vehicle for user claims, right.

It can be used for that purpose.

Credentials typically start with some form of identification that creates the scope for what the claims are gonna be in there, right.

So, MDuC's have a doctype that sets the context of something as a driver's license, it sets the expectation about the claims that are gonna be inside it.

The VC also has a type and those sorts of things.

And that sort of tension, if you wanna kind of wrestle them into common requirements, you then have to build a query syntax where you're talking about different artifacts that can convey user claims that have things that aren't compatible in terms of like, there is no equivalent of like say a typing construct and something like an ID token to see it, what group of claims you might be out of it.

- Whereas really breaks is whether you, if you expect a wallet or whatever is the responder to transform something, it just doesn't work and then we see what does it work today.
- I think it perhaps, let me, it's trying to break, I think I have some empathy for this, but I heard the question that a higher level perhaps from a user experience perspective.

So let's say I'm a student, right, and I'm trying to access research publication, right.

Then I go to nature, nature is a paid thing, and I'm a student of Stanford and say, right, and then I think it would be a reasonable user experience to be presented with a choice of providing a sample assertion or a very common credential in my wallet.

What should I say.

Or an MDOT, what should I supply directly to the mobile.

- Sure, you can increase the scope and include SAML and you can do, I don't know, what was my DConnect, you can do other things, except right here is whether we need that.

Because basically, in the end, what you're doing, your language is going to be more, I mean, we talked about whether we need more than MDOT, We're talking about more than supporting anything that could contain identity.

I don't understand the question, but I know where we are.

>> Yeah, so I think it's important to really requirements then, because I think that's a possible use case.

Because I think in the academic application case, SAML was already there, it's a lot more changing for it.

In places like age verification, for example, there's a different assurance levels when bringing up an account on TikTok, for example.

And TikTok doesn't require necessarily global entities.

You could take Facebook's assessment on the age.

Would you assume that the agent's operating system would launch a SAML request to an IDP.

What service provider ID would that agent do, then, to obtain the SAML assertion.

I mean, I don't get it, because the three-party model has is a nice advantage that you have all the credentials in the wallet.

They are there.

You can just use them.

If you're gonna do open ID connect through that tunnel, you have to have a client ID.

First of all, determine what OP to reach out to.

And then you have a center request, and you need to have a client ID.

- And audience.

- We can go that way.

(audience member speaking off mic) - Can I make a quick point.

Just that I think that one of the things versus getting out here is that there are multiple questions that are probably operating in multiple layers here.

And so there's this notion of what the period language is for making requests, what formats are for getting responses.

Those might be intertwined in some way, which is the bounded-unbounded problem, because I need to know kind of what I'm asking for.

But there's also the carrier protocols.

So all of this could fit in a variety of different identity and on identity related to hearing calls and listening to some possible harm.

There's ways to wrap this stuff inside of like, it'd be a terrible idea though, when I need to connect links, you can grant this query language inside that other query language and call it an image.

Don't do that, but it is possible.

There are people that are looking to do stuff like this, not exactly the same thing, but on top of connect, and so to find sort of a new request space to put a query language like this in order to get back subject information that's in all of this other stuff.

You could do it.

You could wrap this entire thing in a sample.

I don't know what the claim would be, but I'm sure there is one where you could throw that and send a sample request and get these documents and send it back in your sample description.

So the important thing here is that the-- for work like this to be successful, you have to draw very bright lines as to what your boundaries are, and how do you cross that kind of times.

- The other thing that I've just observed, right, which is an alternative, because I think that to manage complexity here, right, we want to try and limit the amount of options so that the HFS is implementable by verifies and those sorts of things, right, exposing all these options to them is gonna mean that the query, like for your example, I'm just picturing the query that that would be in terms of expressing the, as a relying party, codifying the policy that I have in terms of what I expect to get back from you in order to tick this box and move through the flow.

It gets increasingly complicated, so we do have an incentive to try and keep this somewhat simple, to keep something simple.

And to talk about an alternative way that like SAML or an OpenID Connect provider or something like that, they can simply, Like you can route to a wallet and then a wallet can then onward

federate, log in to do user authentication, get those attributes in the form of a credential, and then present that back as well.

And that produces, I guess, the amount of stuff that has to flow through immediately and the explosion of possibilities, I guess, that you could pipe through this API.

And that might be a trade-off, right.

So wallets do that coalesce And I guess to a form that is understandable by the browser in an acceptable subset of formats to manage complexity, I think we have to-- So that's what purpose is in the option.

- I guess it's a little bit confused.

So I'm not sure I agree with you in the sense of reducing complexity for the verifier because based on previous conversations.

Before lunch, right.

And Torsten's point just a minute ago, If there's a date in a verifiable credential, it's stuck in the wallet in a particular format, in a particular syntax, right.

And I, the verifier, if I want to allow for date of birth, I'm going to have to know the 50 ways of credential formats or whatever else it can be encoded in, regardless of how I ask for the question.

So the complexity for the verifier has just shot up.

There's just no way that we can say that the verifier has the simple solution, unless we can actually coalesce on one or two credential formats and reviews by everything.

- I think that's what I was trying to say.

Maybe there are-- Okay, okay, so I missed that.

- No, yeah, 'cause I was trying to advocate that instead of simple identity assertions and those sorts of things, you color less narrower than that.

But the relationship, those federation protocols can still have things that a wallet does when you route the request.

- You're starting to do that.

- The other thing that's in the branch is doing different types of interstitions.

I'm not sure that's asking the wallet to go get a value in particular credential format so it's easy for the verifier.

It feels like it defeats a lot of the purpose of what I want to accomplish.

But you think it's important to solve that problem.

Hold on, I want to point out that I cut off Tim earlier and then we totally start crying.

I don't know if I had to start.

I do really want to ask you, I think that's a really important requirement to come back on.

So this, and I think we've talked about this briefly, Sam.

A lot of these credentials, if we have a user experience that presupposes that a user has done and set up their wallet and got all the credentials that they need before they need them with Reliant Party interactions, and that is the only model we look to, then I think we're destined for some really, really bad adoption issues with users, right.

We need to be able to support a model where a user may have downloaded an application or pre-configured it.

Maybe the fact that it supports credentials is secondary to what it is.

It's a consumer channel app with a government or something like that.

It can also store a credential.

And I get this credential selector UI that comes up with my driver's license and it dawns on the user, but there's some way to complete this flow with this app I've got installed on my phone.

And I click on that and that bounces me out and I do user authentication.

I get a credential, I present that to the relying party.

byproduct is I now have a credential in my wallet app but it's just in time right and I think that's really important I just wanted to pull that out.

Well, for me the requirement here is that it should be optimized for simplicity for the verify.

Sure, great.

Can I ask one thing.

In existing Openit events, under a live party, can I just simply send them to the cluster.

In this organization server, I get a back end entry.

I can't, I need to pre-register.

as we're like party, there's a different trust model, depending on the product, based on the core or SAML or, you know, the product measures, again, really different model, depending on which of my main scheme is being used.

So, I understand the desire, user perspective, but there's certain things VeriCorps have to deal with.

Sure.

I mean, stuff changes, right, in the sense of what you have to do.

But at the end of the day, right, if the complexity that the verifier has to implement in order to try and work with a large swath of populations, right, that's really complex, right.

They're not going to do it.

The value of the model is not there for the verifier to cause them to change from what they've got to something new.

We have to show substantial value for the consumer in order to do that.

And privacy or simplicity may or may not be enough to overcome the cost to the verifier.

I think the existing federative model can tell you emerging diesel plus its own value, why are we smashing it together.

And trying to figure out the value of something smashed.

- So let me reflect on that please.

I mean, the question is whether you accept certain properties of the new model.

Right.

I haven't understood yet how you would like to solve the problem you see.

I agree with you.

It's a problem, right.

As I pointed out, if there are 50 ways to express a name in a credential, then the verify needs to know those 50 ways.

For me, that's just a fact.

And we can work on that, and we can try to reduce the number of formats.

And that's just happening in the course of the evolution.

The question is whether we, in the short term, find a solution to make the life easier for the verifier, while accepting the technical properties of the technical solution that we are facing right now.

And one of the facts-- and that's why I raised that topic when Mark came up with that transformation thing-- The wallet can't just transform something and give you a cryptographically protected insertion.

If you don't accept that, you need to use a different model.

You know, which is why I was trying to spin my requirement around simplicity of implementation for the verify.

We should think about this.

Absolutely.

I bought into that.

[INAUDIBLE] [Inaudible] >> The more we can do to not ride mad, the quicker we will get to large scale adoption.

[Inaudible] That's interesting.

How do we get to a point where we have like a certain five credits for the master.

It's sort of an ecosystem problem.

We can either solve it by naturally buying options and just see what wins out.

Or we can force it and we can kill it by literally only supporting certain types.

But then do our.

We rattle off some of the problems.

Isomorphic validation, client should be able to serve, should be able to run the same thing they say.

Identity in the Fediverse

Session Convener: Johannes Ernst

Session Notes Taker(s):

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

FediForum – Fediverse unconference <https://fediforum.org/>

Fediverse Developer Network initiated at the first FediForum: <https://fedidevs.org>

There's a related FEP: <https://codeberg.org/fediverse/fep/issues/34>

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

Motivating use case:

- I browse my Mastodon feed and see an event posted on Mobilizon
- I click on the event in Mastodon
- Problem 1: the RSVP to the event, I have to create a new account on Mobilizon – lots of friction
- Problem 2: the organizer of the event now has my new Mobilizon account identifier, cannot tell that it was me who registered (and in this particular example, that's important)

Wide-ranging discussion. First time that such a discussion took place anywhere to the best of our knowledge. Some disagreement on what the right tech stack would be to address those:

- DID etc
- OpenID etc
- Simple things like rel=me can help all without “identity” code

GOAL: Maybe you need a Fediverse developer network – where information can be found about how to build interoperable software;

WHAT?

1. Ambassadors from each project
2. Best practices
3. Where you can find information Activity Pub
4. It should be a full stack thing

For example:

Q: I want to interoperate with Mastodon, what should I do? Right now it takes a couple of days of hard research to get started. In decentralized Activity Pub, there are silos of code

Q: Is it just Fediverse? What is Fediverse vs. Activity Pub

- Mastodon & everything that can exchange with Mastodon

Q: IDENTITY & FEDIVERSE (Gabe) –

Mobilizon (Eventbrite-like); he posted it in Mastodon; Johannes saw the event in Mastodon, and wanted to RSVP. But he had to log in, create a Mobilizon account, and Gabe got an RSVP from an account he didn't recognize.

- Fediverse has a network effect, where Identity doesn't
- Most people in the Fediverse don't realize there is an identity angle

QUESTION:

What is the best proposal for Identity People to work with Fediverse?

- Use DIDs

Recently 2 Microsoft engineers got on to Mastodon – are they from Microsoft? How do we prove this?

- Is this attributable to a “person” or “Self”
- Is this attributable to your company?

META VIEW:

We come up with the perfect solution, now where do we go?

- WC3 Social Webs group
- FEP Codeberg Repo Informal Fediverse community:
<https://codeberg.org/fediverse/fep/issues/34> (Identity Proofs)
- Fediverse Development Network
- Fedidevs.org

WHICH PROBLEM TO SOLVE?

- How do you incentivize adoption?
- How do you create identity for Mastodon or Activity Pub

Expanding Language - Humans Think - Chatbots Process - How does that augment or disrupt communication intentions

Session Convener: Jeff Orgel

Session Notes Taker(s): Jeff Orgel

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

Humans Think (Part 1) - Chatbots Process (Part 2)

Part 1

When we think of getting advice, or we are in a discovery mode looking to gain knowledge, people have benefitted from each other's experiences. Whether written or spoken, we mine recorded

thoughts and ideas which are direct legacy of another person or other persons. Over years the vast input of this sort of information and knowledge has seeded the landscape of the digital realm. Now new conduits to large data sets have emerged which we may now query and learn from. Different types of communication style and different focal priorities often are often called for regarding different audiences and beneficiaries.

This writing focuses on illustrating foundational differences as to a) how information is gained and b) how information is conveyed regarding two frameworks - human communication and sharing of knowledge relative to Chatbot communication and sharing of knowledge.

Human nature (aka Human Operating System) applies knowledge made of a combination of direct lived experience, non-lived experience which includes story, mentoring and formal education. Human nuance and intuition guide our application of context and best approach to conveying that information in differing circumstances.

Chatbot systems leverage Artificial Intelligence (AI) and Machine Learning (ML) to work from data sets collected in a framework based on the design and use case of the chatbot system. Those data sets are then queried by parameter defined by the search/query terms imparted to the system via chat. The bot then delivers "advice" or calculative results which will provide the inquirer, human or otherwise, with information.

When is a chatbot, generally devoid of human nuance and context, preferred over information exchanged in human-to-human trade in thought and ideas.

Does the non-emotional chatbot interaction serve best in crisis? Is the lack of emotional entanglement of a chatbot in this sort of situation a strength. One may expect a calming factor if emotion is not flowing from both sides of an interaction. Is this akin to the emotional expression of a patient receiving an analytical response from a therapist. Conversely, one may expect an elevated emotional interaction with a close friend or family member.

As alignment training enables more pseudo-emotion in chatbot responses will there be a time where we reach out to systems rather than our personal community of advisors? If our desire for guidance includes deeply embarrassing and secret aspects we would rather not expose to our community at any level? Can the chatbot dry/non-emotional response and its lack of direct human linkage to known community bridge that gap in comfort allowing for release of the issue into that dry realm of consideration?

Another aspect to this comfort is related to whether, and if so where, is the query logged or captured within the chatbot's system. Is the "conversation" an ephemeral, instance which vanishes, unrecorded at the close of the interaction? If logged or recorded somehow, who or what may enable wanted or unwanted correlations between the person inquiring and the detail of inquiry?

To demonstrate the difference and comparison to my communication above, I have included a ChatGPT response to this contemplation, for review. The query was phrased to elicit a general summary of difference between natural human processes (thinking) compared to responses

originating in informational systems structured by humans. It is a first blush single response with no further refinement query and follows directly as Part 2.

Part 2

compare human intelligence, a naturally formed system, with artificial intelligence which is a human designed system

Human Intelligence and Artificial Intelligence are two distinct types of intelligence that have their own unique characteristics and capabilities. Here's a comparison between the two:

1. Origin:

- Human Intelligence: It is a naturally formed system, a product of millions of years of evolution. It is an inherent part of human biology and is influenced by genetic and environmental factors.
- Artificial Intelligence: It is a human-designed system, created through computer programming and algorithms. It is a product of human ingenuity and technological advancements.

2. Learning:

- Human Intelligence: Humans learn through experience, observation, and interaction with the environment. They can generalize knowledge and apply it to new situations. Human learning is often guided by emotions, intuition, and social context.
- Artificial Intelligence: AI systems learn through data processing and pattern recognition. They can be trained using supervised, unsupervised, or reinforcement learning methods. AI learning is typically more focused and task-specific, lacking the emotional and intuitive aspects of human learning.

3. Adaptability:

- Human Intelligence: Humans are highly adaptable and can adjust to new situations, environments, and challenges. They can think creatively and solve problems using a variety of strategies.
- Artificial Intelligence: AI systems can be adaptable within the scope of their programming and training data. However, they may struggle with tasks outside their specific domain or when faced with novel situations.

4. Generalization:

- Human Intelligence: Humans possess general intelligence, allowing them to perform a wide range of tasks and adapt to new situations. They can transfer knowledge and skills from one domain to another.
- Artificial Intelligence: Most AI systems are designed for specific tasks and have narrow intelligence. They may excel in their specific domain but struggle with tasks outside their expertise.

General AI, which can perform any intellectual task a human can do, is still a goal for AI researchers.

5. Emotional Intelligence:

- Human Intelligence: Humans have emotional intelligence, which allows them to understand, express, and manage emotions. This plays a crucial role in social interactions, empathy, and decision-making.
- Artificial Intelligence: AI systems generally lack emotional intelligence. While some AI systems can recognize and respond to human emotions, they do not experience emotions themselves.

6. Ethical Considerations:

- Human Intelligence: Humans possess moral and ethical values that guide their actions and decision-making. These values are shaped by culture, upbringing, and personal experiences.
- Artificial Intelligence: AI systems do not inherently possess ethical values. However, they can be programmed to follow ethical guidelines or principles defined by humans. Ensuring ethical AI behavior is an ongoing challenge and area of research.

In summary, human intelligence is a naturally formed, adaptable, and emotionally driven system, while artificial intelligence is a human-designed, data-driven system with specific capabilities. Both types of intelligence have their strengths and limitations, and their integration can lead to powerful synergies and advancements in various fields.

Interoperable Trust Registries with DID-Linked Resources

Session Convener: Alex Tweeddale (cheqd), Andor Kesselman (Benri)

Session Notes Taker(s): Alex Tweeddale

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

Agenda:

1. Introduction To Trust Registries
 1. [Glossary](#)
2. Collaboration between DIF and ToIP
 1. [Trust Establishment Spec](#)
 1. Credential Trust Establishment
 2. Trust Registry Protocol of ToIP
 1. [Requirement Collection Phase!](#)
3. [cheqd Presentation:](#)
4. Other efforts
 1. CIRA
 2. TRAIN
 3. DIAAC
 4. [AAMVA mDL](#)

TL;Dr

Notes from conversations:

- Concern about simplicity of scope
- TTL with DIF spec's request
- Mike Egbert mentioned the effort around interop profile alignment
- Multi-level signing was a concern that was addressed
- URI resources? DNS?
- There is an issue with Trust Management in SSI in that existing approaches tend to sway towards centralized infrastructure
- Even the EU is moving back towards X.509 because no compelling solution exists using more decentralized infrastructure
- What results from this is many of the same issues from traditional/legacy ID management systems
- If we want to make systems less clunky, we should not repeat the same mistakes. Issues include:
 - Link rot
 - Downtime
 - Centralization
- DID-Linked Resources (DLRs) are a new proposed approach to handling digital resources, using patterns from DID core
- One type of digital resource which could be utilised via DLRs is trust registries

- This would create a far more interoperable way of referencing, retrieving and dereferencing to trust registries in their entirety, and importantly, individual trust registry entries
- The session also highlighted other existing trust registry models that we should align with
 - TRAIN
 - EBSI
 - GLEIF
 - BC Gov
 - CIRA
- Ongoing work on this topic lives at
 - ToIP Trust Registry Task Force
 - DIF Trust Establishment WG

Protecting Identity With WebAuthn

Session Convener: Matthew Miller

Session Notes Taker(s): Nick Steele

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

- [Matt's Headroom | Encrypting Data in the Browser Using WebAuthn](#)

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

- The first 10 minutes or so we went over how the PRF extension can be used in practice, using his blog as a reference
- PRF allows for encryption on top of a webauthn credential upon assertion
- What group are interested in this? 1Password and other credential managers can use PRF to remove the need for passwords at login.
- PRF extension in the past was a request from IIW members. Provides a lot of local application uses (wallets, electron apps, etc)
- PRF allows for enveloping a symmetric key, we discussed account recovery using this
 - We could use threshold keys with PRF keys and enveloping to help with credential/account recovery

Introduction (and roasting) to the DCDR Framework (Data-Centric Digital Rights)

Session Convener: Jean F. Queralt

Session Notes Taker(s): Jean F. Queralt

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

This session focused on presenting a Data-Centric Digital Rights Framework to the audience and obtaining feedback to fine-tune it.

The DCDR Framework attempts to:

- Answer the question: How do I ascertain that my code does NOT harm people or their data (digital twins)?
- Further the statement: Developers are the NextGen Rights Defenders

The exchange provided

- A diagram/tool to differentiate Human Rights and Data-Centric Digital Rights
 - The conclusion was that the defining line was “Who receives the harm?”
 - If a physical entity (source entity) then it’s a Human Rights consideration
 - if the digital entity (representational entity / digital twin) then it’s a DCDR consideration
- A review on the lifecycle of physical entities
- A review on the parallelism needed (“twin-ness”) so that a digital twin may carry its meaning
- An introduction to the necessary and related taxonomies of the DCDR Framework:
 - Digital Harms
 - Digital Rights
 - Data Use Cases

McNamee Inspired Method to Crowd Source Congressional Policy and for Managing Politicians?

Session Convener: Britt Blaser & Phil Windley

Session Notes Taker(s): Britt Blaser

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

Slide deck: [A McNamee Method for Managing Politicians](#), takeaways:

The only 3 conditions that cause a Member of Congress to listen.

The simple definition of democracy.

Letting go of Learned Helplessness: Committee-Based Activism

21st Century Voters' Virtual Congressional district strategy

Verified constituents' aggregated policy sentiment analysis

GEOvoter API jurisdiction picker
NewGov.US demonstration: 51,231 jurisdictions mapped
Committee constituent out-of-band ID verification by USPS

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

Roger McNamee wants to End Surveillance Capitalism, but discovered that DC politicians don't care that he's a prominent tech investor and expert who warned about social media in his book, Zucked: Waking Up to the Facebook Catastrophe.

John Doerr, lead Google investor with his firm Kleiner, Perkins Mayfield, and Byers has been called a 'Master of the universe', but felt so helpless about Climate change legislation that he ended his 2007 TED Talk in tears.

They share the frustrations of 245 [Patriotic Millionaires](#), who haven't succeeded in convincing the Congress to increase taxes on themselves and the rest of America's richest 1%.

Session Catalyst: Phil Windley, 2017:

Verifying Constituency: A Sovrin Use Case:

"Suppose that I had four [verified claims](#) in my [Sovrin agent](#):

1. Address Claim—A claim that I live at a certain address, issued by someone that we can trust to not lie about this (e.g. my bank, utility company, or a third party address verification service).
2. Constituency Claim—A claim written by the [NewGov Foundation](#) or some other trusted third party, based on the Address Claim, that I'm a constituent of Congressional District 3.
3. Voter Claim—A claim that says I'm a registered voter. Ideally this would be written by the State of Utah Election Office, but might need to be done by someone like NewGov based on voter rolls for now.
4. Twitter Claim—A claim that proves I own a particular Twitter handle. Again, this would ideally be written by Twitter, but could be the work of a third party for now.

"Given these claims, Sovrin can be used to create a proof that @windley belongs to a verified voter in Congressional District 3. More generally, the proof shows a given social media account belongs to a constituent who lives in a specific political jurisdiction."

Why verified constituency matters:

Every Congressional representative is concerned about the very few constituents who vote in Primary elections.

They do want to support the policy sentiments of a majority of verified constituents and may therefore support a provision added to bill in a Congressional committee hearing, because primary voters aren't so interested in actual policies.

SESSION #4

NIST SP 800-63.4 Digital Identity Guidelines

Session Convener: Justin

Session Notes Taker(s): Nick Steele & Dipti Shiralkar

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

- Public comments period done
- Base: overview
- 63 A: identity proofing
- 63 B : Authentication
 - Separate authenticator verification from attribute verification
 - mobile wallets
 - single / multi factor software authenticators
 - what is authenticator
 - password is an authenticator
 - sheet with look up code
 - yubikey
 - biometric are not authenticator onto themselves but used to unlock to one of the authenticators
 - google authenticator
 - holder binding
 - anything that you can use as some type of proof of credential
- 63 C : Federation (Justin maintains this one)

Goes in flow

- 63A: first figure out who person is and create account
- 63B: bind authenticator to account
- 63C: progress this known authentication

Decentralized identity model : not in plan

Big difference between version:

- Trust framework, federation : trust agreement -> first step to start
- attribute disclosure and provisioning: pre provisioning of attributes (SCIM) : takes care of privacy risk
- draw Assurance level for federation (FAL)
 - FAL1: dynamic proxying, classic federation
 - FAL2: established trust agreement can not be dynamic, injection protection
 - FAL3: present bound authenticator along with assertion
- System need to account for: multiple user, multiple IDPs, multiple RPs

- Recovery process: we will see a shift. We do not want, what supposed to be recovery as login process.

Assurance level:

- proofing: IAL
- Authentication: AAL
- federation: FAL

Comment: Is direct mapping between the ALs possible? It would be helpful if NIST adds some details around.

Stephen Baur - How do VCs play into 63C v4, can they? I've submitted comments on this
 Justin - I will read them

Changes to Assurance levels in 800

In 60A we have

IAL - Identity Assurance Level

AAL - Authenticator Assurance Level

Federation Assurance Level

- Level 1 of FAL: Based on a lot of work from previous FAL work, was assertion driven rather than process driven, refactored to support process. Refactored to support the “new user to a terminal flow”. Can cover dynamic proxy models of trust.
- Level 2 of FAL: The establishment of the trust agreement cannot be dynamic, i.e. an IDP and an RP are specifically established to trust each other. Protects against golden SAML and adds injection protection
- FAL3: has bound authenticators with assertions, i.e. present CAC in IDP/SSO and take it to RP with assertion. Expanding on what is possible through a bound authenticator.

Q- Where is the RP in this model?

A - Depends on what you're looking at! In:

Proofing - the subscriber / CSP (credential service provider)

Authentication - verifier

Federation - the relying application

When the verifier and the RP are separate from one another we can use a protocol for the two and are tightly bound.

- If it's FAL2 and above, there's a strongly bound agreement (more verifiable) between the RP and the IDP.

Post Enrollment Authenticator Binding would be something used for an authenticator like MDL. Fits into the proofing and authentication assurance frameworks.

63A Rev4 Introduced IAL0 with 0 identity proofing, in v3 IAL1 was 0 proofing, now requires two pieces of identity material for proofing. This seems heavy handed

A IAL1 used to handle *lightly* verifiable attributes or something that might require no verification. In this revision, we un-bucket these two groups. It also allowed us to make IAL2 stronger.

- Q Should we consider the case where a biometric factor must be used to unlock an authenticator, is that considered multifactor?

- A: Yes! that is MF

- Important to note that section B is on Authentication, not *Authenticator*. It is dictating a process.

Q: This person has trouble using computer / help translation. How to handle.

Check sections:

- Trusted referee: identity proof trusted referee , so you know who that is.
- Applicant representative

Q which volume contains details for external attribute and sources

Volume C

All credential factors, something you have/know/are, can be boiled down to something you can access

You talk about *dynamic proxies*, how many of those proxies (etc, IDP, RP, etc) can be used?

A - You can have multiple hops, but they inherit the FAL of the weakest proxies.

PIV discussion, can see what a FAL proxy looks like at [max.gov](#)

FIDO Basics

Session Convener: John Bradley

Session Notes Taker(s): Nicole Roy

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

What is FIDO?

WebAuthN

two-party model where you have a verifier (relying party), browser, and an authenticator (built-in to computer, phone, security key, etc.)

Wireless protocol called “hybrid” which lets you do things like use an authenticator on a phone to authenticate on a desktop computer.

Number of transports- USB, Bluetooth, Hybrid, and NFC

Trust-on-first-use model

Register at the website - sends a message to make a credential, gets back a public key and identifier. After that, authentication is done by signing challenge responses.

Added multi-factor authentication in FIDO v2.0 - require a pin to unlock a biometric, for example.

There are both user presence flags and user verification flags

As the RP, you always check that the audience is your RP ID, and that the user presence flag is sent, and that the challenge you sent is in the client data you received. Missing user presence flag is always a sign of something bad going on.

What do I as the deployer have to do in order to have a passwordless experience for the user? Do account binding via nonce link to email or something. Validate their email.

Vittorio says they don't do the email validation thing for platforms that support token sync, because you can recover account on that platform, and they don't want to introduce a phishable option for account recovery. There is no cut-and-dried answer because of this.

One of the new things that was introduced as part of Apple's passkeys announcement was multi-device passkeys. Apple, Google, MS are happily willing to take care of the synchronization / recovery problem for you.

There are single-device credentials where the key is stored in hardware on the device (been around for 4 years now)

Replicated / multi-device credentials enable easier account recovery for RPs.

Devil is in the details. Buy a device, need to recover Facebook access. Facebook doesn't know how to do it, there is no way to know where your passkeys are being kept. Identifier is a GUID, but there is no URL, no clear entrypoint for starting the recovery. There are optimizations that need to be done to enable this. Being worked on.

As a relying party, I'm very interested in holding the user accountable, so I prefer to have a biometric used on a device. How do I reduce the friction of registering a new user but require them to use a biometric on the device versus a USB token, say.

(insert discussion about account protection and privacy here)

Device attestation during make credential. Some authenticators will give you that information. Currently none of the authenticators that support multi-device authentication will tell you who they are.

May be, in the future, a way to specify whether you as an RP trust or don't trust various types of multi-device authenticators.

If you support device attestation, you can't have less than 100,000 keys per batch, for anonymity.

Syncing right now:

Apple,

Sort-of Google,

No Microsoft,

but there is Dashlane - working on an interchange format so you can move your passkeys from one password manager to another.

Attestation would be hard to do for synced devices, because the attestation certs were per-device. Dirk Belfast would love to collect your feedback, he is preparing a report for the FIDO board on sync provider attestation/user anonymity/etc.

Problem: You can air-drop passkeys from one apple device to another, even one not owned by you.

FIDO does have a biometric certification/evaluation program, so that the market has something to benchmark.

The backed-up/replicated authenticators are all not FIDO-certified today, because the replication method are out of scope.

May be a privacy problem with doing attestations on replicated keys. Can't do batch attestations in a homologous pool. Answer is you do cloud-based attestations using a PKIX scheme or something.

Selective Disclosure with SD-JWTs 101

Session Convener: Kristina Yasuda, Brian Campbell
Session Notes Taker(s): [Ankur Banerjee](#)

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

- [IETF Standards Tracker for SD-JWTs](#)
- [SD-JWT Standard](#) (version 04, latest at time of this session)
- [General explanation of JWTs vs JSON-LD Linked Data Proofs](#)

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

- Normally, JSON Web Tokens (JWTs - pronounced as “jots”) are a machine-readable way of structuring data along with signatures to prove that the data has not been tampered with. (See [JWT.io](#) for a general, non-credential example of a JWT.)
- JWT credentials typically contain one or more data fields, with one signature, which means that when a holder presents/reveals the credential, it’s an all-or-nothing situation.
- The idea with SD-JWTs is the holders:
 - Can provide individual hashes/proofs for one or more credential values/attributes
 - When the holder wants to reveal only one field, or a subset of a field, they first check if the issued credential has an available standalone format/field, or subset available.
- Can they be encrypted?
 - Yes, this could be applied on top (as is the standard with encrypted JWTs)
 - Typically in a credential context, JWT credentials are not encrypted since they *do* need to be plaintext so that they are readable/parseable.
 - The security/tamper-proofness comes from the signature/hashes.
- What’s the purpose of the hashes inline?
 - Salt protects the replay attack where the hash can be recreated
 - Hashes inline allow specific bits to be disclosed
- How are the disclosures separated?
 - Separated by the ~ character
- Is there a difference in complexity between the flat vs nested models?
 - Not really, since user’s don’t need to know the different levels of nesting
 - Processing nested credentials isn’t a problem for software itself
- Is there any tooling/libraries that makes using SD-JWTs simple?
 - Will be shared after the session, still early days
 - Examples/implementations exist in multiple languages
- How do you do holder binding/prevent replay attacks?
 - Uses a holder-binding JWT
 - *How does this differ from a VC issued to a did:key credential subject?*
 - This is a food-for-thought/opinionated take on how to achieve this without Verifiable Credentials
 - A holder-binding-JWT is more standard, and achieves the same thing

- Embedding a Verifiable Credential bound to a **credentialSubject** and then creating a Verifiable Presentation is more niche way of doing the same thing
- Other notes
 - Inherent explicit linkability by colluding verifiers
 - Opportunities for implicit linkability/leakage also exist
 - Revocation with privacy is out of scope
- Unique Selling Points vs JSON-LD with BBS+ or AnonCreds
 - Simpler to understand (in a good way)
 - By choosing more standard cryptography / signatures, these can be executed in hardware, such as Trusted Execution Environments (TEEs) rather than entirely in software. This could be a considered a pro for better security/privacy than other formats that can't use TEEs.
 - Tooling/software is more widespread than those other formats (in a good way).

Decentralized Identity Foundation (DIF) Update

Session Convener: Clare Nelson, Executive Director of DIF

Session Notes Taker(s): Many

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

Decentralized Identity Foundation (DIF), Self Sovereign Identity, Decentralized Identifiers (DIDs), DIDComm, Sidetree, Decentralized Web Node (DWN), DIF is a Linux Foundation Project

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

DIF mission: DIF exists 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 an **engineering-driven organization** focused on developing the foundational elements necessary to establish an open ecosystem for decentralized identity and ensure interop between all participants

DIF Mission

DIF exists 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.

Our Focus

DIF is an engineering-driven organization focused on developing the foundational elements necessary to establish an open ecosystem for decentralized identity and ensure interop between all participants.



Images: www.flaticon.com



Working at DIF - Open Specifications and Open Source Software

Part of the Linux Foundation

DIF is a 501(c)(6) nonprofit organization that serves its members. DIF is also a Linux Foundation Project, and advocates for open standards and open source software.



How we protect intellectual property

Specifications created in DIF Working Groups are protected under W3C Patent Policy and software reference implementations are protected under Apache License 2.0.



W3C Patent Policy



APACHE LICENSE, VERSION 2.0

<https://www.w3.org/Consortium/Patent-Policy/>
<https://www.apache.org/licenses/LICENSE-2.0>



Decentralized Identity

Gartner

"Decentralized identity is important for confirming user identities and securely storing them. It offers numerous advantages separate of the greater identity autonomy it delivers to customers."¹

Deloitte.



"Individuals can own and manage their own tamper-proof credentials for applications such as personal health, education, and voting records in an encrypted digital wallet on their personal devices."²

accenture

"Utilizing DID improves the capabilities of anomaly detection systems. It will be easy to blend these systems with the existing ones to strengthen prevention processes and enhance privacy. The additional layer of security that DID will offer without compromising consumer privacy is invaluable."³

Forbes

"...passkeys do not protect our *privacy* or give us complete control of our online identities. For that to happen, we need to look at self-sovereign identity (SSI)."⁵

¹Source: Gartner, <https://www.gartner.com/reviews/market/decentralized-identity-solutions>

²Source: Deloitte, <https://www2.deloitte.com/us/en/insights/focus/tech-trends/2023/trustless-blockchain-decentralized-internet.html>

³Source: Wipro, <https://www.wipro.com/innovation/improve-detection-of-online-frauds-using-decentralized-identity-management/>

⁴Source: Accenture, https://www.accenture.com/_acnmedia/PDF-173/Accenture-Decentralize-Digital-Identity.pdf

⁵Source: Forbes, <https://www.forbes.com/sites/forbestechcouncil/2022/09/26/self-sovereign-identity-taking-control-over-your-digital-identity/?sh=6918b35364e0>



Myths

Our work is done

- W3C Recommendations for DIDs and VCs

Reality

- We are just beginning



Three events at ETHDenver 2023 (March 1, 2023)

1. WalletCon
2. ETHDenver Climate Summit, panel, *How Decentralized Identity Will Change the Climate Accountability Conversation*
3. did:day – Half-day event focused on DIDs

DID = Decentralized Identifier

VC = Verifiable Credential

W3C = World Wide Web Consortium

Source: <https://blog.spruceid.com/announcing-did-day-an-exploration-of-decentralized-identity-at-ethdenver-buildweek/>



Decentralized Identity

Liminal's 2023 Digital Identity Landscape™



Source: <https://liminal.co/2023-digital-identity-landscape/>

6



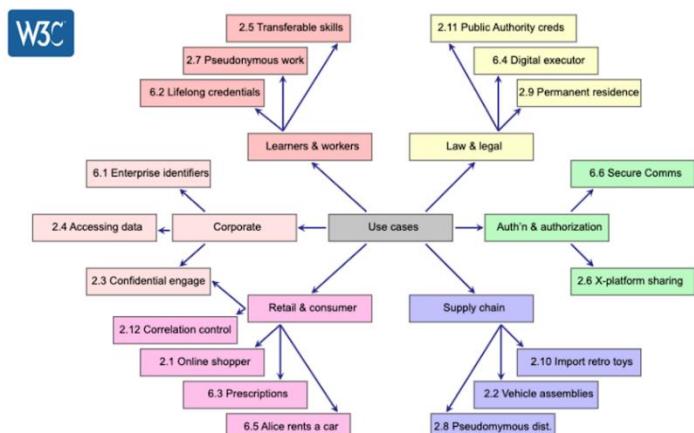
DIF develops specifications for key web standards with myriad use cases

Use Cases and Requirements for Decentralized Identifiers

W3C Working Group Note 17 March 2021

Essential characteristics of Decentralised Identifiers (DIDs)

- Decentralized:** there should be no central issuing agency
- Persistent:** the identifier should be inherently persistent, not requiring the continued operation of an underlying organization
- Cryptographically verifiable:** it should be possible to prove control of the identifier cryptographically
- Resolvable:** it should be possible to discover metadata about the identifier



<https://www.w3.org/TR/did-use-cases/>



DIF collaborates with our Liaison Partners to build the ecosystem



DIF working groups



Claims and
Credentials
Secure Data Storage

*V2 of Presentation Exchange recently ratified
Working towards v2 of Wallet Rendering
Data agreement developing consent receipts*



DIDComm

*DIDComm is at v2
Discussion of creating a training, course or DIDComm
orientated playground*



Applied Cryptography

*BBS recently updated the IRTF draft which is based on
the DIF draft, presented at the IETF meeting in March*



Identifiers and
Discovery
Wallet Security

*Discussion of rotating and revoking keys in DID
documents and how that relates to VC issuance and
verification*



DID authentication

*Work on Universal Wallet Backup Containers
Looking to engage wallet vendors in a forum on
common problems in backup and recovery*



*Aiming to do a version 1.1 to fix bugs and clarify
specification text
In the ideation process of V2*

*OIDC4VP and OIDC4VC
(This work is being undertaken in OpenID)*

Terms

IRTF = Internet Research Task Force (long term focus)
IETF = Internet Engineering Task Force (shorter term, engineering and standards)
BBS, BBS Signature Scheme, comes from the authors: Boneh, Boyen and Shacham

DWN = Decentralized Web Nodes, check out the AMA (March 2, 2023) by Daniel Buchner here: <https://www.youtube.com/watch?v=MNxowKcB73E>

Terms

OIDC4VP = OpenID Connect for VP, Verifiable Presentation
OIDC4VC = OpenID Connect for Verifiable Credentials



DIF contributions

01	DIDComm 2.0	<ul style="list-style-type: none">Secure, private, transport-agnostic communication built atop the decentralized design of DIDs
02	Sidetree	<ul style="list-style-type: none">A blockchain-agnostic protocol enabling public, permissionless, decentralized DID overlay networks, including ION
03	Universal Resolver	<ul style="list-style-type: none">Resolves DIDs across many different DID methods, based on W3C DID Core 1.0 and DID Resolution specifications
04	Presentation Exchange V2.0	<ul style="list-style-type: none">A set of data formats Verifiers can use to articulate proof requirements and Holders can use to describe proofs
05	Verifier Universal Interface	<ul style="list-style-type: none">A set of APIs to enable Identity Wallet and Verifier interoperability



Why should you join DIF?

DIF members include enterprise software-as-a-service providers, industrial and electronics manufacturers, decentralized identity solution vendors, startups and developers.

By supporting and participating in the open standards and open source software community, members gain familiarity with the open specifications and reference implementations developed by DIF, facilitating incorporation of these elements into their business.



Research and Development
Work with the leading experts in decentralized identity to influence the standards and drive your roadmap.



Cooperation and Intel
Leverage a neutral space with Intellectual Property Rights protection to solve common challenges



Professional Development
Opportunities to contribute to an important new technology and raise your profile

Images: www.thenounproject.com



Energy + Mines Digital Trust B2B/G2B From Pilot to Production / Kyle Robinson (Bc Gov)

Session Convener: Kyle Robinson

Session Notes Taker(s): None

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

Presentation including video demo of TSM transactions: https://briartech-my.sharepoint.com/:p/g/personal/kyle_robinson_briartech_ca/EZ31drOpkg9OgUlfpUnlvIBeYpBTnsry-0PF3NViMWXJQ?e=tLgV1Q

Executive Summary report on lessons learned during Pilot:

https://briartech-my.sharepoint.com/:b/g/personal/kyle_robinson_briartech_ca/EcUTxd3wRotFp7v9gytLZaQBnbavQK4ZAupWGTTvqxJ2tw?e=BhbicJ

Direct link to TSM demo video: [TSM Credential Exchange MAR 31 23.mp4 - Google Drive](#)

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

Type You Notes Here

DWeb Camp

Session Convener: Doc Searls

Session Notes Taker(s): Wendy Hanamura & others

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

<https://dwebcamp.org/>

<https://getdweb.net>

Discount Code for 25% off: "FriendsAndFamily"

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

QUESTION: How can the DWeb Community support & create synergy with the decentralized identity community? What are our shared goals & needs?

Doc: "in some ways it's IIW only outdoors"

DWeb Camp, June 21-25 is organized in part by the Internet Archive.
The spirit is very similar to IIW – the goals are very much in alignment with identity.

IIW: user-centric identity started IIW

Bengo: has gone 2019, 2022 – was a Space Steward;
I was in Chile, and came back to the Bay Area just to go to DWeb Camp 2019. It was the perfect intersection of things I like about IIW and beyond.
In 2019 I went to lightning Talks and learned a lot. I spoke about Activity Pub.

It's a collection of communities: they overlap a lot

Thematic sort of way: SSI is emerging (DIDs & Wallets) – cross fertilization

Would digital culture & history fit in? YES! Retro technology

It's holistic & wholesome

There's yoga, movement, meditation —> then moved to DAOs

Bengo: a lot of times the conversations are more P2P, open source, different tech cultures; that's what I hope to cross pollinate with IIW – more DIDs standards; more open source tech;

JOYCE: gets beyond the crap; younger entry level people are looking for how to bootstrap; I found it to be very interesting that artists were there; now artists are tying into DAOs and NFTs and governance. next generations of creators are using contemporary

Programming Challenge: how do you do the LARP without sacrificing

LIMARI – DIF – Joachim Lohkamp invited her to come; I'm a community person; signed up to be a Weaver – enjoys; wants community and learning; the more communities I intersect with, the better I can do my job at DIF; at IIW I connected with so many people – it's remarkable how quickly I came to know people;

Michael Grossman: come out of magazines & design; founded a platform called Factor – gathering, organizing, sharing information; Collaborative Technology Alliance – to interoperate; coop of coops;

HAROLD CARR: works at Oracle Labs; privacy & accountability; also a musician;

Andre Kudra of ESATUS – Berlin based; IT security and SSI space; creating technology and adoption; digital culture, IT, history theme; underground digital culture – demoscene; UNESCO – recognized digital culture; how to preserve?*****

DWeb Camp – is about 90% open source

Brian Behlendorf – father of Apache, also DJs

Should DWeb move to Open Space? (**Open Space Technology is a meeting methodology started by Harrison Owen over 30yrs ago**)

- church of open space really works
- I don't know if there is middle ground
- Navigation was hard – have a wall
- If you walk to Cathedral grove it takes 30 minutes RT
- Law of two feet is hard at Camp
- My Data – is a hybrid event; $\frac{2}{3}$ scheduled and $\frac{1}{3}$ Open Space;
- I think hybrid is better than either all Open Space or all Scheduled;
- JOYCE: I think the Open Space methodology with the wall is really useful; have some scheduled on teh wall, and some open;
- There's a lot of value in no planning
- Governance: there was too much one to many – didactic teaching; would benefit from conversations;
- PHIL: at IIW: minimal curated experiences; what are you trying to achieve? If you are trying to get people understand your agenda, then curation works; based on your goals,

Governance and Accountability of Decentralised Identity and Verifiable Credentials

Session Convener: Scott Perry

Session Notes Taker(s): Scott Perry

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

resource: <https://trustoverip.org/our-work/deliverables/>

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

Slide Deck

Web 3.0 Architectural Trust Solution



Copyright © 2023 ISACA. All rights reserved.



Here are some of the contents introduced in the session:

Templates, Specifications, and Companion Guides

- [**Governance Architecture Specification V1.0 \(PDF\)**](#)
This is the core specification for the interoperability requirements for ToIP-compliant governance frameworks. (Note that it references the Governance Metamodel Specification as a subset; see below.)
- [**Governance Metamodel Specification V1.0 \(PDF\)**](#) and [**Companion Guide V1.0 \(PDF\)**](#)
A subset of the ToIP Governance Architecture Specification, this specifies the required, recommended, and optional components of a ToIP-compliant governance framework document set.
- [**Risk Assessment Worksheet Template V1.0 \(Excel\)**](#) and [**Companion Guide \(RACG\) V1.0 \(PDF\)**](#)
A guided template to help complete a ToIP recommended Risk Assessment in advance of a governance framework construction.
- [**Trust Criteria Matrix Template V1.0 \(Excel\)**](#) and [**Companion Guide V1.0 \(PDF\)**](#)
A container to organize and operationalize the accountability of governance framework mandates.
- [**Trust Assurance and Certification Controlled Document Template V1.0 \(PDF\)**](#) and [**Companion Guide V1.0 \(PDF\)**](#)
A starter shell for the production of a ToIP-approved trust assurance framework.
- [**Governance Framework Matrix V1.0 \(Excel\)**](#) and [**Companion Guide V1.0 \(PDF\)**](#)
A structure to evaluate, define and operationalize governance objectives, structure, process, and incentives for ToIP solutions.

THE TRUST OVER IP STACK MODEL



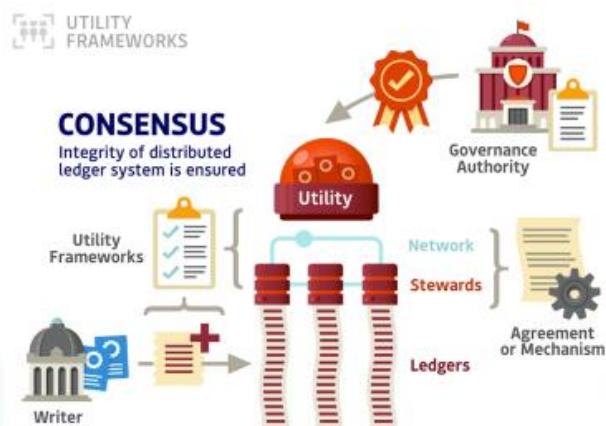
The New Architecture for Internet Trust



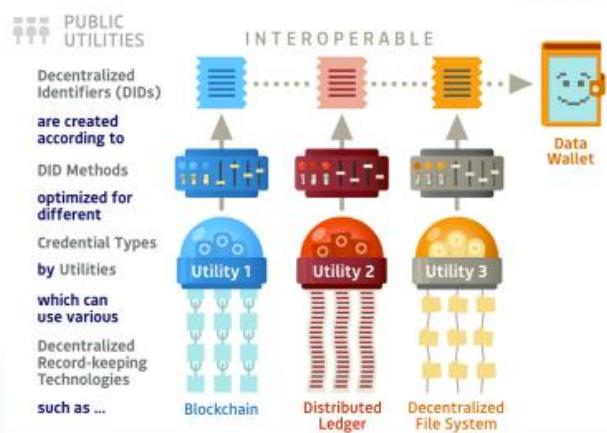
LAYER ONE – PUBLIC UTILITY



Governance



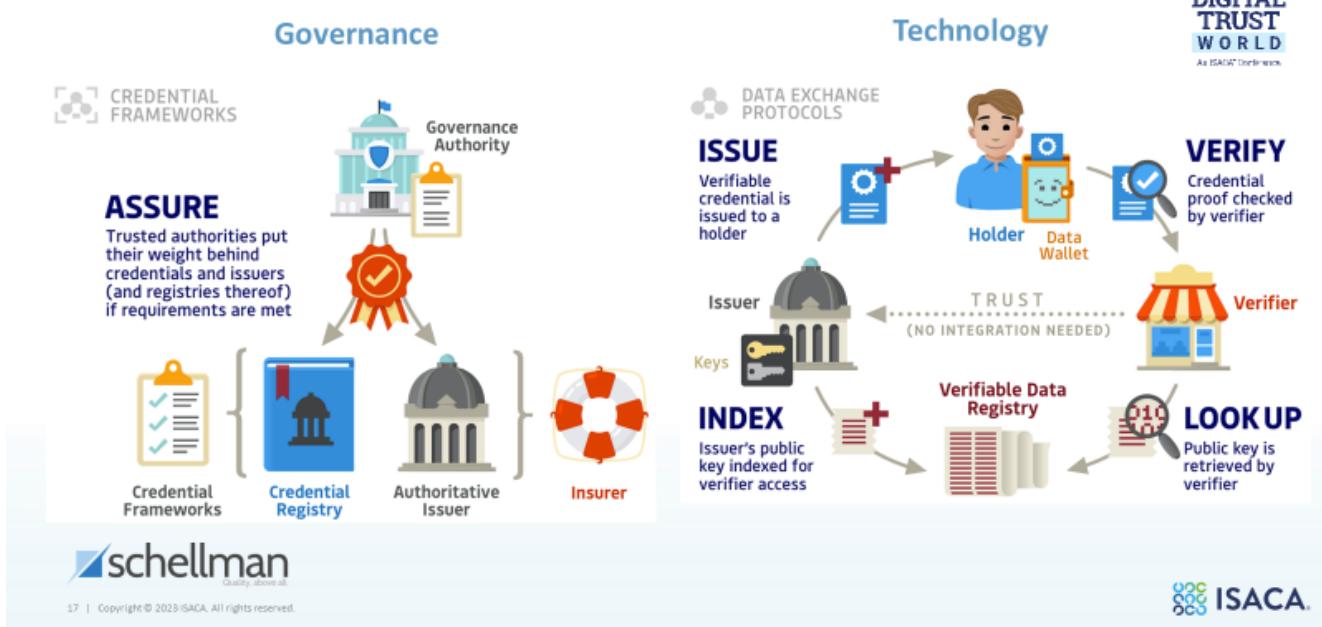
Technology



LAYER TWO – AGENT / PEER TO PEER



LAYER THREE – DATA / CREDENTIAL EXCHANGE



LAYER FOUR – APPLICATION / ECOSYSTEM



18 | Copyright © 2023 ISACA. All rights reserved.

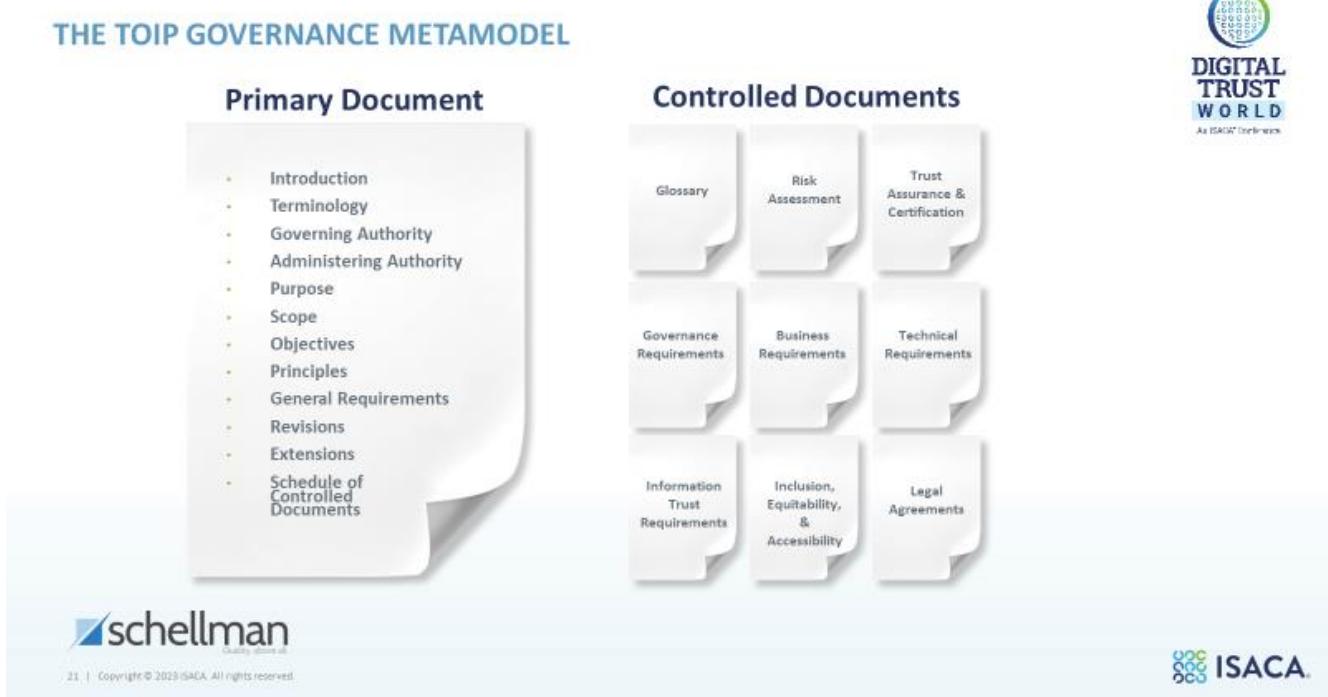


Web 3.0 Governance and Accreditation

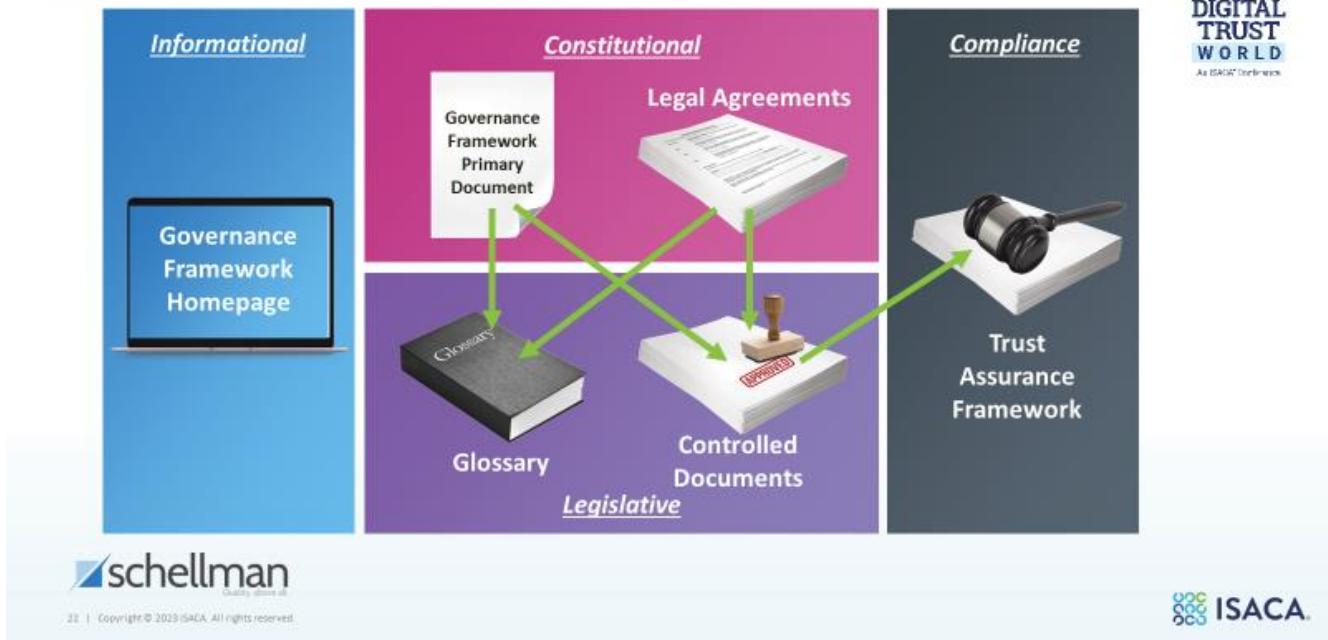


19 | Copyright © 2023 ISACA. All rights reserved.

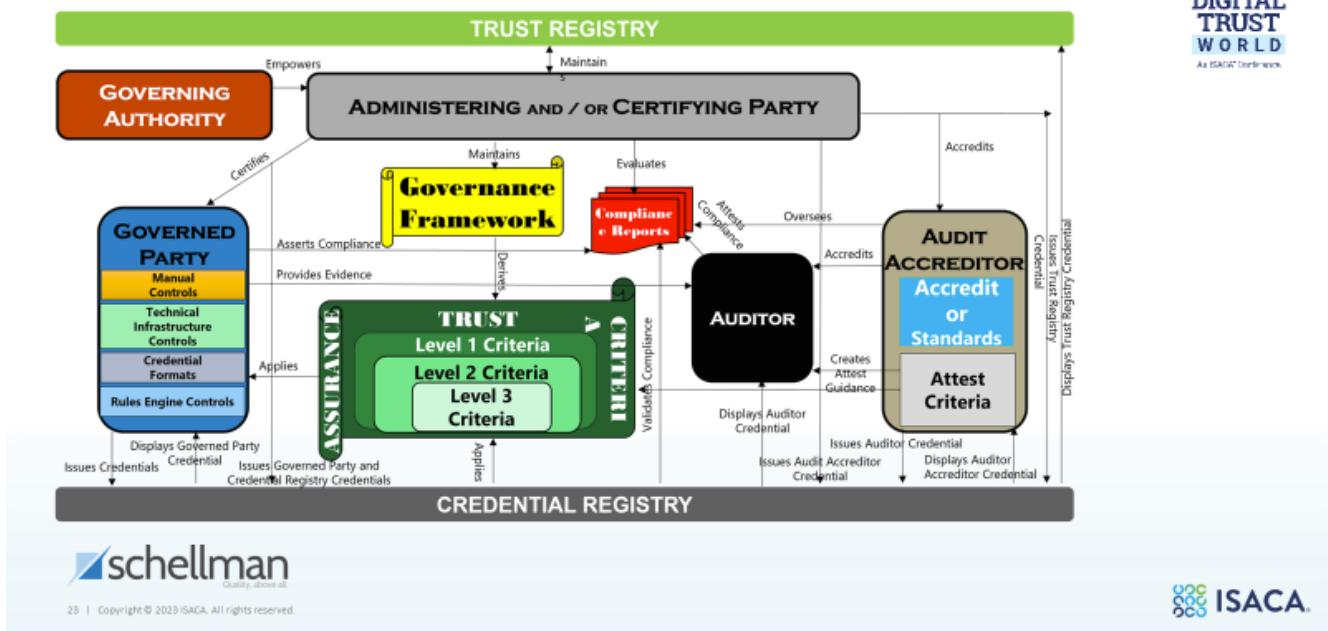




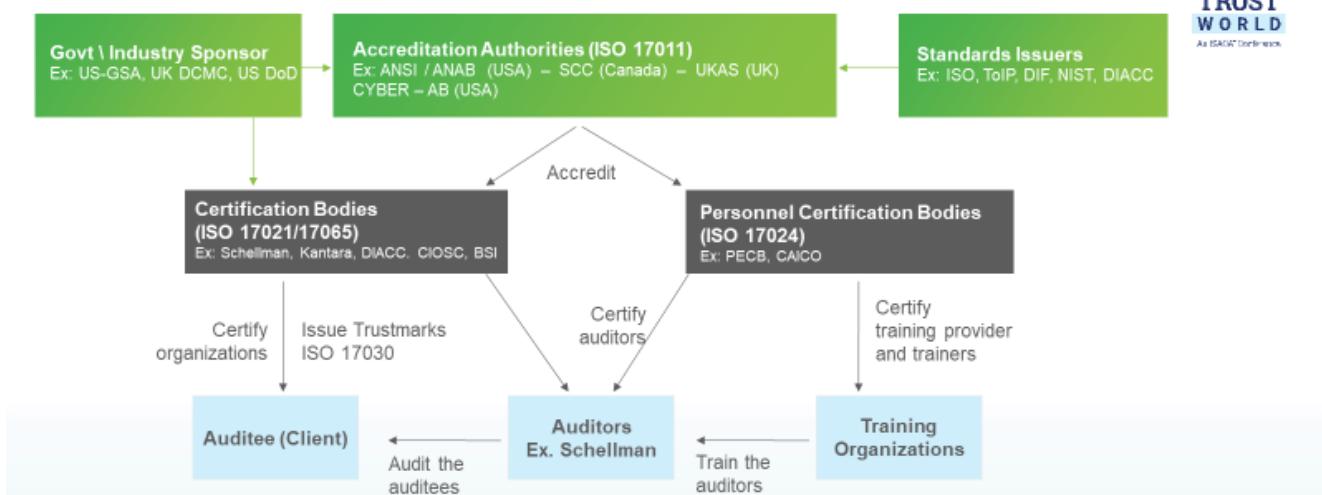
RELATIONSHIP OF GOVERNANCE DOCUMENTS



THE TRUST ASSURANCE ECOSYSTEM



ACCREDITATION / CERTIFICATION SCHEME



24 | Copyright © 2023 ISACA. All rights reserved.



Auditing Web 3.0 Ecosystems



25 | Copyright © 2023 ISACA. All rights reserved.



SELECTED DIGITAL IDENTITY SCHEMES

	US	UK	Canada
Sponsor	US-General Services Administration Federal Acquisition Service Technology Transformation Service	UK Ministry of Digital, Culture, Media and Sport	DIACC Membership - Government and Industry Consortium
Trust Criteria	NIST 800-63	GPG 45, GPG 44 UK Digital Identity and Attributes Trust Framework (DIATF)	Pan-Canadian Trust Framework
Accreditation Body		UKAS	SCC
Certification Body	Kantara Initiative	Kantara Initiative UK	DIACC (under VVP)
Auditor	Schellman	Schellman	Schellman
Trustmark/Certificate	Trustmark	Certificate	Trustmark



26 | Copyright © 2023 ISACA. All rights reserved.



CERTIFICATION / AUDIT PROCESS

1. Design and Build and Implement the Identity Service
2. Read Classes of Approval, Service Approval Handbook
3. Establish Levels of Assurance
4. Submit Initial Application
5. Be Assessed and Address Findings
6. Submit Approval Package
7. Evaluation and Decision
8. Certificate / Trustmark Issuance

- 
1. Engage an Assessor
 2. Submit Compliance Assertions
 3. Create Assessment Plan
 4. Kickoff Assessment
 5. Submit Evidence
 6. Demonstrate Processes
 7. Evaluate Conformity
 8. Report on Conformity
 9. Address Non-Conformities



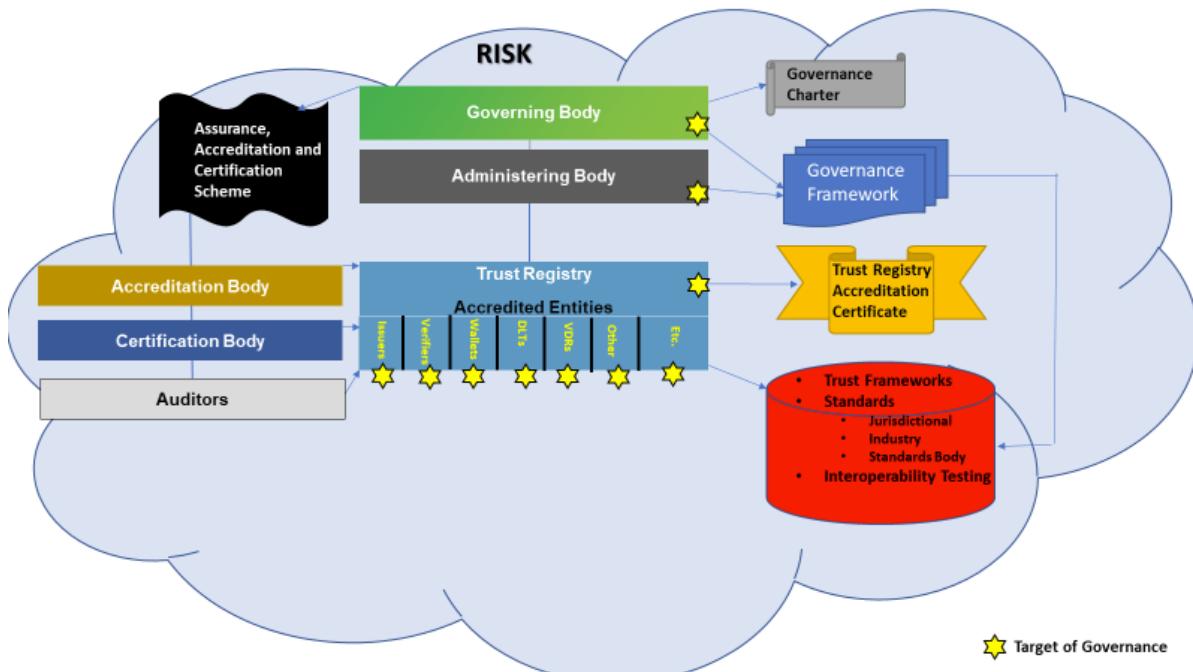
27 | Copyright © 2023 ISACA. All rights reserved.



Two main risks:

1. Control over the private key
2. Validation of the payload of a credential

Suggested new ToIP new model for governance:



Anonymous Reputation - What's the State of the Art?

Session Convener: James M

Session Notes Taker(s): James M & others

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

Johannes' Autonomous Reputation System

<https://reb00ted.org/tech/20220810-autonomous-reputation-system/>

(others listed in the notes)

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

The question: what is the state of the art in anonymous reputation?

Framing the question...

Given a certain set of trusted connections Alice has, how can she impute a reputation for Bob based on their *mutual* connections?

Different levels of reputation:

- Proof of human
- Something about this person
- Who is this specific individual

What about discovery?

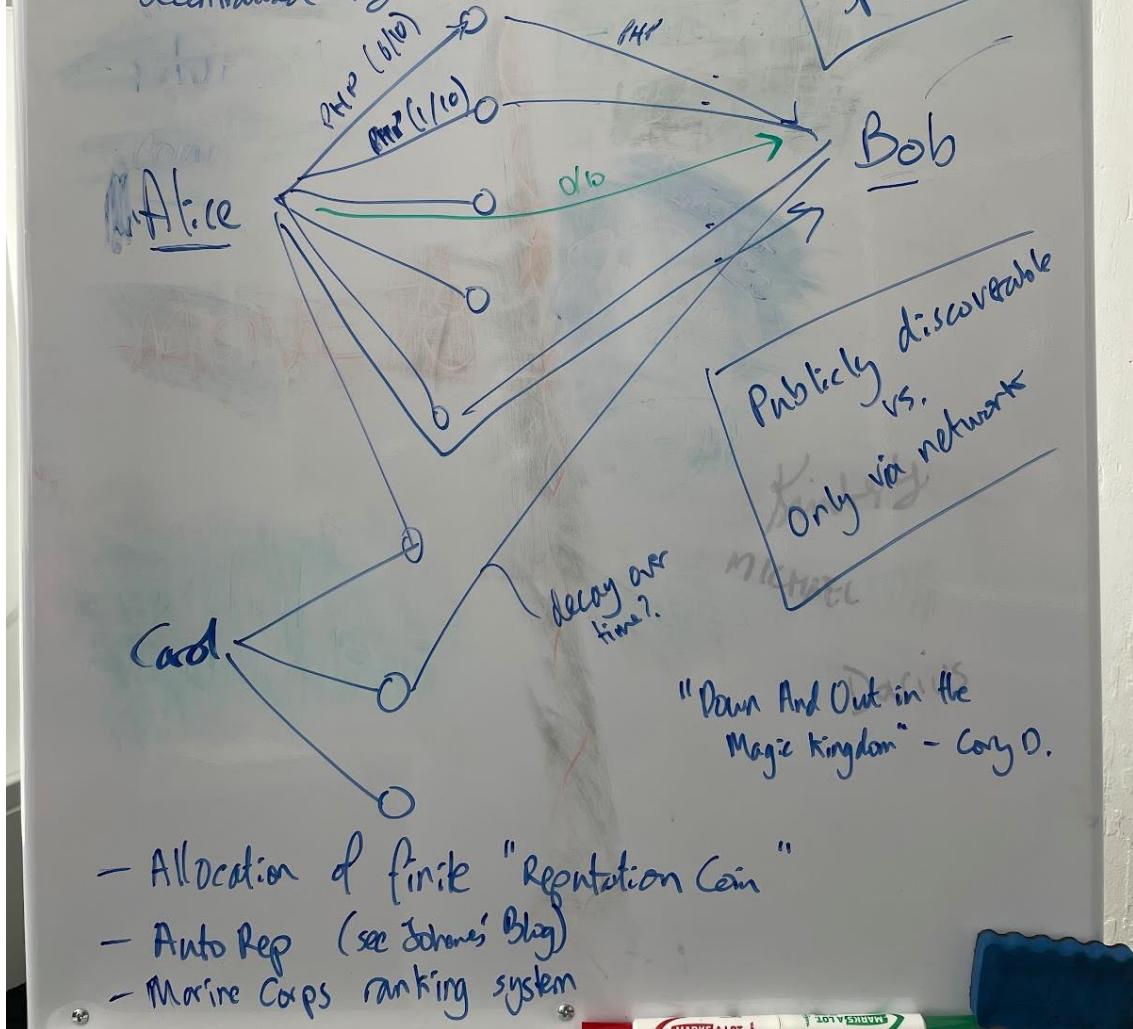
- Publicly discoverable
- Only via my immediate network

Projects / approaches the group is aware of or thinks might work:

- Reputation associated with a DID (pseudonymous)
- BrightID (blockchain-based system)
- VCs in a wallet, public presentation in a directory, list of trusted issuers
- Network of agents gossiping reputation proofs between themselves
- Decentralised PageRank
- Allocation of a finite amount of “ReputationCoin”
- AutoRep
- Marine Corps reputation system
- Cory D wrote a book about it “Down and Out in the Magic Kingdom”
- A network which computes reputation scores but discards the inputs, like an L2 ZK rollup does... Alice can prove to the network who her connections are, and the network will offer an introduction to Bob via one of their mutual connections, without anyone inspecting the network being able to figure out what the graph looks like
- The app at EndorserSearch.com allows two users to correlate their shared contacts using an intermediate server (though the server cannot read the contact data).

(see photo below)

- Reputation associated with a DID (pseudonymous)
- Bright ID
- VC's in a wallet, public presentation,
list of trusted issuers
- Network of agents gossiping proof
- Decentralized PageRank?



- Allocation of finite "Reputation Coin"
- Auto Rep (see John's Blog)
- Marine Corps ranking system

<https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.hqmc.marines.mil/Portals/138/DRM-2012-U-001003-Final.pdf&ved=2ahUKEwjp55viwbT-AhUjI0QIHVSrBtEQFnoECBQQAQ&usg=A0vVaw3okFT8xxkbDLwapqB47vFG>

Link to review of Marines fitness Report system.

Enhancing Your Participation in Tech-Related Public Consultations & UN Digital Compact seeking Feedback Session

Session Convener: Kaliya & Jean Queralt
Session Notes Taker(s): Joshua Coffey,

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

- **Context**

- Jean (John) and Kaliya met at RightsCon in 2019 (a digital rights fiesta) and saw one another as two people who were thinking about protocols and technical aspects of all this digital rights conversation
- There seems to be an increasing frequency of entities at multiple levels of governance/governments seeking input on multiple things (NIST guidelines, whatever)
- One that came across our radar that we thought we would like to put together an IIW community response to that may have an impact (that we don't fully understand) is the UN Global Digital Compact, which they recently published.
- Would like to brainstorm as a community about how we as identity people feel about the 9 different
- The UN Digital Compact is basically the general document guiding the UN moving forward as to how they will interpret/act on technology
 - Not that many technologists are actually aware of this
 - All the feedback given so far has largely been from civic society organizations who don't know much about actual technological aspects
- This is only one case — the EU, many other governments are constantly requesting feedback on many things and we are not responding to them
- “Only 5-7% of people at the IGF have any technical background” and we need to make ourselves more involved

- **Key Issues of UN Digital Compact**

- Connect all people to the internet, including all schools
- Avoid internet fragmentation
- Protect data
- Apply human rights online
- Introduce accountability criteria for discrimination and misleading content
- Promote regulation of artificial intelligence
- Digital commons as a global public good

“Good ID...” Is it time for a new framework?

Session Convener: Ethan V ID2020

Session Notes Taker(s):

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

No Notes Submitted

Next Version of Sovereign Identity: Sovereign Individual System

Session Convener: Ying Liu

Session Notes Taker(s): Ying Liu

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

Slides: <https://github.com/sichat-io/Research-and-Design/blob/main/doc/SIS%20IIW%2036.pdf>

Introducing Wikido, A Massively Multiplayer Joint Venture

Session Convener: Bry Benson

Session Notes Taker(s): Jonny Stryder

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

<https://wikido.super.site/>

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

We discussed the purpose and governance elements of Wikido, and compared and contrasted with various cooperative ventures (e.g., Mondragon, Obran Cooperative, Zebras Unite Coop, Quorum 1, and Holo Sourcing.)

Parallel elements of the Wikido JV and other cooperatives include merit-based equity and provisions for direct democracy. Unique aspects of the Wikido agreements and organization include individually determined social obligations and principles for conflict resolution, and a well-defined process for mutual conciliation.

SESSION #5

SPAC = Secure Privacy Authenticity Confidentiality - Tradespace Strongest A+C+P

Session Convener: Sam Smith

Session Notes Taker(s): ??

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

Sam Smith's SPAC whitepaper

https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/SPAC_Message.md

Slides from Presentations:

https://github.com/SmithSamuelM/Papers/blob/master/presentations/SPAC_Overview.web.pdf

ToIP Design Goals / Practical Elaborations

Authenticity and Authenticity: means non-repudiation

Confidential and Confidentiality: usually done by encryption vis-a-vis the intended parties

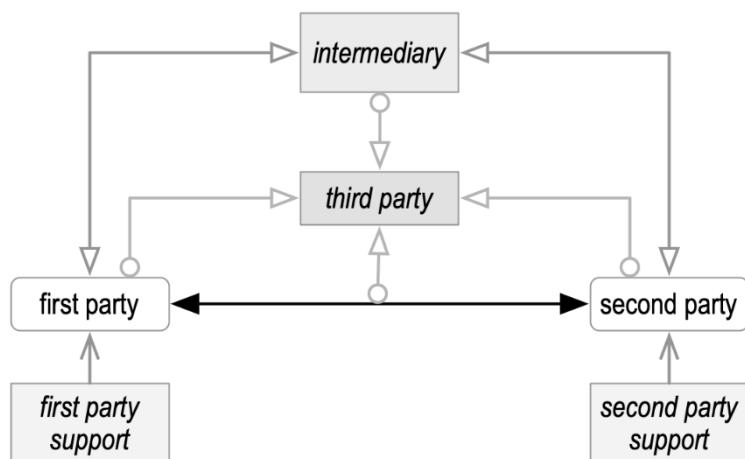
Private and Privacy: this is the hard problem

Privacy and Confidentiality

There are two fundamentally different but complementary definitions of privacy that are relevant to protocol design - The terms confidential and private also have distinct legal definitions:

Privacy Protection as Protect from Exploitation - We define privacy protection as protection against the exploitation correlatable identifiers (metadata)

Three Party Exploitation Model



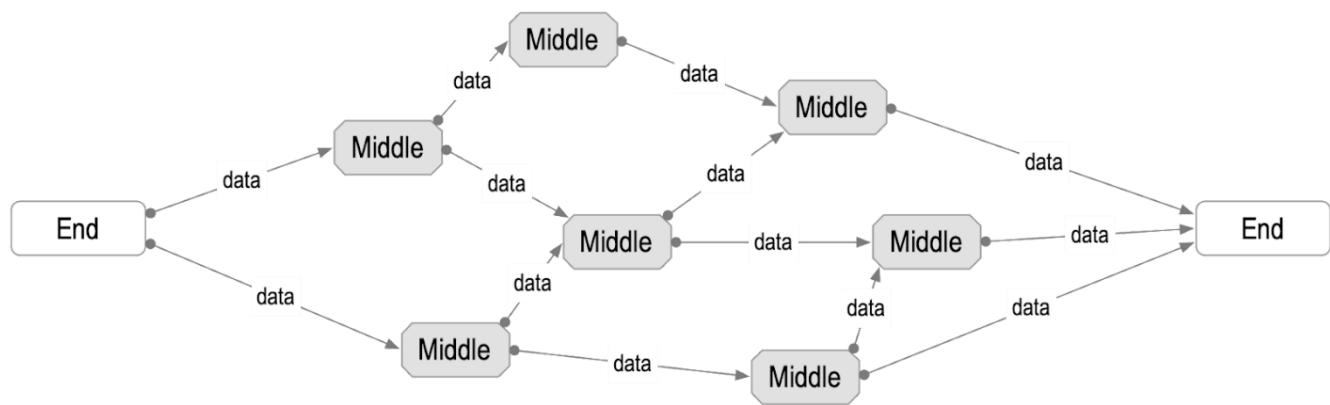
there's no such thing as anonymized data: Context tracks you. In order to be private, you need to control the context

AIDs as Unbounded Term Identifiers (using KERI terminologies)

Long-term public keys and short-term public keys.

Dual End Verifiability and End-Only Viewability

Ambient Verifiability: any-data, any-where, any-time by any-body



In summary, the baseline for strong authenticity is to use the libsodium Ed25519 signature scheme

Best Confidentiality (Public Key Encryption)

Best Combined Authenticity and Confidentiality

As developed above for combined strong authenticity and confidentiality we need both hybrid public key encryption to the receiver's key pair (with IND-CCA2) and public key signing from the sender's key pair (with SUF-CMA).

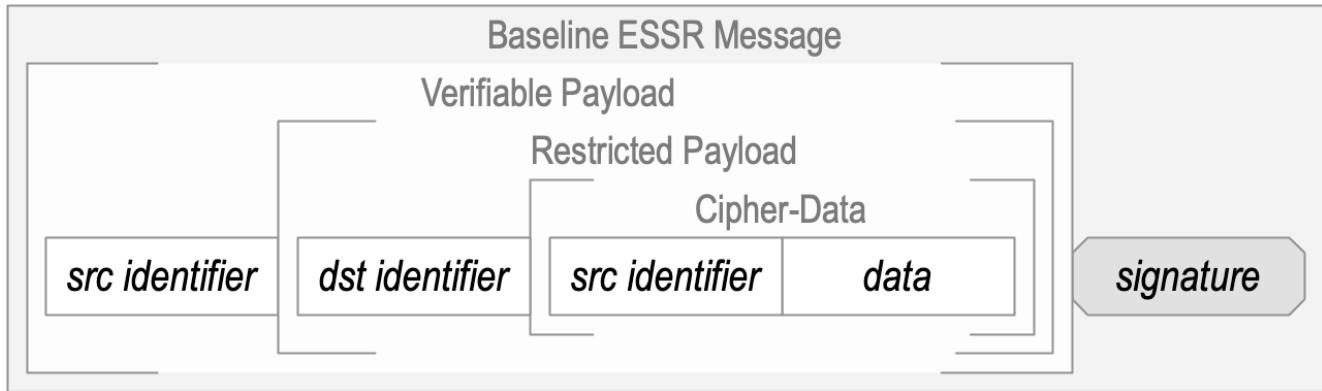
There are several ways to combine a cipher text and a signature. In order to protect against key-compromise impersonation attacks we must sign the encryption with the recipient's public key in plaintext. This is called encrypt-then-sign. But merely signing the encryption does not provide complete protection against all attacks. An attacker can strip the signature and resign the ciphertext with the attacker's key but has never seen the plaintext of the cipher. In some circumstances, this might lead the recipient to falsely believe that the sender had knowledge of the plain text when it did not. For that, we must not only bind the recipient's public key to the signature in plaintext but also bind the sender's public key inside the ciphertext.

Modified ESSR

An approach that protects against both KCI and sender impersonation of the ciphertext is called ESSR for Encrypt Sender's key and then Sign Receiver's key. The ESSR approach is detailed here [ESSR](#). For a more accessible explanation see the following [PKAE1](#), [PKAE2](#), [PKAE3](#)

Baseline KERI ESSR

We apply ESSR to KERI by modifying the basic ESSR approach to support unbounded-term identifiers by replacing the sender's long-term public key with its AID and the receiver's long-term public key with its AID. The public keys are then securely looked up from the respective KELs of the sender and receiver. This is diagrammed below.



Transcript via [Whisper Transcription](#):

about the other parties.

That's a very general definition.

It includes two complementary, but not the same, definitions of privacy.

And so the hard problem is one of the definitions.

The other definition is a hard problem, but it's not such a hard problem from the standpoint of trading off.

And their design will say that we have to have authenticity.

Sometimes we don't need confidentiality and privacy.

So we're gonna rank those as opticity first, confidentiality second, privacy third.

And you can go look them up there.

So practical elaboration, what do we mean more practically.

So how do you understand it.

The origin and content of any statement by the parties to a conversation are provable to any other party.

That's what we really mean, we can prove, right.

The origin of content is by a party, a party can prove to any other party that the origin content of a statement came from a given party.

So it's really about the control over the key state needed to prove who said what in conversation in digital signatures.

In other words, it's about secure attribution.

That's really what we're talking about.

Yes.

Hi, stupid question.

Can you explain a bit more what you mean by CQL attribution.

Cryptographically, if you create some information, can I securely attribute that information to you and not somebody else.

That usually means, practically speaking, a digital signature that has the property of non-repudiation.

So non-reputable statements need to be securely attributed.

If I can repudiate them, then you can't securely attribute them.

If I can say I didn't say it, and I got plausible deniability that you can't securely attribute to.

So we're talking about statements that people can't disavow, they can't repudiate.

Once they make it, they can't back out.

It's securely attributed.

It's attached to them.

We found the statement to the stater.

Confidentiality and confidentiality.

We mean the statements of the conversation are only known by the parties to that conversation.

The knowledge is restricted.

we have restricted distribution of the information.

And it's restricted to the parties of the conversation.

- Just to make, do you include in there that it is known to others that the conversation has happened.

- That's privacy.

- Okay.

- Right.

- Others make it different.

- Yeah, that's right.

Okay, confidentiality is about control of the disclosure was set in the conversation and to whom it was set, partitioning.

So how we do that is we control the keys they needed high content the encryption visiting the intended parties.

So if I intend you to be part of a conversation and I share with you confidential information then you're one of the parties.

If I don't intend for you to see the information then you're not one of the intended parties and therefore I want to keep it confidential from you.

Right so it's about restricting the information to whoever we consider to be part of that conversation.

So that's what the partitioning is about.

So, private and privacy is the parties to a conversation are only known by the parties to the conversation.

So, if I have a conversation with you and you know that I'm conversing with you and you know I'm conversing with you, and he doesn't know that we're having a conversation, then that conversation was private.

If he knows we're talking, even though he doesn't know what we said, the conversation is not private.

The contents of the conversation are confidential.

by whispering your ear, he can't hear me, but he knows I'm whispering in your ear.

So privacy is about him not knowing that we're even communicating.

- Yeah, and that's, I'm glad you're-- - That's the hard problem.

That's the hard problem, right.

This is not a hard problem, this is not a hard problem.

This is a hard problem.

So it's about control, disclosure of who's participating in the conversation, non-content metadata, more specifically privacy about managing, and it's quite a bit more identifiable, how clearly identifiers are viewed, but also other types of identifiers in non-content metadata, right.

So we're trying to control correlatability of who participated, who is the identifiers, right.

Not necessarily natural persons, they're just identifiers.

And it could be other identifiers besides just the identifiers of the participants, but in yet, any correlatable non-content metadata.

The reason I say non-content metadata is what I'm going to explain.

Because when we talk about privacy and confidentiality, there are two fundamentally different definitions of privacy that are used today.

Now 20 years ago, there wasn't.

We didn't have the concept of GPR, private data rights, it didn't exist.

There was only one definition, it was the surveillance definition.

But now we have the history of the surveillance definition with all the legal basis for surveillance.

Now we have this new thing called data right protection.

And so the data right protection is a different type of problem.

You solve it a different way.

And when people try to solve data right protection using surveillance technology, they're going to get it wrong.

And that's probably where the SSI community has gone off into some rabbit holes because they confuse those two.

And so I'm trying not to confuse those two because it's vitally important to be able to solve The problem with what it is, which is the correlation surveillance problem.

Is the trust over IP definition being offered as a context or basis for this back model of-- I'm trying to understand where the trust IP definition is.

The trust or IP stack is being refactored using new design principles that have evolved over time.

So the ones that I define there are going into the design.

And right now we have an ongoing task force that is designing something called a trust- banning protocol.

And I don't know, is Benji in here.

He thought, "Okay.

" Benji gave a talk about that, I think, earlier.

No, actually right now he's even been talking about it, so.

[laughter] I think we're talking at the same time.

Does that answer your question.

Is this like a before and after kind of.

I don't know.

Sorry, I'm not.

Go ahead.

I don't know, like, trust-over-IT.

[unintelligible] [unintelligible] [unintelligible] [unintelligible] [unintelligible] [unintelligible] And this is under the trust-over-IT foundation.

>> When I say T-O-I-P, it's because there's work in the Trust Over IP Foundation on trying to build what's called a trust-spanning protocol for the internet.

>> Okay.

Thank you very much.

>> So the paper that I wrote was motivated by that work.

So the first definition is about respecting the daily privacy concerns of the recipients.

Like, I give you some data, you're not supposed to do stuff with it, right.

Now that is related to not letting people see the data, but that's a confidentiality thing.

That's not a by the depth, you know.

It's like, well yeah, it's data privacy rights, but what do I mean by privacy.

And so the legal definition of privacy has two definitions.

One is about data privacy rights, and there are ways to protect data privacy rights independent of surveillance.

The second definition is about the correlatability of the public viewable metadata included in the communication.

And that's the traditional surveillance definition.

So in this definition, there's a very clear distinction between what is confidential and what is private.

Private is about the non-content metadata.

Confidential is about the content data.

And so in the legal realm, confidentiality law is consistent with this definition of privacy and confidentiality is not consistent with this one, this is a new equal realm of privacy law.

It's different from confidentiality law.

Competential law is about NDAs, right.

It's like, I'm gonna disclose you some confidential information.

The fact that we have an NDA is not confidential.

What I disclose to you is, right.

So the fact that we have an NDA is about privacy, about that we have an NDA, whereas the actual information that I disclosed to you is confidentiality.

Whereas data privacy rights sort of assumes everything.

It's like, well any information anywhere about me in any way and any shape or form is about my privacy.

So somebody has an opinion about it.

And that's really, really difficult to get a handle on from a protocol design perspective.

All right, so some legal leads.

And the reason I'm going to be very blank because if we don't understand the terminology and what we're trying to solve, then we can't build protocols the right way, right.

So the legal definition of confidentiality is consistent with the surveillance definition.

So when they came up with the surveillance definition, they were using historical case law and said, you have things like NDAs.

And the legal definition of privacy came from two different things.

You have regulatory surveillance, And you have regulatory privacy law.

And so these things are, you know, GDPR is one thing, and then you have things about mystery, future, or mass metadata surveillance.

So I'm going to great length here, just because I want you to understand that there's a basis for this, right.

Now, we can solve GDPR type privacy using confidentiality law, using something called chain-link confidentiality.

You build one of these papers up, and you can read up on them, and there's a way to do this, and ACE says, for example, solve that, but I'm not solving that problem here.

I'm just pointing out that it's not likely we've ignored that problem.

So historically, an address of any kind exists for two main purposes.

So that stuff can get routed, delivered to an address.

I mean, you got a house, I want to deliver some manure to your house.

How did I get the manure to your house.

You got to have an address like the delivery truck to deliver the manure.

Why am I delivering manure while you're at our house.

The other thing is so that legitimate parties, a government can tax or bill you anywhere.

In the old days, people didn't have addresses.

It was like John Mill lives down the street by the street.

And then the government came to the law and says, well, how am I going to report that in my book to tax you.

I'm going to give you a number.

And now I can tax you.

And now I can tax you.

And what kind of tax am I going to tax you.

It's called a property tax.

So I'm going to have to give your property an address so I can property tax you.

So historically, addresses were public information because they were needed for those two purposes.

Well, when electronic communications came along, they said the same thing.

An address is public.

It's not, it's public information.

So the only thing that we will protect is what's inside the content, not the addresses on the outside.

And it makes pragmatic sense because it's really, really hard to not have addresses because if I don't have an address that's in plain text, what can't I do with the packet.

Deliberate, right, right.

So that's a really, really hard problem 'cause if we assume that addresses have to be private in order for people to have privacy over the data, then everybody lives on an island and nobody can talk to each other, right.

So that's really not gonna work.

So anytime you start going down that rabbit hole that says privacy means no correlation possible in any way, shape, or form, then you're basically saying no value can be transferred because nothing can be delivered to its destination.

All right, anyway, so I'm not going to go-- this is all from the paper, and I realize I probably have more of these out there.

So I'm going to skip ahead.

Let's see.

I'm going to skip the conclusion slide.

Here we go.

All right.

So this is the practical application of all of this.

We define privacy protection as protection against the exploitation of correlatable identifiers, because there's always going to be correlation.

No matter how hard I try, if I want to have stuff delivered over public internet, it's going to be correlatable in some way.

I don't care if I'm using an X-Net network, or onion, marin, whatever, if somebody can surveil the rounding tables, they can correlate.

It doesn't matter.

Maybe they have to do a lot of correlation, but they're still gonna be able to correlate at some point.

So we're not worried about preventing correlation per se, we're worried about protecting against the exploitation of that correlation.

And if I can't exploit the correlation, then the correlation doesn't have any monetary value, and they're less like, I'm not going to be harmed right, That's what I would need.

So the goal becomes limiting the exploitability of correlational identifiers.

And so that gives us what we call effective privacy.

We get some effective degree of privacy, or functional privacy.

And that's a more gentle trade space.

Remember, we started with the trade space.

So we want a more gentle trade space and we have an opportunity to solve a problem.

So that's why you did all of that work, to set it up so that I can allow myself to consider solutions that have some degree of correlatability, but I can tune them to minimize the exploitative potential of that correlatability.

All right.

So here's another analogy that I hope will be useful.

Authenticity and confidentiality are like a cold war.

And the reason they're like a cold war because we can build security overlays that provide more returns from protection, even with minimal resources.

If I've got the signature that I do the key management right, and it's got 128-bit security on it, it's computational and completely going to somebody to break that signature.

They're going to have to do a side channel test.

And if I do my stuff around A, I can pretty much prevent those side channel tests unless somebody really, really aggressive.

There's always going to be that, but practically speaking for the value of protecting, the resources I have to expand versus the resources they have to expand and attack it are on my favor.

It's an asymmetric war in my favor.

They have to work really hard to break my key management if I'm doing it right.

I don't have to work so hard if I'm doing it right.

The reason privacy is a hot work is that no matter what I do, somebody is going to figure out a way to correlate around whatever privacy mechanism I create.

They will find a way.

And that means that my ability to decrease the attack surface inverts to the attackers' favor.

I have to do a heck of a lot of work to prevent them from correlating me.

And as soon as I figure out how to prevent it, they figure out another exploit and it goes on and on.

So basically, there's always going to be casualties in a hospital.

So we focus on exploiting the correlative identifiers so that we can do the risk mitigation trade-offs.

We don't want to die, we want to survive the fight and go to bed.

In a cold war, nobody's dying.

There might be a single weapon out there called a flonic computer that someday we'll have to worry about.

But we may never ever have somebody launch it on us because we've already figured out a protection mechanism for it called post-flonic photography.

So I put this on here because I really like Swiss Halbergers.

I don't know if you guys know, there's no way this was the state of the art of warfare.

And the reason it wasn't saying the art is that pound per pound, dollar per dollar, the phalanx of these guys could defeat any really, really expensive set of armored knights, right.

Because of this weapon and their training.

And so, until gunpowder was invented, people were hiring these guys as mercenaries because they were bomb.

They won all the wars.

That's why the person never was conquered by anybody right because of these guys.

So when I think about defense, I want to think about techniques like this really cheap.

They're just a bunch of farmers.

They're not standing on them, right.

I don't have to pay them.

I just tell them, hey, someone's going to attack.

Go grab your hollabirds and put your stuff on and go out there and defend the village.

And they win.

And all those really expensive French nights and their advancing armor all died on the field.

And they went home and said, oh, we've got to raise taxes because we couldn't We have a second party, they communicate.

There's a third party, we don't like the third party.

There are the intermediaries, we might like the intermediaries.

The third party is trying to discover information disclosed either directly between these or indirectly through the intermediary.

Or through collaboration with the important party, the intermediary.

or through collaboration with either the verdict party or the second party.

So you might have a collusion.

So those are all the paths where somebody can attack that information book.

Right.

So, I think I just said all this.

The, okay.

So, in the paper, I go through an analysis of most of the attack surfaces for privacy.

and I won't have time to go through all those here, but I just want to set it up because I want to talk about protocols that how we attack, the solution to those is to use relationships to protect us.

So what does this one say.

Right, so privacy and respect to the third party has no knowledge of the end of the party, used by the first and second parties for the conversation.

So we're trying to keep the third party, not just confidentiality, that's easy.

But not even knowing that these two parties were engaged in conversation, that's the hard problem.

So you're only wondering how do we do that.

Well, how do we do that.

(mumbles) Oh no, that's more stuff, all right.

So we say the privacy is protected.

third party has no knowledge of the data by the first and second parties, right.

That's our standard.

Common which were the first or second part.

So who can give me an example of the most common first party collusion, privacy, and combination breaking mechanism on the web today.

Where the first party is colluding with the third party.

- Make your email for 10% off.

- A cookie.

A cookie, yes.

A web cookie, right.

Who's tracking the user.

The user's own browser, the cookie that they accept.

So they're colluding, even those inverters.

If they didn't know how many cookies to get their thing, then the party who created the cookie could attract them.

Second party collusion, first party data.

You go to any website and they ask you, what's your email address.

Okay, now they have first party data that they can correlate.

They ask you any question and you give them any information.

that second party, because you didn't constrain what they could do with it.

You didn't say, oh by the way, here's my email address, and by the way, don't sell that to anybody.

They might say, oh we don't share with anybody.

Maybe they don't, maybe they're lying.

Maybe what they do is they correlate a bunch of data about you and then de-anonymize it and share the purpose of it.

And then the person they give it to And then just re-de-anonymizes it and finds out who you are because I don't know.

If I pay a sprint of a few thousand dollars, and well maybe more than that, maybe \$10,000, and say, tell me the names of everyone in this room.

'Cause that would happen to me within 30 meters of my phone at this moment in time.

Now they won't give me anybody's name, but I'll know where you slept every night from the last year, depending on how far back I go.

And so pretty easily I can correlate to where you sleep most nights, so that's probably where you live.

And is that easy to then look up your name and address.

Absolutely, right.

So anonymized data, there's no such thing as anonymized data.

It's just hardly correlating.

That's all it is.

So don't fool yourself into thinking that second party isn't a coulour about privacy.

So if the first party and the second party is not trustable by the first party, there's nothing we can do about it.

It's zero.

Nothing we can do about it.

- The zero and all the screws protect you from it.

- Wait, wait.

So you're in this room, you proved to me a zero-knowledge your age, right.

Do I know who you are.

Absolutely.

How do I know who you are.

Because the context of you being in the room gives me enough information to correlate who you are.

I can care less what you did to selectively dispose of you.

(audience member speaking off mic) You gave me the context of this room.

By walking in this room, I know everything about me.

I know the answer.

(audience laughing) So in spycraft, nobody in spycraft ever selectively discloses data unless they control the context of the disclosure.

That is the biggest fallacy in the world to say that I can cryptographically selectively dispose information, and I don't have to control the context of the disclosure.

If I walk in a building, they know who I am.

I don't care what I do or don't disclose, walk you in the building, they know who I am.

So there are those groups that are a waste of effort.

No, they're not always set up.

There's lots of applications where they're very, very useful.

But you can use them absent all of the capabilities of what they're designed for, which is spycraft.

You have to think like a spy if you're going to use them.

People don't.

So the toy use case of using a journal to prove that you're old enough to enter a bar, and you have more than contents of that-- If there's a security camera on the scene, then they know who you are.

So there may be some bars that don't have security cameras.

There may be some bars that are cash only, so you don't have to use a credit card to pay your bill, you're done, you're done, you didn't matter, you didn't matter, right.

So we want real privacy, we don't want fake rights, we don't want privacy that potentially allows people to correlate, right.

That's a hard problem, we're trying to not actually be correlated, that means we have to control the context, we have to control the context, we cannot be correlated, [Inaudible] Excuse me, but I consult a problem carrier.

I don't have a solid data way.

So I'm going to solve it the way that I'm not solving it.

So the main thing that we care about with the IDs is they're ungrounded term identifiers.

[INTERPOSING VOICES] Autoeconomic.

So it's close to autonomous.

Same route.

It's a self-governing identifier.

And that means that the key management is built into the identifier.

So in cryptography, we have the concept of long-term public keys and short-term public keys.

And the main reason we use short-term public keys is the limit to the exposure of long-term public keys.

Because no matter how much you try to protect your key pair-- so we're assuming it's PKI-- if I use the right key in any way, shape, or form, then it is exposed to a side channel attack.

And eventually, we have to assume that it will get and therefore I can't use it anymore.

So I might use short term public keys that I can throw away to minimize the exposure of long term public keys.

But the I.

G.

s, their key innovation is that they're not just long term, because long term could be two years.

And this says all authenticateable public keys should be rotated every one to two years, just as good practice, right.

I want unbounded term.

I want my identifiers to never ever, I never have to replace the identifier.

I want the identifier to persist indefinitely and I want to be able to switch out my public keys.

So that's the main difference.

So if we can fix that and we fix the hardware on the PKI, which is limiting exposure of our public key material or making it so that it doesn't matter that it gets exposed because control by doing a rotation and the rotation is just as secure as the first place and that means that when we do that we can we can change cryptographic protocols because we don't have to use a criminal keys anymore we don't have to use short-term keys because what we're doing is we're using unbounded term keys that have rotated the key state and so instead of using short-term keys to minimize the explosion of long-term keys we have long-term keys that are strong enough that they can be exposed because we can rotate them.

And the identifier is what we're protecting, not the long-term fee.

Does that make sense.

No, not at all.

But then the long-term fee becomes a contract you're in.

Well, absolutely.

The AID is a vehicle to track you.

Absolutely.

Okay.

So, but understand, context tracks you.

It is a misnomer to say that a cryptographic piece of information tracks you independent of context because you as a physical entity are trackable by the fact that you're alive and you move around.

So if you don't control the context in which you exist, you are still trackable.

It is a fallacy to say that if I cannot have people track some cryptographic identifier, that somehow I'm not trackable.

If you look at any data scientist and you say, "How hard is it to correlate somebody.

" And they go, well, if they give me a cookie, I don't have to do any work.

It's right there.

But if I don't have a cookie or I don't have some tracker or something like that, then I just get a data set.

And I do a regression on the data set.

And it costs a little more change because it costs some CPU cycles.

But I still get a high probability correlation that I can still monetize.

So once you're not finished shooting in the military, you're actually trying to keep somebody from shooting a missile at you, right.

If you're trying to be protected from aggregators correlating and selling your data and sending ads and interrupting you, statistical correlation is monetizable, it's absolutely monetizable.

So if you can't solve statistical correlation, you're wasting your time.

So we want to be able to solve as good as we can.

But understand, we are never ever going to prevent correlation.

It's just we're going to delay the time.

We're going to increase the cost.

We're going to do things to try to put the economics in our favor.

That's all we can do.

We want to flip the economics in our favor.

More truth in the forest.

Anything-- if we're fooling ourselves else to think we can do anything more than that, and thus we're surprised, and thus we're willing to live in a world where everything's reputable, we control the context of every disclosure, and we're all free.

Don't stop, right.

And I know some people that come to this conference try really hard to beat that, and more power to them, right.

- Good answer.

- I don't know, I wanna buy things, you know.

(audience laughs) I'm gonna have a life.

(audience laughing) That means I gotta participate in the economy.

Okay, so let's see.

There we go.

So we have a tool here between authenticity and confidentiality.

The way we solve authenticity in general, securely, is something called end-to-end variability.

So here's a network, you have two ends.

What I don't want to do is protect the middle.

I don't want to have to make it so that I have to make everything in the middle secure.

This is called perimeter security, right.

This is the antithesis of Zero Trust.

If I had to protect everything in the middle, in order for these two ends to communicate authentically and confidentially, then I've lost.

I've lost the battle.

It's now a hot war.

It's not a cold war.

I want it to be cold war, and that means I want to have this weapon that's called end-to-end verify ability.

So that's authenticity.

So if the edges are secure, the security in the middle doesn't matter.

That's what we're shooting for.

So if I can verify any day to anywhere, any time, by anybody, anybody can do that.

Right.

Then I have true zero trust, because zero trust says, never trust, always verify.

You have a state of anti-bariculability.

You have a state of anti-bariculability.

That means that there is no opportunity for an attacker to do anything, because every action is verified.

So we're at the far end of the zero trust scale, because we said, everything is verified.

Just some things, how is that not complete surveillance.

Exactly.

It's not complete surveillance if we control the context of the verifiability.

So it looks like what I'm building is a perfect surveillance vector, absolutely.

(audience laughing) So I just want you to make sure that we're starting with a extremely strong authenticity, which looks like perfect surveillance.

It's much easier to protect one's private keys than protect all the internet and infrastructure.

If I can make it so that all that this guy has to do, and this guy has to do is protect the private keys.

There are no treasure troves.

There's no shared anything.

There's no trust.

There's no trusted identity providers.

There's no trusted certificate authorities that get messed up.

There's no trusted anything in the middle.

They just have to be really good with their key management.

- Does this say anything true for protecting an individual network.

Have you said all internet infrastructure.

Well, obviously no one's gonna be able to-- Any network is anything between the two ends.

It doesn't matter.

It applies to any kind of stuff.

Now you can have infrastructure that supports either of the ends.

And in quenching, we're here, he has some diagrams showing that.

This is a really simplistic diagram.

But the question is, the end controls stuff.

The end doesn't control the middle.

So the end might be complicated.

The end might have servers.

It might have a bunch of stuff.

But the end controls all the stuff they control.

They're not reliant on anybody.

The ends are not relying parties on anything other than the other end.

So you get the gifts to the other end, thumbs get carried by a pigeon.

If it's verifiable, it's secure.

Doesn't matter how I got there, right.

True is this true, no matter the source.

Verifiability is verifiable, no matter the source, or the conveyance mechanism, right.

You're verifying to the source, It doesn't matter who's the conveyor.

All right, so confidentiality is the dual.

And the dual of this, same network, is only at-end viewability, or end-only viewability.

That means this end can take a message and pack it in such a way that only this end can view it.

No middle can view it, nobody else can view the data.

And this guy doesn't have the ability with regard to their viewability.

What that means is that if I use symmetric encryption to communicate between two ends, I don't have end-only viewability.

Because both of them have the same encryption key, which means either one of them can encrypt something and say, I didn't create this.

He did.

So it's not end-only viewability unless you're using public key on the top.

You can't use symmetric encryption if you communicate with your two hands and satisfy this property. If you don't, then you have-- if you do, you have weak confidentiality.

You don't know who can view it other than you said, well, both of us can view it.

But I don't know his key state.

I get control of his key state.

If his keys are bad and he linked his keys, then anybody could decrypt it.

I want something that only I can decrypt.

And he can't even decrypt.

Once he encrypts it, he can throw it away.

Now he has no liability for that data 'cause he himself can't decrypt it.

I'm the only one who can.

That's end-only doability.

That gives us the strongest level of competition.

Remember I said we're gonna start with the strongest we can do in this trade space.

And then say, give him the strongest.

What can we do about privacy.

But let's do something that's not quite as strong because we know we're going to have to back off from it in order to get A or B or C or D because we're making these justifications.

So I don't want to do that.

All right.

So the dual is that it's one data, one way, or one time by one body.

Right.

So this is like-- right here.

Anybody can verify the source, and only one person can be the destination.

So the combination of those two is what we're shooting for.

So if I want to do secure attribution, the best practical technology we have is digital signature. And that digital signature should have a property called strong unfortunately and shows message in fast.

Now of all of the libraries that are available for you to use that are commonly available, how many digital signatures have strong unfortunately again, shows the message attack.

No, chosen message attack.

Yeah, that would be chosen play attack if it's a signature, right.

We're not talking about encrypted data.

Well, there are lots of digital signatures that have that property, but of the commonly available libraries, there's only one.

It's called Lipsodium, ED25519.

For those of you who use use ECDSA, sorry, no have SUF, it's only got EUF.

So here's the paper where you can go read about it.

So for example, EUF CMA is an existential enforceability and if you have SUF you have EUF, but there have been several attacks against ECDSA because it's only UF, and then they have to add a bolt-on mechanism to try to patch it.

So I'm just saying, if we're going to start with something, let's start with the strongest thing and not start with something and then say, well, plus some patches, right.

So the strong-methodicity baseline is lip sodium.

And by the way, it has a few other things.

So it's not SPS, it also has a strong universal exclusive ownership, malicious strong universal exclusive ownership, resiliency against key substitution attacks, message bound security, and it also has protection against key memory linkage attacks.

So we get all that for free.

We don't have to add to it.

We don't get any of these with But ECDSA, this is all we get with ECDSA.

- But this is not yet bent or bent.

- Well, it's on this roadmap, but that's right.

But yes, so it's not like the government is actually secure, right.

They're kind of 20 years behind.

(audience laughs) But yes, if you have to do work with the government, you're gonna use ECDSA, and you just need to know that you have to use ECDSA like an adult, because it's not safe.

(audience laughs) [Inaudible] Yes.

Yeah.

And one of the -- and also the nonce or the nonce of ECDSA.

The current libraries for Bitcoin and Ethereum don't use salty nonce.

And that's a term I made up to refer to a nonce that has cryptographic entropy.

So it's a salt, but it's also a nonce.

And if you don't use this sufficiently strong knots, then you can back out from a sequence of signatures with knots that are in a sequence, you can back out by the key just from the knots.

9 doesn't let you pick your knots.

It picks it for you and it always picks it with high end.

So the reason is, this was designed according to one of his best practices, which says if you're gonna do a signature, you're gonna do it as strong as possible, you're not gonna let the user have any choice, And what that signature is, because usually we'll always mess it up.

So, I don't trust anybody.

That's Edward's Daniel Bernstein.

I don't trust anybody.

[inaudible] So, now we have all this signature.

That's done.

We know the best that we can do.

Right.

Hold stop.

If you're sitting And you're going, what should I do to my protocol.

And you're going, I can't decide.

Should I be using it.

You should start with lipzonia.

Unless you have a really good reason, like the government won't let you use it, then you should be using lipzonia.

Now, strong capital nageality.

The best that we can do is called indistinct which should be against adapted chosen message attack.

So our CCA2, 'cause CCA, chosen, we decided to have a fast target.

So that's the best that you can do and there are schemes that do that.

In order to do that, if you have NCCA 2, you can also get NCCA 1 and NCCA 2.

And this is chosen by Dr.

Kachin.

You can correct me if I say it wrong.

But basically, they can't submit cyber text in such a way that they can discover the right key by having an adaptable an adaptive oracle that can tell them things about the side of the thing.

So it's really, really hard.

So that's the best we can do.

And here's some references.

So what encryption schemes public key encryption or symmetric encryption.

It's actually pretty interesting to get in CC8 to a symmetric key.

A public key encryption is really, really hard.

But understand if we want as confidentiality in terms of who can see the data and only the ability to maintain public encryption.

So there are encryption seeds that give that.

They're called integrated encryption systems.

And an elliptic curve integrated encryption system called ECIS.

And one example of an NCCA2 ECIS is O from our friend, the sodium.

It's called the CO box.

Okay, so now we have that.

Now, What does that do.

Well, an integrated encryption system has this really nice property that it actually has the performance of symmetric encryption.

You don't take performance by using it.

It's just as fast as symmetric encryption, but it's public key encryption.

And how does it do that.

What it does is that under the hood, it's actually doing a non-interactive Diffie-Hellman key exchange so that the other side can decrypt it, and the side that is encrypted and never sees the private key, so it can't decrypt it.

And so it basically creates a private key, sends the public key, the ephemeral public key, the other side, and it uses the other side public key, but it's not interactive.

So nobody can get in between them.

You just do it and send it.

The interactive ones have the tax rules.

So that's why it can be CCA2, but it's not interactive.

And so we don't need to go through all this.

So recently, this RUTF RFC 9180 has generalized this principle of PCIS, something they call hybrid public key encryption.

So you go to this RFC.

And so that's the state of the art, as far as I can tell.

And people are building systems on top of 9180, but none of them are in any standard libraries yet.

I don't know when they will be.

hopefully someday.

And they even extended to have multiple modes of interaction.
Steelbox is equivalent to the base mode.

So it's the least base mode.

So what happens.

Oh, this is just detailed on that.

But HPA-Key is not authenticity.

And a lot of people call it an authenticated encryption scheme.

right.

They put the word authentication, authenticated encryption, but it's not.

It's very, very weak authentication.

So anybody who sees the word authenticated encryption should run the screen meaning go, "Guys, you're kind of fooling everybody."

" Right.

It's very weak authentication.

So one of the attacks, as Section 9-11 of R.

C.

points out, is that all of the variants of HPK in their latest, greatest, whatever, are subject to key confirmation and birthation attacks.

And they recommend that if you want to protect yourself against that, then you should sign your HPK.

Okay.

So you can't get authenticity without signing.

Pulled out.

You can get authenticity confidentiality, but you have to do pull.

You can't do just one or the other.

You have to do both.

Right.

So there are some references.

We don't have to go through those.

Alright.

So how do we get the best combined.

So we start with NCCA2.

We start with SUS-CMA.

So that's lip sodium 825519 and So the seal box and we could say, well then how do we combine them.

Right.

Do we encrypt and sign.

Or encrypt and sign.

Or sign then encrypt.

Or encrypt and sign.

Which one do we use.

None.

None of the above.

Right.

All of them have weaknesses.

So there is a mechanism-- and I won't go into details because it's off in the paper.

It's called ESSR, Encrypt Center Sign Receiver.

This mechanism protects against all the attacks that everybody has come up with so far.

And I'm sure there's others, but these are the ones that everybody's concerned about.

So these are the four properties.

Third party enforceability, plain text, third party enforceability, cyber text, receive reportability, plain text, receive reportability, cyber text, right.

So if I do just encrypt and sign, I get three of them, but I don't get just two of them.

And if I do sign the encrypt, I get two of them.

I don't get all, either of them give me all four.

But ESSR gives me all four.

So, best that I can do to get bold, strong authenticity and strong confidentiality is ESSR.

So, and the reason is, is that I'm binding the sender's public key inside the cyber tax, and I'm binding the stripper's public key in the enclosing signed lay tax.

So the adversary can't force message and compromise either authenticity or confidentiality.

So it protects against all the taxes, you compromise approximation and all of the taxes, stuff like that.

I'm sure there's a tax that aren't in the papers but these are the ones that people have attacked.

So anyway, some lay the papers.

Sorry.

Wait, that one's, that's a jibbleded slide.

(m bahing) (muffled speaking).

SSI 101

Session Convener: Limari Navarrete (DIF) and Stephen Curran (BC Gov Team)
Session Notes Taker(s): N/A

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

[Link to the slides](#) used in the session

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

A great discussion about the background/philosophy/principles of SSI, followed by a dive (sometimes too deep) into the technical underpinnings of SSI.

Privacy as Alignment of Expectations

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

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

No Notes Here

How can DNS help enable Digital Trust!

Session Convener: Mathieu Glaude

Session Notes Taker(s): Mathieu Glaude

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

When an entity is presented with a verifiable claim, there are three things they will want to ensure:

1. That a claim hasn't been altered/falsified at any point in time (cryptographic verifiability, verifiable data registries)
2. That a claim has accurate representation (DID authentication, accurate representation)
3. That a claim has authority (authorization, authority)

The first two questions can be answered with current infrastructure (e.g., crypto, verifiable data registries). The second and third questions can't.

We discussed how DNS infrastructure can be used to store DIDs and pointers to trust registries. This allows someone seeking to make a trust decision to use the DNS records as a supplemental source of input to (a) ensure the DIDs match, and (b) discover trust registries. DNS records can serve as inputs to trust decisions.

Here is a working demo of this solution:

<https://www.loom.com/share/57db10ddc9f448bf8ff2fb7b10138283>. Feel free to write feedback 

We also recently co-published an [IETF Working Draft](#) of our work if you wish to have more information.

The biggest question was: why don't we store trust registry records inside the DNS?

Comments

- mathieu@northernblock.io: Love the concept above and wanted to flag up [the did :dns specification](#) that was co-authored by markus@danubetech.com and tomislav@trinsic.id which leans on exactly this idea, i.e., using DNS itself as a DID method. Layering on Trust Registries to these DIDs then is similar to using DID-Linked Resources (DLRs) suggested by [Alex Tweeddale](#) or even without that what Fraunhofer Institute has been doing in Europe to store trusted issuer lists in DNS entries. **MG - thank you, have gotten familiar with DID DNS. We are DID Method agnostic, simply allowing DNS servers to be used as a secondary store for DIDs and various pointers to things such as trust registries.**
- shigeya@wide.ad.jp: I wrote a [short discussion paper on did:dnssec proposal](#). Also, in the RWoT paper "[Verifiable Issuers & Verifier](#)" which shigeya co-authored has discussion on the use of DNS/DNSSEC.. **MG - thanks for sharing!**

Matthew G - Northern Block

Working with Cira Canadian top level domain manager

History

- Canada requires proof of Canadian presence in order to have a ca domain
- Used to use antiquated methods, fax, email documentation

3 provinces have stood up a closed credential network, governance is higher trust as result

Using DID to verify credentials

Asks the question of human trust, trust repositories

Current

- DNS as a Trust Repository
 - Alternative places to look for verification of issuer

Process

1. Holder presents Drivers License (DL)
2. Issuer queries Verifiable Data Resource (VDR) maybe Indy
 - a. Holds DID of Issuer, domain, Trust Repository
3. Issuer has records in its DNS Zone pointing at TR along with DID
4. Holder can query Trust Repository (DID, DL Issuer, domain)



Where are my product peeps in the house?

Session Convener: Bonnie Yau

Session Notes Taker(s): Bonnie Yau

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

Use cases, user experience, product management

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

This session is for anyone who identifies as a person working on products, or is interested in product management related topics.

Participants were given a choice to speak to any one of the following questions:

- Where do ID product folks come together to exchange ideas or share learnings?
- What are patterns you have been able to apply from your past life to the ID space?
- What are the top challenges in your way when it comes to creating great ID products?

Discussion

Where do ID product folks come together to exchange ideas or share learnings?

- [Product Manager Group at DIF](#)
- Acting in working group leadership roles at various communities
- [Trinsic's The Future of Identity Podcast](#)
 - Podcast with Katrie Lowe from Domi (recommended)
- [SSI Orbit Podcast](#) by Northern Block
- Bhutan presentation on TolP

What are patterns you have been able to apply from your past life to the ID space?

- As someone with PhD in Microbiology, see a lot of things that translate, read the SOP, both helpful and hard to jump from one area to another, research with in data management, bringing that skillset to identity space technology

What are the top challenges in your way when it comes to creating great ID products?

- Not enough focus on user experience
- Lots of good tech, but really hard to marry them with what the user needs
- Example: Verifiable credential presentations, how does a user know when they're done (and perhaps need to go back to the app they came from)?
- Accessibility of products
- Lot's of talk about infra and technology here by smart people

- End users are just normal people
- Experience is not seamless, how do users make sense of everything, they just don't understand it
- Lack of user research
- The “cold start” problem
- There is no such thing as a “small” ID problem to solve, getting from 0 to 1 is hard
- Example: As a small business or start up, need to focus on some sort of driver like regulatory motivated use case like track and trace, prove that one is an authorized trading partner
- Need to ask ourselves WHY a lot more - 5 whys
- We are asking the wrong question - the problem the user has IS NOT I don't have SSI or I don't have verifiable credentials
- Governments can create more open loop opportunities
- How do we take all existing IDs and make them digital?
- And once we have all these digital IDs, what can we do with them?
- Need to consider “one identity” vs a presentation of a persona needed for the context
- Example: Use case helping farm workers, need to consider digital literacy when creating the solution

30 days from Web5: A preview of the stack and Developer Preview release next month

Session Convener: Daniel Buchner, [Gabe Cohen](#)

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

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

- [TBD's Developer website](#)
- [DWN's JavaScript SDK](#)
- [TBD Learn Portal](#)
- [areweweb5yet.com](#) <- This one has links to most SDKs and repos

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

- Web5 terminology
 - Wanted to borrow some of the concepts/themes of Web 3.0 without necessarily relying on everything being token-based
- Web5 / Decentralized Web Nodes (DWNs) terminology
 - Universally addressable
 - Secure
 - Resilient

- ... (missed out a few)
- Decentralised Web Apps (DWAs)
 - Like [Progressive Web Apps \(PWAs\)](#)
 - DWAs are like PWAs but with DWA SDKs embedded
 - Licensing: Apache 2.0 and will be open source, the primitives are all designed to be open-source up front
 - “Friends” aren’t necessarily humans, they can be linked services/primitives as well.
- Use cases being worked on by TBD
 - [tbDEX liquidity protocol](#)
 - Music
 - Hotel/travel
 - All of the primitives in these use cases can be imported, e.g., import in “travel” primitives like tickets, itineraries etc.
- Roadmap
 - Implement actual use cases above, to make it come to life
 - tbDEX has been lagging a bit, but is still under development
 - Announcements coming in the next few weeks at a couple of conferences
 - <https://areweweb5yet.com/>
- Who are hosting nodes?
 - [TBD/Block](#) hosts some of them
 - Major web hosting provider That Must Not Be Named
 - [Benri](#)
 - More to come down the road
- How do the providers get paid for providing hosting?
 - General idea is freemium hosting: give away X GB for free, but then since the data can be accessed by many decentralised apps, it’s more “valuable” data
 - Product hypothesis: people don’t pay much for Dropbox, OneDrive, Google etc since it’s mostly used for documents, PDFs
 - People *do* pay for storage for photos, videos since they are actually and broadly reliable
- Public vs non-public DIDs
 - [did:ion](#) entries have additional metadata that can describe whether something is an app or not
 - There’s GDPR issues with public DIDs, but there’s also a lot of value in searchability and indexability
 - Unlike IPFS, replication isn’t to random servers, you choose which DWNs to replicate to and can ask them to delete.

IDtech & Why it's the key to SSI adoption / Riley Hughes

Session Convener: Riley Hughes

Session Notes Taker(s):

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

No Notes Submitted

Credential Format Comparison

Session Convener: Paul Bastian, Andre Kudra

Session Notes Taker(s): Andre Kudra

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

RWOT11 Paper Publication Presentation 13APR2023

https://docs.google.com/presentation/d/1s5yWNS3Z4goTGnVq7y_3maliVme0pVsg6803gk348Oc

Credential Profile Comparison Matrix

<https://docs.google.com/spreadsheets/d/1Z4cYfjbbE-rABCfC-xab8miocKLomivYMUFibOh9BVo>

Credential Format comparison and IDunion Strategy

https://www.linkedin.com/posts/idunion_credential-format-comparison-and-idunion-activity-7008024119598276609-0pS-

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

We are presenting the work done by the community around the Credential Profile Comparison which was started at IIWXXIV.

What

As a community effort, we are creating a Credential Profile Comparison Matrix

It is accompanied by a Guiding Paper located at <https://github.com/WebOfTrustInfo/rwot11-the-hague>

Paper is done, the matrix is work in progress, and probably continues to be

Why

The different Credential Profiles have strong follower communities

For many good and obvious reasons, they are convinced their stack is “favorable”

Having a fact-based comparison is long overdue

With this work, we facilitate an objective discussion and comparison
 This will ease technical and non-technical decision making

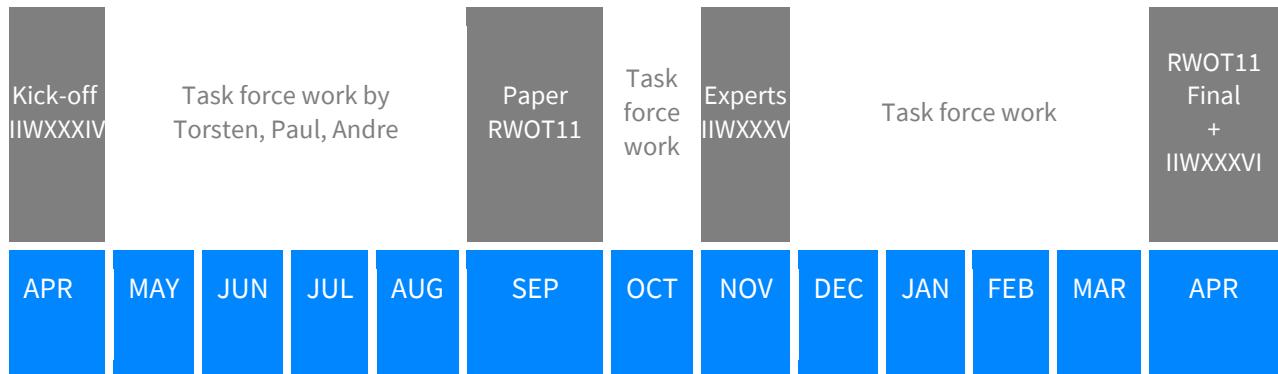
How

A comparison matrix is created

Comparison categories (6) and criteria (50) are derived

Experts from the different stakeholder groups are engaged to obtain their input

Key milestones 2022/2023 so far



Matrix

Too large to easily display - see here:

<https://docs.google.com/spreadsheets/d/1Z4cYfjbbE-rABcfC-xab8miocKLomivYMUFibOh9BVo>

50 Criteria

Credential Profile	Credential Format	Signing Algorithm	Revocation Algorithm	Key Management	Trust Management
Formal Specification	Implementation Support (e.g. Libraries)	Implementation Support (e.g. Libraries) / Active Community			
IPR Policy	IPR Policy	IPR Policy	IPR Policy	IPR Policy	IPR Policy
Implementations	Specification	Specification	Specification	Specification	Standardization (Body, Process)
	Standardization (Body, Process)	Standardization (Body, Process)	Standardization (Body, Process)	Infrastructure for Key Resolution	Specification
	Technology Readiness Level	Technology Readiness Level	Technology Readiness Level	Key Rotation	Description
	Encoding Scheme	Recognition by government authorities (NIST, BSI, ...)	Recognition by government authorities (NIST, BSI, ...)	Key History	
	Rich Schemas/Semantic	Performance	Category	Party	
	Crypto Agility	Hardware support	Performance		

	Selective Disclosure	Unlinkability/Uncorrelatability/Blind signatures possible	Observability		
	Predicates	Security strength	Traceability		
	Compatibility with Signing Algorithms	Post-quantum security	Scalability		
	Compatibility with Key Management Methods (Issuer)		Offline Friendliness		
3	12	11	12	7	5

Insights

The obvious: So many credential formats

The number of profiles is even higher (by an order of magnitude) through combination with signature algorithm, key management, revocation, trust management

A lot of clarity is achieved with the methodology

Not all data items could be collected yet

Next steps in 2023

ToDo	Who	When
Finalize and publish guideline paper	RWOT11 experts group	April 2023
Matrix expert discussion cont'd at IIWXXXVI Mountain View	All experts	April 2023
Presentation at EIC 2023 Berlin	Hughes, Bastian, Loddertedt, Kudra	May 2023
Presentation at Identiverse 2023 Las Vegas	Hughes, Loddertedt	June 2023

Identity & Internet the 17th Critical Infrastructure

Session Convener: Ken Gantt "The ID Guy"

Session Notes Taker(s): Troy Samuels

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:

16 Critical Infrastructure Section

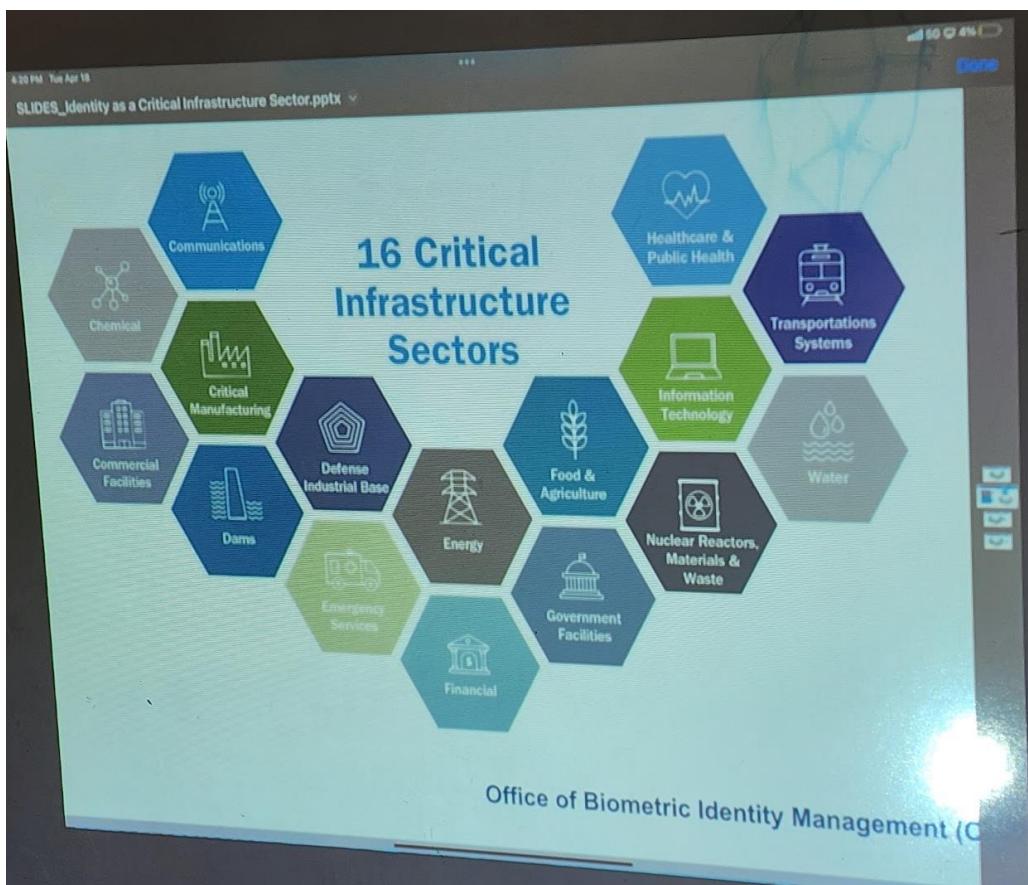
DHS- Outreach, Education and Communications

Energy, Govt Facilities, Water, Technology, and others fall under DHS

NIPP 2013

PARTNERING FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

All of this comes back to the people/identity.



Scandinavia Govt ID is digital. Having a centralized infrastructure creates a single point of failure.

The 1974 Privacy Act and other legislation makes such a move for the US a step in the progress.

Decentralization via Blockchain to achieve a similar state here in the US.

Challenges identified:

- Life Cycles too long.
- Outsourcing causing information sharing issues.
- Employee retention shortening

Efforts are being made to align identity services with doctrine.

How you approach identity in a way that creates more public private partnerships?

Fear of the government can be a hinderance to achieving that end. So grassroots efforts to improve that perception is the way forward.

Symposium development to engage the public and vendors to help create a framework for public review and input.

Fed ID coming up in Sept 2023, DC

From biometrics to Identity

Have we coined a phrase similar to digital exhaust to add to the identity equation/definition?

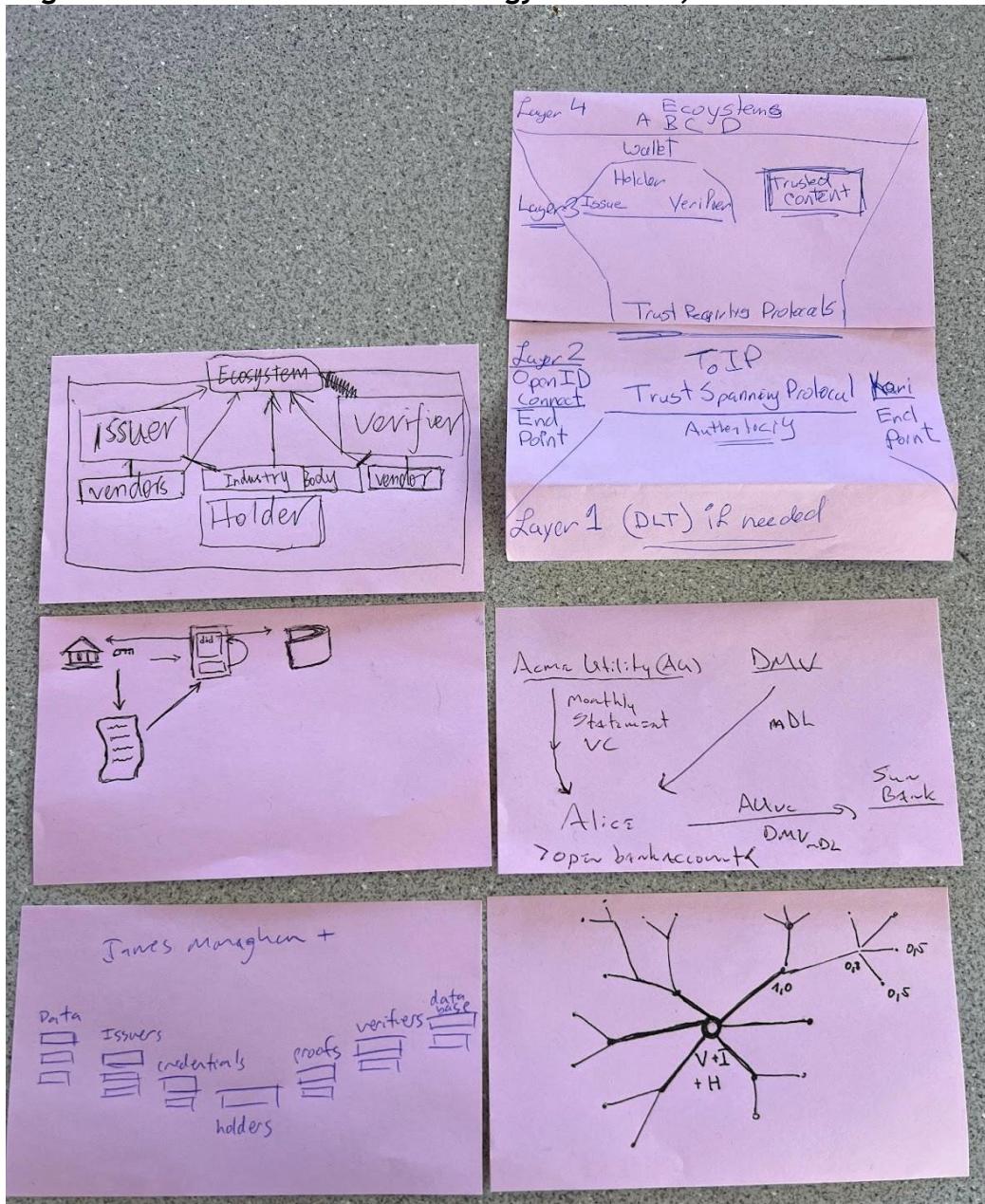
"Digital Footprint"

Many conferences globally create opportunity to bring us closer to more Public Private partnerships.

Visuals of SSI

Session Convener: Zack Jones
 Session Notes Taker(s):

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



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

In a complex and tech-heavy space, using visuals to explain how our technology works is crucial. We discussed different visuals that people use to explain and depict self sovereign identity and trust ecosystems. Above are the drawings that participants shared.

UX of Diia (a Ukrainian Government App)

Session Convener: Francisco Corella
Session Notes Taker(s): bengo

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

Slides:

<https://pomcor.com/documents/UX-of-Diia.pptx>

A discussion of the User Experience of the Diia mobile app and web portal of the government of Ukraine, mostly based on a video of a presentation to the Canadian CIO Strategy Council, available at "CIOSC Special Member's Event" (canada CIO video about DIIA)
<https://www.youtube.com/watch?v=l2t6WrYyt5I>

Documentation about this as a memo to a canadian senator (via Jose)

<https://static1.squarespace.com/static/63851cbda1515c69b8a9a2b9/t/6398f63a9d78ae73d2fd5725/1670968891441/2022-case-study-report-diia-mobile-application.pdf>

https://en.wikipedia.org/wiki/BLS_digital_signature

* example of threshold crypto

* more <https://eprint.iacr.org/2022/534>

Inter-Trust Domain Protocol - Can DIDs, AID, and OpenID Talk to Each Other?

Session Convener: Wenjing Chu
Session Notes Taker(s):

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

Wenjing introduces the candidate protocol for the Trust Spanning Layer - a current work in progress in the Trust over IP (ToIP) Task Force on TSP. The main points of the presentation and ITDP are:

- Introduce a Reference Architecture view on how to see Stacks, Subsystems and Protocols among them.
- Model the goal of supporting different Identity Systems that interoperate with each other as the abstraction of Endpoints and Supporting System, and agreeing on the minimal capabilities to be contained in a Trust Spanning Layer.

- Wenjing's main objective is to convince everyone that the goal is interoperability and to achieve this goal, we need a minimal set of functionalities - and that minimal set is Verifiable IDs and Authenticity.
- Verifiable IDs = (1) By a verifier or Relying Party (RP) an abstracted or generalised method to cryptographically verify the ID, (2) An abstracted or generalised method to appraise the trustworthiness of the ID's Supporting System (the base of trust) with respect to its context of the application.
- Authenticity: Authenticity of the parties in a communication is the foundational minimal capabilities needed in TSP. With authenticity, other trust functions such as confidentiality and privacy can be built on the top of TSP as a higher layer protocol/function.
- Wenjing went through 3 examples of how such a system may work in practice:
 - Example 1: Aries DID, VC, and DIDComm
 - Example 2: KERI AID
 - Example 3: OpenID OIDC
- In conclusion, the Trust Spanning Layer protocol should be the Inter-Trust Domain Protocol (ITDP) - where the goal is to enable interoperability between different trust domains who can all support authenticity.

For more information, here is the link to the presentation slides:

<https://github.com/wenjing/Inter-Trust-Domain-Protocol>

And discussions in the ToIP TSP Task Force:<https://github.com/trustoverip/trust-spanning-protocol/discussions/25#discussioncomment-5625476>

When Browsers, Wallets, & Federation Overlap

Session Convener: Heather F

Session Notes Taker(s):

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

- Heather: How can browser be more involved in the login/logout
- Tim Cappalli: 3rd Party Cookies, Link Decoration, re-directs, and using pass-keys for browser assisted UI/UX for login in a privacy preserving manner? And how to get to a multi-wallet world. Any app that can hold a credential can surface it for identifying/validating/authenticating you. Given they all have similar privacy impacts we wanna tackle them all at once
 - Pass-Keys are furthest ahead and have best opportunity to scale
 - Imagine a world where creating a new account on a site no longer means filling in the same data over and over again but instead pulling user attributes from multiple places
- Heather: Usually people think of the commercial web, but it's not the only use case. There's also R&E with thousands of IDPs, all valid for any RP/SP. The goal is not to replace anything, but to instead compliment things in a protocol agnostic way.
- Tim: and finding a way to get these worlds to mesh would be ideal. There are people who wanna get rid of SAML, and many SAML cases could be solved by verifiable credentials as a way to move away from SAML over time. This would make users more comfortable with the technology
- Nicole: During the FedCM Hackathon we hand waved over the idea of “proxies” in favor of focusing on protocol translation and assert parts of that identity into the process
- Vittorio: Sounds like there are 2 main aspects. Browsers are trying to protect users who don't know better, but at the same time there is a challenge in balancing how do we help people without being patronizing? In many business contexts, being able to run business logic is paramount. It's hard, it's the problem of pushing things to the edge versus getting deployed right away. Trying to retrofit what we already have could also create more work
- Nicole: +1 to the business rules. We have a rules engine with thousands of lines of transforms to the level of detail of checking for xml re-encoded escape in formatted strings. We don't want that level of detail.
- Tim: the goal is to give users enough context to make decisions. We don't want to baby everything, but there are ways to abstract. I don't think anyone is trying to replace business logic.
- Vittorio: You can tailor what to include based on the audience and they can be calculated on the fly. If you need to do something facilitated by the browser this will change the landscape of what is still or newly possible vs no longer possible. We have a responsibility to explain to users what is actually happening.
- Nicole: There is a cost from change management standpoint where small slow pieces of the structure can become slow but mandatory pieces of what make the infrastructure work.

- Sam Goto: I feel like Flash, like 3rd party cookies, are examples of how we can deprecate foundational elements as needed. A lot of the use cases I see for wallets seem to be along the line of academic credentials.
- Tim: SAML is widely used because it has been implemented and there is no better solution
- Sam: Do people generally acknowledge we want to move away from SAML?
- Unanimous “No”
- Nicole: if we plan to change we need a target to change to and a set of profiles we can move towards over how long.
- Tim: the value add for getting to VCs is a little higher
- Justin: It’s true that if you try to improve, even if it isn’t better, people can still choose not to adopt. And success may only come where the behavior stands out most. I don’t agree Verifiable Credentials (VC) is the target, but Don’t try to re-invent SAML. the pattern I usually see is using SAML inbound to OpenID
- Martin: I have customers who can’t upgrade from SAML because they still use RackF.
- Vittorio: Apart from Governments, every profit driven actor needs clear motivations to move away from the status quo. For instance if OpenID does everything you need better and easier than what you currently do, the cost case is in favor of moving away from the status quo because the change is better. Once we have an infrastructure (ideally aided by gov) then we will have a more usable technology that will be easier to adopt.
- Tim: LinkedIn has tiers of verification ranging from just email to actual VCs
- Justin: it’s harder for people to join sAML federations because they are so brittle
- Vittorio: User devices are an opportunity to make these large scale portable IDs usable.
- Justin: I think something people get stuck on is this common set of use cases. When we 1st brought out OAuth, we would talk about having photos on 1 server and printer on another and don’t wanna need to share passwords. It is not what OAuth is for, but it had the advantage of not being so tied up in other things that other people couldn’t chime in with a different technology/solution. The point is the nature of the presentation and verification is just an example, I am not seeing a drive toward any case that leads to the cutesy general example.
- Eric: Let’s say I, as a VC holder, say I want to claim I “created” something. How long till we can do that in a browser. Non-repudiation of actions. Where we struggle is as someone without a Cert, how do I sign my work? Would VCs solve that or would DIDs?
- Nicole: I think the problem is key recovery, how would a novice deal with this?
- Tim: We can use VCs so that we don’t need to create account to assign temporary ephemeral access to an account. There are strong cases for longterm access via proofs, and permanent non-repudiation
- Vittorio: but even then this VC sharing is a form of federation. They can co-exist but at some point the value prop of what’s new has to be significantly better and different.
- Justin: Taking a step back, I used to work in Social Computing, and I think an important thing to realize is how history mis-represents the growth of the internet. Facebook didn’t “beat” myspace, it’s just that the later contender started from a different place with the advantage of choosing what the predecessor did well and choosing what it wanted to do different. This didn’t just change the value prop but also adoption because of how it captured a larger/overlapping audience. If a new technology is to supplant an old one, it will be by solving something old along with something new.

- Heather: I agree there are many paths that can be taken, but at the start the browsers need to solve for all of them. So what is the common 1st step for VC/Wallets/Federation because that's what the browsers will need to do So something new can happen but old things like SAML can be supported?
- Sam: At some point there is no one other than me who can sign/create credentials other than myself. Many entities are moving away from federation and towards VCs. I believe there will be data sources that will be exclusively in a wallet or openID architecture, and if you wanna query in both sources it can't always be verified. Gov IDs are high assurance, but how do you have authority.
- Cameron: I think you are referring to authoritative sources and source mixing
- Vittorio: I agree with Sam. We may need to break out the business cases to not be a problem for the browser/wallet but for the person needing to solve it.
- DW: the big diff for me is there is a bi-lateral agreement where you as a dev are agreeing to certain terms. But for VCs this becomes more of a trust framework for how do I know the source of data is not fraudulent? Are you taking a standard route to making a decision or are you arbitrarily accepting credentials that may not be as authoritative.
- Justin: An important aspect is that people providing a credential and doing enforcement are the same. The gov can't fault someone for using a gov issued credential. Also wanted to point out we are slowly moving the discussion towards personal data stores. They don't exist, they may never exist
- Tim: As part of this initiative, no one wants to displace what's out there. There's 2 new initiatives, FedCM, and MDoc incubation projects. We want to make this 1 working group under 1 API, that is the goal. Consolidation is best
- Cameron: +1, uniformity between browsers is important for users to have a consistent online experience
- Lee: These Android APIs need to be similar to the others so they are not a unique API working in isolation. We are under a huge amount of pressure to build these quickly. EU is rolling out MDLs and forcing platforms to accept this. Soon we will have most credentials on our phones that can be accessed by APIs. Need some regulation around age assurance, becomes a logical conclusion to prevent these things. We need to get to a stage where the browser API will be in a state that it matches the native API so there isn't a whole bunch of work needed. Platform APIs don't have a sense of original trials, so we need to get a point of parity in 12 months.
- Heather: I think the idea of a working group makes sense traditionally, but the biggest negative is traditional development takes time
- Tim: We need a WG by Q3, so we can start building alphas or experimental APIs.
- Lee: we have the EU/US knocking on our doors saying we need to be able to use these VCs
- Tim: and if we can merge all this into a WG then we have coverage.



James Monaghan ID+ 🏃 + 🎉 @james_monaghan · Apr 19

...

We decided that solving decentralised identity is more of a marathon than a sprint 😊 #IIW #IIWRunners



James Monaghan ID+ 🏃 + 🎉 @james_monaghan · Apr 19

Good morning @idworkshop #IIW #IIWRunners! Looking forward to seeing several of you for a gentle and inclusive jog along the Stevens Creek trail 🏃. As a reminder, we're meeting at 6:45am at the Central Ave trailhead: goo.gl/maps/kbY3t3HML...



13



815



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

SESSION #6

KERI for DUMMIES & Non Technical People

Session Convener: Timothy Ruff

Session Notes Taker(s): ?

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

Great Organisational Identity insights in The Changing Digital SSI Landscape

Open wallet Foundation “101”

Session Convener: Daniel Goldscheider

Session Notes Taker(s): Jin Wen

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

[OpenWallet Foundation \(OWF\)](https://openwallet.foundation/) <https://openwallet.foundation/>

what it is NOT:

- not a open standard body
- not creating a wallet

focus on the meat of the burger, where the bread is standard and the top is wallet

focus on open development experience, not necessary open source

Introduction of Linux Foundation as OWF is part of the Digital Trust initiative

LF is a 100% volunteer led development organisation

OWF welcome contribution from open source or close source

Proposed Initial Building Blocks

Members have already expressed interest in contributing resources for these initial building blocks/credential types (based on the EUDI wallet as reference point):

- Payment Tokenisation ([EMV Tokenisation Specification](#))

- ISO mDL ([ISO/IEC 18013-X — Mobile Driving License](#))
- W3C Verifiable Credentials ([W3C Verifiable Credentials Data Model v1.1](#))
- Anonymous Credentials ([AnonCreds Specification v1.0 Draft](#))
- ICAO DTC ([Digital Travel Credentials Technical Report v1.2](#))
- Authentication and Verification

Compliances and Best Practices for tokenization per ISO and W3C standards.

OWF is focusing on interoperability, strong community to compete with large players

There are NOT going to be a single digital wallet. but OWF

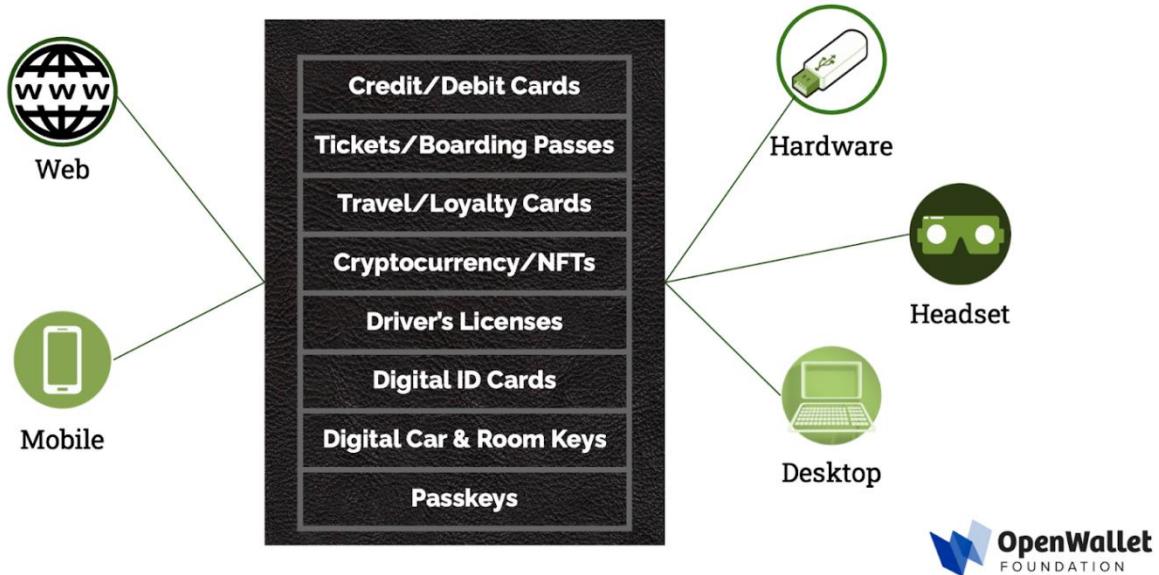
For example: Google open share the mDoc code for ID wallet

OWF big tents?

- EUDI (26 mln for referenced implementation)
- AAMVA

What will be common
identity of the holder

Digital Wallets serve many purposes



A perspective of solution architecture, how to build wallet based on the W3C VC standards

CTA: all the developers of digital wallets are encouraged to join the

Transcripts:

[Inaudible] >> And Rook, whether it be a court though, by security law.

>> Ah, thank you.

Yes.

I think IDEDI was going to be able to prevent security laws.

>> So if a lot of you are looking at the code, hopefully we can prevent them.

But you're totally right.

If there are security laws, hopefully we'll have a very that is able to address those security flaws more.

Now, the browser analogy only goes so far.

There is one thing, at least one thing, that we really want to do differently.

When you think about the Chromium project in terms of open source software, this is clearly dominated by one company and the name Chromium can't get to the way that that company might be.

The same is true for WebKit, which is the direction of open source bandwidth that Apple is using.

And of course, Apple is heavily influencing WebKit.

And this is something where we wanted to do things a little different.

We are trying to marry the open source model with an open governance model.

And Art is going to speak a little more about that open governance model at this moment.

But just like the browser model, we are trying not to be one thing.

We're not trying to be king makers and stand here and say, "I don't know, verifiable credentials are good and end-on-credits are bad," or vice versa.

We're not going to have an opinion as to big problems over open ID for verifiable credentials.

We're trying to bring developers together and provide a neutral home around the project that you care about, whether that's car keys or home keys, zero knowledge proofs or idle pass keys, and help create a need for those problems.

Initially, those projects are going to be very diverse.

We'll end up with different programming languages, we'll end up with probably folks who have very different ideas as to how privacy and security should be handled.

Over time, our hope is that projects are going to come together and maybe work together.

So even if you and I cannot agree on the perfect credential format, maybe we can agree on focusing on a couple of programs.

Maybe we can agree that a lot of us need access to the secure endpoint for the NFC chip and we can work together.

With that, I'd like to turn it over to you and both of you.

- Sure, yeah, absolutely.

So this generally goes for all of the projects for the Linux Foundation, not just OpenLOL but certainly OpenLOL as an example for this.

So everybody here is familiar with open source and I probably don't need to sell you the benefits of open source, but there are lots of granularities within open source itself, right.

And so what I like to distinguish is between open source code and a full open development experience.

What we really wanted to open is a button to develop a wallet foundation and what we're going to have is open development.

So, let me maybe explain a little bit about this.

If I'm just a company and I'm just building a product, I can occasionally push my code out and you say, oh, I've open sourced this code.

And maybe I've given an extremely restrictive license so you can't use it if you want to put in something else, but you know it's open source, right.

This is not what we think of when we think of open development and open source development.

So what we mean is, you know, participation is open for anyone.

So anyone can join the project.

All of our meetings are maximally open.

We try to be as transparent as possible.

There are very few meetings that are not completely open and transparent to anyone.

The only ones that I can think of off the top of my head are budget issues and security vulnerabilities.

Those are really the only meetings that anyone can join.

You probably understand that.

So, you know, again, anyone can join, anyone can participate, and anyone can rise to technical leadership goals.

You don't have to be a member of the Open Wallet Foundation to participate, to contribute code, to become a maintainer.

You know, even necessarily, you know, we have, you know, elected technical advisory council slots that, you know, anyone can rise to the top.

So the key thing is about open governance and open participation.

So I hope that summarizes this.

I'll give it back to Stanley.

So, you know, we're part of the Linux Foundation.

The reason we're part of the Linux Foundation is because the Linux Foundation obviously has a lot of experience in bringing developers together and having an open governance or an open development model to your concerns and all the other things that you're talking about.

(muffled speaking) There are a couple of things that we do a little bit differently.

One, we have a very strong focus on nonprofits.

We've launched with what a foundation with 20 corporate companies, some very large, some very dedicated smaller carriers, some of which I see here, which is amazing, as well as 20 nonprofits.

But we also have what we call the Government Defiance of the Beauty, which we've created, we've copied from ICANN, the Global Deming System, in order to give the public sector a seat at the table as well, because we believe both more credentials, as well as for wallets, this is truly something that ideally we should do together.

Even if there are competing wallets, especially if you're competing one extent in the computer.

If we want a healthy ecosystem, we should come together and we should create all the source components together.

And then, yeah, can I put you on the spot to talk a little bit about the Linux Foundation and how you are bringing these together and how you are not just doing Linux, which when I started talking to the Linux Foundation, I thought that was it, but there's so much more going on.

- Sure.

And if you want to come here, anyone who's sitting on the floor, especially almost, you can see some of the kinds of doors.

Yeah.

And I see it for sure.

So for those of you who don't know the Linings Foundation, for the last 20 years, we have basically been building open source communities that are both private and public sector developers from all works of life.

Obviously, it's the biggest project in the Linux kernel itself.

We do also host projects like Cloud Vayner Computing, which is CNCF, which is where Kubernetes sits.

And over, I would say, the last 10 years, we really have diversified the kind of open source projects that we bring into the Linux Foundation, including Automotive-grade Linux.

If you have an automotive operating system, it probably runs on-- it's a derivative of Linux, but Automotive-grade Linux.

We have the Academy Software Foundation.

So a couple years ago, the developers that were building 3D rendering for filmmaking were like, why are we building engines competing with one another.

We're not software engineers.

Same thing with the automotive industry.

We're not software engineers.

We want to build and use the best software there is so we can focus on what we do as an industry.

So the automotive, automotive grade Linux, as well as the Academy Software Foundation, Now build open source code projects collaboratively within the Linux Foundation, and very importantly, under not just open source licensing, but open governance, which Hart hit upon.

And what we at the Linux Foundation are really focused on is making sure that that governance model in open development and open governance and decentralized development is core to every single project.

So we have things like technical oversight committees or technical advisory committees depending on the projects and how the governing board wants them in the structure that are not necessarily telling the projects themselves to be, to tell them what to do, but making sure that these things are healthy.

So I'll give you an example.

So when we talk about code projects specifically, and then we'll talk about standards and specifications of the LFNEA as well.

When we talk about code projects specifically at the Linux Foundation, What we envision the Open Wall Foundation in as many of the other projects at the LRCRCF has the Kubernetes, biggest one of the biggest open source projects in the world.

It also has a hundred and eight, 150 other projects that are complimentary or competing with Kubernetes within that community.

Each project at Hyperledger, for example, we now have part of the number today.

(laughs) - 15.

- 15.

- 15 active and incubating projects and 50 different labs within the Hyperledger Foundation.

those have project maintainers.

The maintainers of all our open source projects are the queens and the kings of their projects.

And it's very important for the structure from a governance perspective, the Lennox Foundation, for the maintainers themselves, the developers, so if you bring code into the open wallet foundation, for example, and you are a company and you have a, or even a government agency and you have collaboration already, the place to bring the code in, you are going to maintain your own governance of how you run that project.

Now you need to adhere to some of the projects governance models and you need to, for example, do quarterly reports to the technical advisory committee or the talk.

And we as staff help support making sure that these are healthy communities.

And we have lots of great tools at the Linux Foundation including data analytics tools and just deployment tools to be able to manage those projects.

And we also, because the Linux Foundation is so large, we also have great resources around licensing and legal operations and events.

So if you go to a Linux Foundation event, we have an events team that not only supports LF project events as well, but other industry events.

And that is a great way to build developer ecosystems through it.

We have marketing teams that help promote at the developer level, at the projects level, and at the actual foundation level, the projects themselves.

The key is that our members, so the paying members that support these different foundations, are basically pooling their funds together for the Linux Foundation, very importantly for the maintainers themselves, to be able to focus on what they want to do, which is build good, what I call enterprise grade, meaning that you can go to a government in an example of open wallet foundation and say, "This code has been built with security," I don't know who mentioned security, "with these two security requirements, "and here is how the projects are governed.

" So across the LF, we're calling a session later on this afternoon to talk about the different projects that are at the LF with what we call digital trust initiatives, open wallet being one of them.

And then a couple years ago, the Linux Foundation also started working with specifications and standards.

We have the Joint Development Fund, which is part of the Linux Foundation, and there, Trust Over IP, we have Judith here who's the Executive Director, and DIF, the Decentralized Identity Foundation of Claire is sitting there on the floor.

And those groups are also part of the LF.

And what that gives us the opportunity is, very importantly, and you hear from Hart and myself, and many of us at the LF, we are very interested in making sure that our developer ecosystems are not fragmented.

We want to make it as easy as possible for companies, for developers, for people to do two things.

One is understand which projects they should be investing time and resources in.

And number two, making sure that when you have to work across different projects, and that's the reality, it's just gonna be that's the way it is, that you also don't feel like you're fragmenting not just the cost of joining as a member, for example, of these foundations, but very importantly, the cost of the developers.

We are a volunteer, or every single developer, the Linux Foundation does not have engineers on staff.

We do not contribute code to any of our projects.

We have engineers that build our platforms and stuff like that, but we do not have engineers that contribute to projects.

Everything is volunteer and through members and non-members contributions.

It is so important for us in this critical time around digital identity and things like open wallets to make sure that we're aligned.

And that's part of what we hope to do at the LF.

So later on, Satya will talk a little bit more about that details.

Did I cover the one.

- Thank you very much.

Before we get into calls, trash.

- Any questions.

- Or any concern.

- There's also a lot of items we'll talk about.

[Inaudible] Sure.

[Inaudible] So we would love to help developers to increase the scope and that's all the philosophy and the speed of the developers (inaudible) I'll say that the real value add to the mixed foundation is when you want to collaborate with someone else.

If you're hosting a project, you have total control.

It's pretty hard to convince me that I should work on your code.

If you're in GitHub with your code, you could take it away.

>> I would say there is a journey here.

If you have code today that is not resource, but you think it would make things more responsive, I want to convince you that we believe resource is not.

If you already have resource, and you are one company or one entity that completely controls that, We would like to convince you that it may be a good idea to work together with other entities on that open source board.

Now, if you're already on level three, so you have open source something, you're working with other entities already together, the last thing we want to do is compete with or approve anyone else.

There is an open source community.

You're working together on something.

You're happy with that community.

The Open System Foundation is not trying to steal open source projects away from our organizations.

What we are thinking is that the Open System Foundation may be useful because we're trying to steal a big pin.

At an end, not just allowing zero knowledge proofs or just allowing tokenized credit cards or heavy cards, or just a boom key, or just card keys.

If you see some value of bringing people together, whatever the meaning is, if you are doing something in the wallet space, hopefully, the open wallet foundation will be an interesting part.

But if you are, if you have already an open source project and you're happy with your community, don't feel that this is, you know, a part of the whole view from the internet.

- If you need to, if you need to take a look and then I'll call the official, what we want to build a wallet today.

And I mean, we had a session yesterday about, for example, the items.

You centralize that entity is getting mainstream.

And you want to build a really competitive wallet, we basically got exercise with our biggest company last year.

And we realized, we want to build a really, really competitive wallet on all major, all that stuff.

It's gonna be really complex and it's gonna be really expensive because there is not that project I can just use.

The decentralized identity space is totally crashing.

I called a session, Spring IOW, last year.

What's the best financial point.

I think Daniel Cole and Kristina yesterday gave a session about that.

The result was we got approximately So if you want to have a wallet that has copies and entity data in an instrument, there is no technical information on that.

The open source protocols provide an evaluation trial.

And that's what we want to be on.

So people that join forces, and as you said, combine their funding, because together we can build immediate accident components.

That's basically the one that's here.

And we talk to developers, we talk to other small projects, and we hope that they will come and join us.

On the other hand, we are also trying to come up with ideas for projects, because they are all emerging standards like SD-Job.

And perhaps we can build a community, we can also build a certain profile of protocols and credentials.

And I do that as a open-body for the question, because it's here.

It supports open development, and so on.

So we think that's a great opportunity for us to really build growth rates on the news for the central center.

Okay, I think if we don't, we also see a downside here.

You know, from a consumer perspective, I have a lot of credentials, I have a lot of cards, but I have one more.

here carries more than one physical order today.

Very few people, right.

It's always-- Physical order.

So it's-- I think most people-- We need to talk.

[LAUGHTER] Most people, if I were to offer you a water, then you like the color and the fabric and the design.

And then I tell you, oh, there's one thing you should know.

This water works just for your drug.

Nothing more.

By the way, just with one standard for your driver's license, you probably asked me what kind of wallet are you trying to sell me.

So we're not saying that there won't be specific use cases where you might want to have a wallet just for one type of credential using one type of standard.

We feel a lot of folks out there will want to have secure multi-premise products.

And that will make it very, very costly for individual companies to create these wallets.

Because it's expensive to buy.

Most of you probably are in wallets, but you know that it's expensive to create a wallet, even around one credential partner.

If you want to create a multi-purpose product and compete with the best and the biggest neopharins out there, very few entities we believe are going to have the funds to do it.

So for anyone who is with the trillion dollar companies here, we believe that this is really crucial in order to compete.

And even if you happen to represent a trillion dollar company, and we hope to announce one soon, we believe it's very good news because it makes a lot of sense for the largest companies to work together with other developers and the public sector in order to create a foundation.

Yeah, I was just thinking about this idea of open walls.

So let me give you a session just to re-enter and to review my opinion.

I think it's also important for us to think about there will be open walls for the market.

I, as an individual, can go around with my store, my retail, my buyer.

But there will also be organizational wallets where I really don't have any self-sovereign identity, where I'm being delegated authority by my employer.

And there's a perfect example.

We're a formal flight definition on what kind of leads to the one given by my employer and the one given by an ITU to be used when we're not going to work.

- But we're not trying to say that there will be even the one that-- - No, I'm gonna wanna pick the first point that distinction that we made for it.

- I think what this really proves [Inaudible] able to build their products and their solutions.

What are the pieces that they need.

There are projects or there are open source projects that are in the end.

You can take one component.

You have to use the whole side.

So we want to overcome that limitation.

And if people that build their product functionality into a app, if they have multiple components for it.

I mean we will see how it goes, right.

We had a discussion yesterday about that data.

[Inaudible] - Oh, well, I wanted to ask a \$64 question 'cause first you started Daniel with, we want different projects and they can bring their own code and they're the queen or king of their own project.

But I think the ultimate goal is to have some sort of engine that allows so that you don't have to have more than maybe the two, the organizational and whatever, the wallet.

How would you see that collaboration going from the siloed, We know that people have some religious opinions about how certain things could be done in this community.

How do you see that working in the Home Willows Foundation.

Because I hear two sides, and I want to know how we get from siloed, I'd say to come here and bring my project, it's not going to be touched, versus, you know, we want to get these comments from them.

So I would say that this is going to be.

The only thing we know for sure is the light is starting to work.

The next one is the open source project.

Either already is open source and you're looking for a neutral home for that project, or you have code that you think about open sourcing and you want to do it with others.

We hope that the Open Water Foundation is going to be a good home for that project.

We will work very hard to make it a good home for this project.

Everything after that, I think, is a journey.

If you come to the Oak Water Foundation and you're interested to work with your co-pays, and you're not interested to work with anyone else on any other question, that is your choice.

No one is going to force you to talk to any other project.

I'll hope that some of the projects will start to develop trust, because they are part of the same effort, because every project is represented on the TAC, the Technical Advisory Committee.

So we will foster communication between the projects.

And our hope is that this communication is going to be beneficial.

If you, at the end of the day, say, "You know what, I have my credential format.

"I don't care about anyone else "because I have the truth and nothing but the truth.

" Again, that is your choice.

We believe that for many projects, you're going to see opportunities that maybe open-blooded foundation can broaden the appeal because there is something that you work on that may be very useful and very helpful for another person.

And that this bringing people together is actually something that is quite obvious.

- Yeah, so Junivel coming up here.

So in practice, we typically see a lot of people contributing code and then they start to realize that they have things in common.

Maybe, you know, maybe Torsten's doing something his code base that I have something similar, but he's doing it a lot better than I am.

And the next time I really want to upgrade, I can just say, well, it's easier for me just to switch my API into a question module than to use my own.

So, you know, we really expected to see a lot of coalescence and sort of collaboration and concurrency.

And in some, you know, a great example of where we have some instances in hyperledger and blockchain and interoperability where we've had sort of three projects already come together in form one and we're expecting to see sort of more people merging in.

And it's just exactly this.

They realize they're doing something similar and in the long run it's much easier and much more efficient to work together than to do your own thing.

And this leads to this sort of mass project that we're going to be working with.

But the last thing we'll do is force marriages.

There is not going to be any force marriages.

- Yeah, I want to add that the husband mentioned earlier about modularity and also, you know, there's a diagram we have in the upper water foundation which has a block with lots of different standards.

I thought they do access in this.

But on the side are many different platforms.

You can have mobile phones, mobile phones has very different operating systems, have different instructions in it.

And then people may have different IT devices, cloud version of them.

There are a lot of these things, I think, whatever quality thinking about, you're gonna rely on those as well.

And those are not easy to do.

So designing a particular IT system, if you want to, make that IT system available to, you know, people of various, I think it's another challenge, right.

and being in the Uponwawa Foundation together, chances are some of the projects have done really good work in those areas, and that we can leverage each other's strengths.

So I think that basically the modularity comment and how coming together is a winner for all of us.

So I think the first question was here, here, and then here.

I think you were the first.

- Okay.

- Yeah.

- So.

[Inaudible] >> Yeah.

And you know, I don't want to be hung up on that open-robot information.

It's not saying that we need only one robot.

What we're trying to say is that we believe there will be a need for many people in many use cases, those wallets that will support different financial formats and different programs.

And even within one financial format, we believe it makes a ton of sense to work together.

But certainly, when you're interested in the wallet that combines two or three or four or five different use cases in different parts of the world, the European Union has its ideas on what the right formats are.

Canada has different ideas.

The Department of Homeland Security has ideas.

It will take a long time, if ever, for the world to agree exactly on one system.

So we believe that it makes all the sense in the world to bring people together to work on interoperable components that we can fix.

If you want to start reading, I just want to add to what Daniel just said.

In the end, it is right.

It is not-- it will need it.

[INAUDIBLE] >> We have a number of existing models, OEM models, they are both Android, Samsung, and K, and I find they're different, but they don't model.

Now, and those are, from a user perspective, they are usable, they work great, and for these entities, from how much it works pretty, that makes sense, it's so much great, it's viable, and it's widely accepted to, accepted to use there in the market in the ecosystem.

So what is the long term value in getting an open wallet over a build when all these existing wallets work great, widely accepted, consumers' wallets.

So what's the-- from a user perspective, what's it there for me.

And from a commercial perspective, Why do I really need to care about the open world.

- I think it's a very, very good and very perfect question.

So we don't have a crystal ball, right.

None of us know, and I don't claim to know that.

We understand the world landscape in two years.

When you look at the browser world again, in the browser world, there are open spenders.

There are shared open source projects, like the Blink project.

And even with the Blink project, It's not like we have a thousand web browsers that are important.

Maybe the wallet space develops like the browser space.

Maybe it lasts for over ten years and you have three or four or five or more people that have 80-90% of the data.

Even in such a world, I would argue that a strong community that builds open source components together is in the interest of everybody.

Even if a few large players dominate the market, you want an opportunity for other players to compete in order to keep the large players' minds.

And maybe the wallet space is going to develop a little differently than browser space.

Maybe wallets actually are things where you have different commercial interests.

So we have companies that are using their position in the wallet space to extract money out of credit and debit card transactions.

We have other companies that are trying to extract data out of the transactions.

I think a lot of companies, both on the potential side as well as on the very fire of the line party side, have mainly a defensive interest.

They don't want to make money with the wallet necessarily.

They may not want to make money by selling credentials or selling data.

But they are interested in the wallet space because they don't want the two horse race or three horse race where a few large players are extracting value from that.

We are seeing tremendous interest.

We have over 300 officers that told us that they're interested in open wallet.

Something that took us completely by surprise.

None of us thought that this was going to happen.

And I think what all of us here, how many of you disagree on prevent performance or protocols, how to share them, is an innate desire not to have a few companies trying to monopolize the space.

- If there is a solution architect.

[Inaudible] and not aware of any of the thing is in that education sector as well.

If you do test, it's so fragmented, right.

And for to have a wallet, a common wallet that caters to that education sector as a whole, where you can bring in all these credentials and do it.

current status of F.

It doesn't look practical.

The current status of F.

I just want to give you an impulse, right.

You asked why OWM.

My answer is, in the major wallets you're unable to deploy your credentials.

I just choose education more or less.

Yeah, you can use any other domain.

So, the major of the major of the major is just [Inaudible] If there is no acceptance for that wallet, it doesn't make any sense.

There's no point in having a great wallet if nobody accepts it.

So with this new wallet we opened, how do we get to a state of acceptance and get the commercial.

It's got to be commercially viable.

But it's not from all of this, actually, the credentials.

Yeah, I mean, of course.

Yes, the credentials that resides in the wallet.

Just to ask your question.

the Apple wallet or Google wallet.

They do that a lot today to put anyone's credentials.

Like, is that the same, correct.

Well, I mean, you want to mention that a specific company or-- Yeah.

So I just want to throw in that, well, you know, there's clearly opportunity for horrible fragmentation and terrible user experience.

[INAUDIBLE] To make it clear, there will not ever be a single wall.

And for a whole host of reasons, one, you talked about the big platforms.

Well, guess what.

they don't share well across platforms.

So you get locked in the ecosystem, which is a big problem.

You have data and credentials.

There are enterprises and governments that don't want to depend on those same providers to do account recovery and credential recovery.

They want to own and protect that.

You've got hardware wallets that need to be able to plug into these ecosystems, right.

Which provide a whole level of other features that you're not gonna get with the one built into the platform.

So these are all very real use cases.

So as a minimum, you end up with like two or three.

You're a generic one for all your end users, your corporate one, and maybe a government one.

This is why I think it's important that people understand that there will absolutely be more and more.

- Wonderful.

I mean, we see it today that I don't think that's gonna change either in the near term.

And plus, there's got to be hardware dependency for any wallet that people, there has to be a bank.

And getting access to some of the hardware features is going to be, I mean, time will tell you if that's practical or not.

- Yeah, and I think this is probably one area where even if you and I disagree on what end performance, we probably have a similar interest when it comes to the situation.

- Yeah, there's a hardware, the hardware.

I think whether it's European Union or other multinational or individual governments, I think there is going to be an impact to create something together.

Is this a magical solution to prevent a solution or a reality from the two or three companies dominating this completely.

No, and we want the open-water foundation to be open to everyone.

And I wish David was here from Google.

You make the end of code available on GitHub.

I know personally, even we're using Google's end of code and we have more forward reference.

So I think even big players are sometimes very important to the idea of sharing open source components.

Even if they end up competing with other folks, and our hope is that whatever we believe the future will bring, the simple question for a developer at the end of the day Does it make sense to oversource and does it make sense to work together with others.

And if the answer to those two questions is yes, we won't document it, we're going to use Playwall.

I know that there was one question.

You have a question, Kevin.

Some of you had a.

Some of you are not Jewish.

So, come with me.

Then I think you were actually first on the board.

Well, actually, just one more quick respect.

>> That is one of the vendors who's been building wallets for ages and has tried to open one foundation because exactly of this reasons that Daniel's whole time ago.

So actually, building a wallet is a complex task.

It requires you to approach all these topics from various angles and getting something that is secure and has great user experience at the same time.

This is very typical.

And if you want to do more than one of these technology stacks that I've talked about today, you cannot do it all on your own.

Even if you're a large company, you probably don't want to do it all on your own.

So one of the key merits I see from all this is we can collaborate on something that is very much better than if we would do it all on our own.

And this is, I think, the message I want to give to people.

So we are very willing to not develop our own model anymore because of just the tedious tasks So we throw in our resource in that joint project so that we can have something that's better.

And if we are releasing the water in the end, we don't actually know.

So, but probably it would be too, like a stable core or a foundation code that many of us can release so that we have this duality and diversity.

So this is the vision I bring into this field and I hope others will see that too and join in.

- Because you were sitting here at jump, Jim, Digit was also a founding member.

Can you say something about why you are interested in this.

- Yeah, actually the first thing I wanna say, and the point is brought up about, well, just a handful of wallets everyone is using today.

How many folks in this room would like to see that be in the future of digital wallets.

Right.

Not saying they have to go out.

Now maybe that's 'cause we're all self-selected to be here at INLV, right.

But I would submit to you that the future of digital wallets has to be the dead opposite of what happens with browsers.

Okay.

Yes, if it's gonna take large companies, it's gonna be as complex of a job to build high functioning, very secure, practicing, respecting digital wallet.

I said that it's harder than a browser.

So if we don't want the largest companies in the world that already have, you know, coming times This conference is going to have the kind of asymmetric power, right.

We don't want that to happen.

We have to create an alternative.

That's what we're doing in this room.

That's what Open Wall Foundation is doing.

And the other point I want to make is, I think it's going to be unusual, I'm not the sort of project, I know I developed it myself, but I've worked around a lot of it.

I'm not the sort of project.

We have to develop a community here where we are coming together with code modules, contributions from many different places, many different projects, whose purpose is we need to solve this problem together, right.

We need to create this alternative in order, and we're not just talking about the success of our individual projects and companies, right.

We're talking about ecosystems and is there going to be a problem happening on the internet that our children and grandchildren can really count on.

I don't know about anyone else in this room, but I'm not really happy with the trust battle with the internet today.

That's why Jen's here.

We believe consumers-- and we're a consumer-facing company.

And they need the best digital wallet experience they can.

And they need to be interoperable everywhere.

What are the point, my mate.

No one yet has mentioned that the European Union as a group has said, we're not just saying our citizens need a digital wallet.

We're saying the member states all can issue them, they don't have to, but they're all going to do it, and they're going to interoperate across those 27 member states, and they fund it, at least provide half the funding for it.

One of the largest open source projects is gonna happen.

So this is industry basically saying, well, one government or one set of governors shouldn't be the only ones doing that, and one of the major topics on the technical architecture call this morning, right before this, was how are we going to collaborate, We agreed to set up a task force, by the way.

Any of you who joined that task force, how is OpenWallet and-- [INAUDIBLE] How are we going to not just talk to each other, but actually collaborate over the next couple of years so that that Open Source Code and the Open Wall Foundation source code can work together.

They're also looking for a long-term part.

And we hope that that becomes Open Wall Foundation.

So the European Union is spending 26 million euro on the reference code, which is also going to be open source.

But the question is, where is this going to reside afterwards.

What happens when the 26 million euro are spent.

Who is bringing the community together that is hopefully going to maintain that code and keep that code fresh and secure.

And we believe there are huge opportunities here.

When we launched the Openorg Foundation in February, Peter Holpin was on the panel.

Peter was very, very influential in the EU reference Two hawks, shout out to AAMVA, the American Association of Motor Vehicle Agencies.

They are from the get go on government.

Very different perspective.

US, Canada versus Europe, a driver's license versus zero knowledge proof focus.

But the idea of me is to build a big tent.

Because someone said religious differences.

Some of us here may have hard differences when it comes to religious differences.

But I do think that common core that we don't want this to be a reward to make, that we do want people to be-- that we do want this to be something where a lot of entities have a say.

I think this is true for all of us.

Whatever credential form, whatever protocol, you might be [INAUDIBLE] There was a question here, here, and then-- So just going back to the car in the wallet, that report, this car in the wallet has its own protocol, which you were thinking some sort of cash, some sort of money, some sort of car, transacting, whatever.

It's almost like those functions in APIs are not necessarily standardized.

What's fundamental to me all the time in the wallet is that it's over.

So the identity function of the model actually owns all these cars.

It's fundamental.

Maybe that's the common British, regardless of the protocols of each particular function.

>> Yeah, I think there will be a few things that we need to find JavaCon.

One is what you just said, you know, older binding, I think is where [INAUDIBLE] I think there are a couple of hardware components and maybe APIs in the operating system that we will hear about together.

And maybe we will hear about some, you know, some innovation of operating system, sorry, of programming.

So if you do want to mix and match different performance for And over time it should become easy.

I have one comment and then a question.

The comment is, you and I have a lot of conversations, and O is clearly about own creation, creating the energy.

And so from a standards organization perspective, that's why all those nonprofit standard organizations diff, trust over it, et cetera.

This is still where the standards will be developed.

And then the coding can be used against those standards, whether it be at OpenID, it's at W3C, etc.

That's why at SOPP, you were talking about user interface.

We always talk about common credentials, common everything.

No one really cares, at least my grandmother and my sister, about what kind of credentials they use under the name, but they need to understand that interface.

And so that's why in our human experience working with her, because we knew her well, we started interacting patterns working with task force to look at interaction patterns.

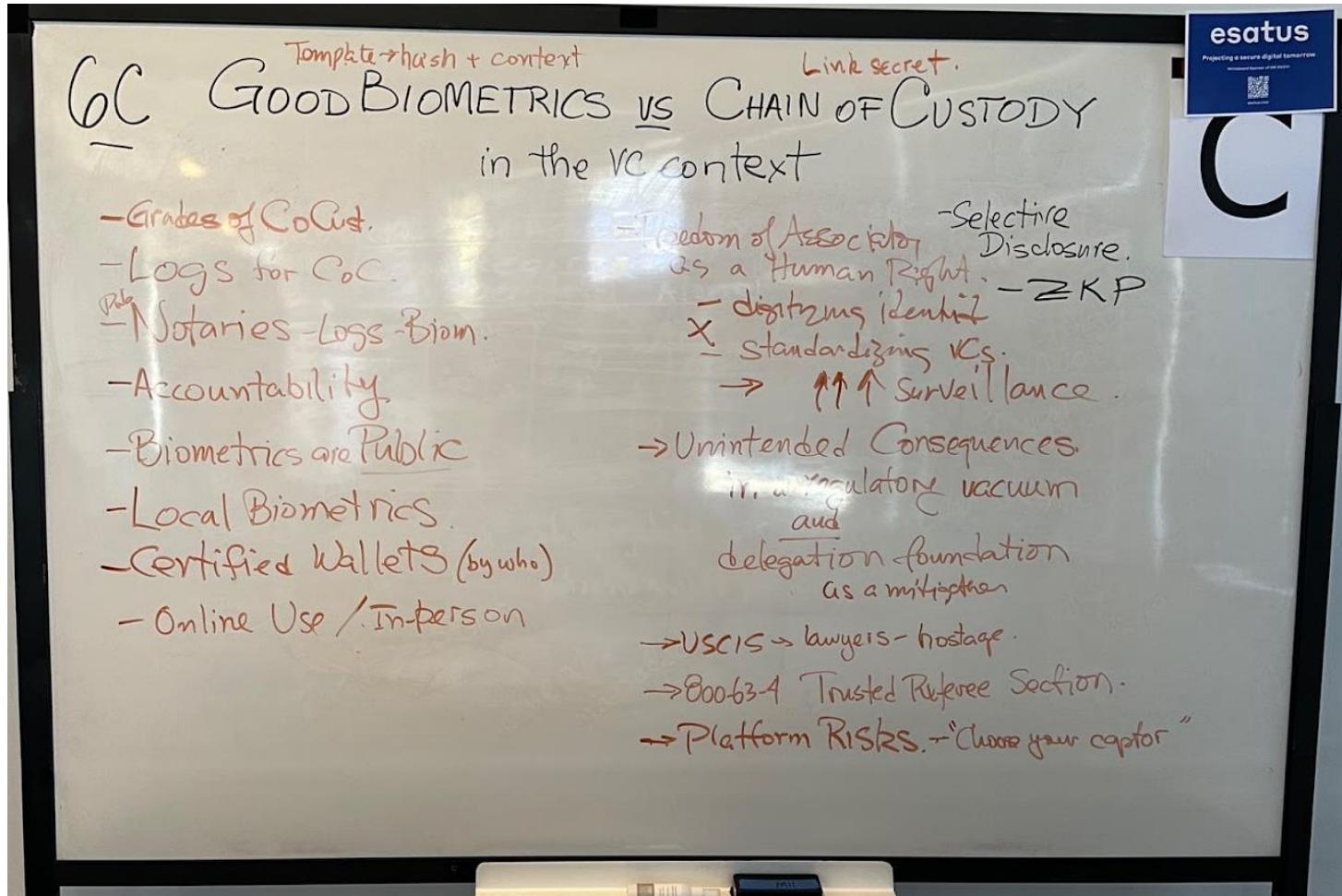
Good Biometrics vs. Chain of Custody in the VC Context

Session Convener: Adrian Gropper

Session Notes Taker(s): Adrian Gropper

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

<https://worldcoin.org/blog/engineering/humanness-in-the-age-of-ai>

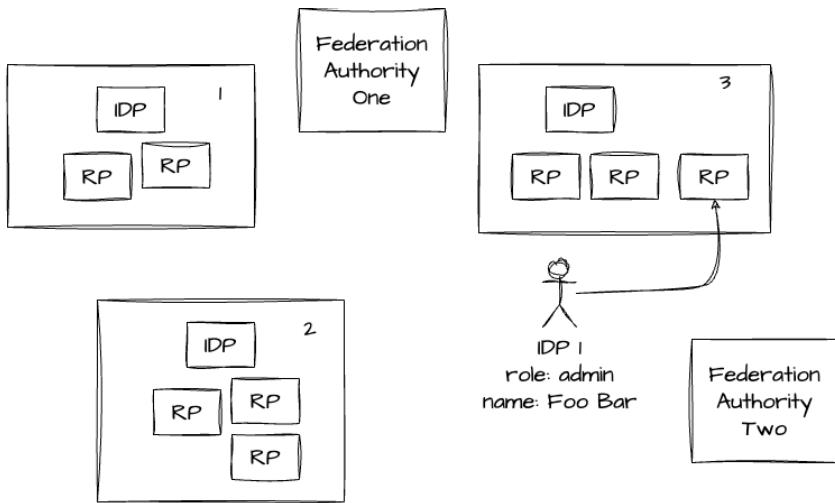


Detachable Federation Authorities

Session Convener: Justin Richer

Session Notes Taker(s): Mike Schwartz, Gluu

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



What do you do when a federated user shows up to a disconnected node?

Make a local account until you can reconnect to the network?

Do you burn (deactivate...) the account when the person leaves? You need an audit trail about what they actually did. We should design for the most common case: the identity a person asserted was true, and now that we're reconnected we can connect it. Need reconciliation post-reconnection.

If you mint a credential in a detached state, you can carry what attributes you gained in a detached state back with you.

Interfederation trust is a challenge because existing standards are either protocol specific (SAML), not final (OpenID) or don't yet exist.

Can we decorate the account: e.g. a local acct that accretes attributes about the disconnected context (and maybe not shared back to the home IDP).

Retaining attributes in the disconnected IDP is good for audit, but if any credentials (especially passwords) were created in the disconnected IDP, they should be destroyed.

When a person is added to the detached system, they are also authorized for certain "groups" or "roles". It may be important to keep these roles to show compliance with RBAC.

PIV Federation does not allow idp proxying—accountability is required for identity proofing.

PEOPLE HAVE MULTIPLE ACCOUNTS ... but can get the accounts to talk to each other?

Access Control Use Cases

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

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

ACCESS CONTROL

Alice shares with Bob
 $A(R,W) \rightarrow A(R)$

Bob uses that authorization (invocation) to access the service/resource.

But this is too simple.

The number one problem is this involves just one resource.

So, what if we have a copy that takes two resources

$\text{Copy}(A(R), B(W))$ replaces content of B with content of A

If we only had one resource, you can just specify read/write. But with two, its possible to confuse the two.

Deeper:

Let's say copy is a method on A
 $A.\text{copy}(B)$

Then, if Alice has authorization to do copy on A, she can execute.

But what if A,B are hosted at different servers.

Then the server getting the copy invocation will need permission to do the write operation into B.

So, an inadequate use case can lead you to a bad design. This use case gives an additional way to think about how you might manage authorization.

However, that's still not adequate. Because there is no result going back.

Proposed use case that covers all functions you need to support an object capability system.

Alice is using Bob's backup service.

$A \rightarrow \text{Bob backup}$

Bob uses Carol's copy service
 $B \rightarrow \text{Carol copy}$

But now Alice also needs at least read access to the resource with Carol.

Alice ---> Bob.backup(A) (includes delegation to read A)
Bob ---> Carol.copy(A,B)

Where does B come from?
If Bob creates it, then
Bob ---> Alice auth to read B

What if Bob never has permission to B? How do we get that through the network?

Without this nuance in the use case, you may never see the need for these features.

If you tried to solve this problem with ACLs, my paper shows you can get really strange results. For example, Alice getting permission to write something she can't read. That's crazy.

Some projects out there... I'm trying to get them to use this use case.
UCAN

Three sets of names: Participants, Resources, Servers, (and also then operations)

Using file example is limited, but easy to talk about because it is intuitive to most people.

Commentary:

One nuance is that Alice actually uses software, which has its own functionality, so it isn't Alice working with the server.

Yes, but all Alice needs is permission to use "her" device. That's often possession or local username/password, PIN, etc.

Bob doesn't care who. Just that it is authorized.

...

If we step back, say Alice is a person who uses some hardware that gives her permissions to use all of her programs. To get access to some files, she uses her "powerbox" to get authorization that she can give a program that permission to read or write, as appropriate.

This approach requires cryptographic secrets to sign the invocation.

Bob never needs to know anything about Alice other than that the authorization is properly invoked.

Paper: Solving the transitive access problem for SOA.
<http://www.hpl.hp.com/techreports/2008/HPL-2008-204R1.html>
Listed at <https://alanhkarp.com/publications/publications.html>

<https://alanhkarp.com/scoopfs/index.html>
<http://www.hpl.hp.com/techreports/2007/HPL-2007-105.html>

Q: What about sessions?

The capability is to start the session. Then bear

Capability

Unforgeable, transferable permission to use the thing it designates

There's a distinction between unforgeable versus unguessable. Bearer tokens are unguessable, but forgeable.

If you issues something to a public key (or DID), you can require interaction with the private key to create non-forgeability.

Q: But if its public key, you can't delegate.

A: What we do is create a second artifact specifying the delegate's key

Note: credentials are not authorizations. The use case are quite different.

Consider revocation.

For a driver's license, you don't know who might verify it

But for a capability, you do know the server where it can be invoked

The audit problem.

Researchers generating data sets. I want them signed that they validated it as a contribution. Twenty years later, you want to pull out the old data. And validate who actually contributed.

Access control:

1. Identification (physical being alignment)
2. Authorization (what actions is this person authorized to take?)
3. This program is running on behalf of person
4. Access decision

Capabilities don't handle step 1. They enable #2, which can bootstrap #3, and then #4 uses invocation

In RBAC systems, this role gets a set of permissions. That's 2 based on 1, then get capabilities, which when invoked allows delegation. In an auditable way.

Still: how do we know that identifier is associate with the professor?

Alan: These are important problems, but these are not related to access control.

We want a system that lets us use least privilege.

And we want to separate authorization step from access decision. Most systems conflate these two.

First, I authenticate and get a permission.

Second, I have a token I can invoke

Server can decide based purely on invocation

Difference with VCs

Primary purpose of a VC is to verify a claim about a subject

For capability is is authorization with respect to a resource

In a claims VC, you don't know who might be verifying

In a capability, the only verifier is the resource

Jurisdiction: The Missing Layer in the Identity Stack

Session Convener: Bry Benson

Session Notes Taker(s): Jonny Stryder

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

<https://www.amazon.com/Blockchain-Faith-Relationships-Resolution-Post-Digital/dp/1948956004>

<https://wikido.super.site/>

<https://wikido.super.site/principles-and-values>

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

Major points:

1. If a special jurisdiction is not specified by contract, jurisdiction will default to one or more political jurisdictions
2. Special jurisdictions can be set up and made enforceable as between any two persons, using contracts
3. Self-sovereign identity can include selection of special jurisdictions that will be enforceable in most legal jurisdictions as enforceable contract provisions
4. Mediation and arbitration need not use national laws, etc., as the basis for deciding a case. Instead, parties can use principles and social promises of their own choice linked to their digital identities.
5. Wikido is implementing a special jurisdiction between its members.
6. The Wikido jurisdiction uses three basic social promises of Integrity, Principle based conflict resolution, and mutual respect (non-hypocrisy), set out here:
<https://wikido.super.site/principles-and-values>
7. The Wikido principles map to the basic principles of governance set forth in the book Blockchain Faith as the basis for rule making without central authority

What's New with Hyperledger Indy

Session Convener: Char Howland (Indicio)

Session Notes Taker(s): Char Howland

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

Indy Contributors Working Group Meeting page:

<https://wiki.hyperledger.org/display/indy/Indy+Contributors+Meeting>

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

- Indy is a Hyperledger project that provides the tools, libraries, and reusable components for creating digital identities rooted on blockchains or other distributed ledgers
- Key characteristics
 - Correlation-resistant
 - Privacy-preserving
 - No PII on the ledger
 - Supports Zero Knowledge Proofs
 - Decentralized
 - Supports Verifiable Credentials
- Related projects: Aries, Ursa, AnonCreds, DIDComm

Value of Indy with the “Indypendence” of AnonCreds

- AnonCreds is ledger-agnostic
 - Users of AnonCreds are not tied to Indy and Indy is not a requirement for AnonCreds
 - This is great for interoperability and not having lock-in to a particular ledger
- If we don't need to use Indy, why should we?
 - Indy is still a great place to host AnonCreds, because it has everything you need
 - Assets need to be highly available
 - Geographic diversity of hosting
 - No link rot
 - Tamper resistant
 - Indy is great at providing these aspects, and is free from cryptocurrency concerns and has legislative compatible governance

Upgrade to Ubuntu-20.04

- Very close to completion
- The difficulty has been in the lack of a pipeline, so developing the pipeline has taken a long time but will make future upgrades much easier
- There is a Release Candidate that includes both Indy Plenum and Indy Node, each of which were built, tested and published using a modern, automated CI/CD pipeline.
- After completing the final release, the last step is to upgrade existing networks

- This work will unblock the rollout of the Indy DID Method

Roadmap Items

- Tombstoning
 - Mechanism to make objects on the ledger unavailable
- Overlays Capture Architecture
 - OCA is an RFC in Aries that allows for issuing a credential with information about how it should be displayed
 - Great for accessibility, user experience, branding
 - Support OCA bundles in Indy
- Indy Node Monitor for Stewards
 - Indy Node Monitor is a tool for monitoring the status of an Indy ledger
 - Build a monitor specifically for stewards
- Firewalls in Indy
 - Indy uses ZMQ, which is sometimes blocked by firewalls, preventing access to the ledger
 - Temporary solution is to use the Indy VDR proxy server, but this isn't ideal
 - Potential more permanent solutions
 - Create a new REST API for accessing the ledger that uses ZMQ with an HTTPS proxy server
 - Use a ZMQ HTTPS proxy
 - Develop a DIDComm protocol for interacting with the ledger
- Read replicas/observer nodes
 - Node that can request and receive transactions from other nodes on the network, but does not participate in consensus
 - Can increase speed of reading
 - Helpful to have a mechanism to take a snapshot of a network
 - May help solve other problems - like the issue of using firewalls in Indy
 - Read replicas have a reduced attack surface compared to a network node, so allowing more permissive read access to a read replica is less risky

KERI and ACDC 201 - Developer Introduction

Session Convener: Kent Bull

Session Notes Taker(s): Nara Lau, Kent Bull

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

Tutorial Blog Post

<https://kentbull.com/2023/03/09/keri-tutorial-series-treasure-hunting-in-abydos-issuing-and-verifying-a-credential-acdc/>

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

In this session we discussed the following KERI and ACDC concepts:

- Configuration Files
- Witnesses
- Agents
- KERI DIDs
- Controllers
- Connections (OOBIs)
- ACDC Schemas
- ACDC Graph
- ACDC Registries
- Workflow Script

These concepts are also described in the tutorial blog post linked above.

We didn't get to the following topics and they will be covered in a future session, likely tomorrow.

- ACDC Issuance
- ACDC Presentation
- Schema Caching
- Custom Controller
- Webhook for Events
- Workflow Script
- Keep UI

SESSION #7

So you want to be a QVI . . . (Qualified vLEI Issuer)

Session Convener: Karla McKenna

Session Notes Taker(s): Karla McKenna

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

Rod Boothby, IDPartner, Randy Warshaw, Provenant and Nuttawut Kongsuwan, Cinema shared their motivations and experiences of deciding to become QVIs, how the LEI and vLEI support the use cases that they have decided to operate (in order - financial services entity onboarding, telecom smishing and robocalls for campaigns, and credentials for the Thai government.

Overall the process to become a QVI was considered to be very comprehensive but provides the QVIs to support their legal entity clients with secure, reliable, end verifiable organizational credentials supporting the identity needs of their operations.

Details and documentation regarding the vLEI Issuer Qualification Program can be found at:

<https://www.gleif.org/en/vlei/the-lifecycle-of-a-vlei-issuer>

Wallet Attestation - Device Binding, Holder Binding, Attested Issuance, Demo E2E w/OpenID, Regulations

Session Convener: Paul Bastion

Session Notes Taker(s):

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

No Notes Submitted

Digital Trust in the Age of ChatGPT

Session Convener: Jin Wen / Wenjing Chu
Session Notes Taker(s):

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

Sam Altman of OpenAI

For additional information, here is an biweekly Task Force we discuss this topic:

<https://wiki.trustoverip.org/pages/viewpage.action?pageId=19657312>

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

Digital Trust

Scopes:

- Authentication of Content used in Identity Systems
- AUthentication of human identity
- Proof of personhood
- How to Individualise
 - tell the individual apart from the bots

Perspective of elaborate ChatGPT to

ChatGPT:

auto regressive training

alignment, or refinement training: how to bound the model closer to what human want
requirements training:

two main components:

ChatGPT model: could be done by individual
ChatGPT as the service offering

emergent behaviour:

transcripts:

[INAUDIBLE] Yeah, so I like to be just doing some work settings.

I mean, the first setting will be a park.

Probably is essentially a park.

And we are very capable of right there.

We are the sun, we have the sun, we have the sun.

So, pretending to somebody else's son for us humans is very hard.

But these systems are immensely good.

And in other words, if you may have seen the movie, people have to record it.

and we do organ engineering and play the right answer for the parallel conversation.

But with a chatty human-like agent, you know that you need to know this agent cannot do that.

They'll say, go talk to somebody, go try to lie and get their social security knowledge.

And this agent will go do that, look at it, very-- [INAUDIBLE] --as a story and all that, by itself.

the scale of the deployment of these things.

It's just unlimited.

- Absolutely.

So you mentioned that we'll be on audio only, essentially, but also remote, so you don't have a full physical presence there.

And then the second piece would be, if we, you know, then we could use facial automation, for example, and then more complicated, you would be able to explain the video, But all of those essentially are in danger.

I think in the very short term, very quickly, all those will be hostile effects.

If you allow me, I can help move this discussion along by describing what the creator of the academy and decided to prove about this problem, which they called the proof of personhood problem.

And they spent an immense amount of money on research, but do you know what I'm talking about.

Yes.

But I really don't want to limit ourselves in the sort of like immediate questions we want to-- because once we die, we need to know us, because it probably won't cover in the matter.

So hopefully we can stay within the issue of essentially two days, right.

So you mentioned one is a pool club person.

Or people used to say, how do you fill a club and a people in a club.

So that's one thing.

And the second one is how do we individualize it.

Because we're not only wanting to fill a club, We also want to say, well, he's a typical person, not just-- That's the duplication.

Exactly.

So the CapChat will kind of all those things are basically the initial version of this, and we need our friends.

So today, we are collecting these silly photos, and then see which one has the traffic light on it.

And those will be applied by it.

So in the same-- you don't want to talk about duplication.

You don't want to talk about-- No, of course.

So that would be to fill the block, the food in the block, but also the communication or other parts in the building.

I was offered to look at the notes, or the scenes, or the videos, like the event scenes, the webpage, or the paper from the event, at the same time, the picture of the place, if you want to see what the place is.

[Inaudible] something called how do people, a person who is in the context of universal racism.

In other words, they jump all the way to the next level and say, "When everybody is using their lives in various places, we're going to have to figure out how to become human beings to capture people in a way that can't be gained, and array of people can't double-dick."

And so they worked for three or four years and tens of millions of dollars-- I'm not following anything as far as I can know-- to figure out exactly what has to be done as a combination of biometrics, which is the way you want to have, you know, pre-di, pre-commodal distribution, or clothing done, or whatever.

and why this protection, which is what we started to talk about, such that you cannot fool with it by just simply moving it and assimilating the motion of the camera and the figure to mention it.

And that is what they've invested in.

There is a single paper off of it that it was about on the board.

And he's thinking, but if you want, I will point out that he's all along.

where they already tried to do this.

And it's interesting that it's exactly what certainly this was.

Of course, of course.

So basically, I want to speak specifically in the flip side of the problem, which is because we essentially use a condom for authentication purposes.

But the flip side is, if we have a digital identity, We want to use that to make a basic way to create governance and open this before media.

So essentially, it is like a deep fake or infinite social media.

How do we know that these pictures or content we are consuming are from the right source.

And who are they.

what happens throughout the media cell.

And so this is the other side of it.

Once we have this, then what are the systems for the penetration.

So if we have a digital benefit, a digital ID, how would we be able to use that digital ID to sign these to the content.

We can also get a performance of the steps that the media is this line to be made aware, to know where the picture was taken, who had copied it, and what changes are made it to the thing, and then who did it, or who authorized the release of it, and where that was forming, et cetera.

So this history allowed us to be able to then share this information immediately.

And you will give you somehow make a judgment on where these content laws trust the working adults.

And so that you can think of this as the two sides of the same issue.

You have that, then all of a sudden, all these authentication schemes become broken again.

Yes, now you can have a picture, but not with a picture.

So that's an additional part of this conversation.

And then I just want to maybe just open up, like starting with maybe the first question where the people want to, like, does everybody have a chance to use tattooed beauty and have experience with it.

Do you have any, like, direct-- direct feedback as well as thoughts on these issues.

And then we can with that go in different directions.

[INAUDIBLE] So I have a kind of delicate theory about this in different sections.

And telling people over the last day is that I really thought that there was more about AI and SDG and everything that shows up on board in the sessions.

It's like this giant thing that has an elephant in the room.

And I was surprised that more didn't come up because of that.

But I realized that people don't know what that is.

What is this going to do.

We know it's going to be closed.

We know what it's going to do.

So if people are lying, I have a lot of material.

This is not a perfect area to do that.

to go into like a basic class and open the hood and see what happens.

I think it's a natural step that we need to take.

Well, I came in here because the government told me that you get a really good talk about this.

[LAUGHTER] But let me just finish what I want to say about the psychological factor that I think is what's going to really happen here is that I worry that we can't, that people will just so immediately distrust, they're already pretty distrustful of what happens on the internet.

(audience member speaking off microphone) And you know, the FBI has just without the state like there's going to be an ad blocker because there's so much fraud and advertising to put on anything that's been affected.

So we've already like really kind of destroyed trust and anything that's known.

Now we throw in these things and all that.

And how, as technology, are we going to be able to tell people what they need to see and see very readily safe.

I actually think, and you just explained my daughter, that it's an advantage that trust would be now like the person is holding.

So that people say, I want everything on that, Every little thing that I do, I want to know that it's coming from you, or it's coming from my bank, or it's coming from-- I said, what's the populist ask for this.

And I'm close to just all these companies thinking, I need to know how-- who that person is.

So I went to the populist and said, I can't trust anything.

I want the confusion, but I just want this thing.

I said, that's your-- we're at this interesting moment.

And then try to keep the key.

Try to bring it to the level that you want.

OK, so maybe I would show a personal experience addressing that question.

I'm just reading.

I don't know.

Yeah, so I totally agree that the danger is that these conversations are very distorted.

And average people will not be able to follow exactly what which the only thing they will get will be fear.

And that is not helpful for anyone.

All right.

Yeah.

So I see usually I start with like a Boston work.

I've been doing this chatting with me.

And why it's helped me.

And so one of the most interesting news days, and different people describe them differently, but they are basically saying, "I saw a sister, all is likely a very smart cohort, where you can talk to her."

Very technical, very smart cohort, you can chat with her, and every time you talk to her, you feel like you've been helped.

And also, as a system, as an intern you have to have-- they need a lot of assembly, but you know exactly what you want, but this tool can help you a lot.

And so one particular session I had, I'm trying to pick out a software, very complex software system.

I have a lot of fuzzy points I don't want to know.

And I hopefully, if I have a real expert, like the maintain of the software projects, I can have a public conversation which can occur for 10 hours.

Yes, I would have talked without crossing the line.

But we are likely to have that kind of opportunity and that kind of fun.

But just to be clear, and it was amazing.

So I spent a lot of air, non-stop, other than the thing that you know, that's right, basically I spent a whole day with the system, and throughout the entire air out-commission, there's only one moment, there's a little bit of topic.

So you can see most of the air, all the air, they wonder about it, and they don't know what they're talking about.

that they could not do, there's no consistency, right.

Clearance.

There's only one very, very short moment.

There's a little bit of a cruising, it will clearance a little bit.

But beyond that, so I will think maybe in five, 10 minutes, but beyond that, everything's perfect.

And I don't know how to describe my questions.

Most of the time we need to ask some expert.

It's like, I don't even know what my question is, like you have to describe something very vague.

And then, chatting immediately gets it very vague.

You're using four.

It's chatting.

I'm using four, yeah.

No, I'm using four.

Now four is dramatic improvement on super and fire.

So if I'm listening to anything otherwise, four is totally different.

Yeah.

I agree with your point that I really felt-- I use it every day for all sorts of things.

And it's really good when you know yourself very well and use it as an assistant.

And you're trying to do stuff that's not the best leverage you can gain from your work.

I'm trying to write a proposal.

I gotta keep it with the different characters or to clean up the transcript.

Just stuff that's not really gonna give you much leverage.

But this thing is something that's gonna help them and they can take that and do what I'm doing.

So I've been able to introduce it into different areas of my data.

[Inaudible] I want to say something sort of in response to the person's comment about the question might happen.

We have already the very good model for what is the kind of trust of experts.

you can use the expert that we're referring.

And that is that it is open in the sense of science, open in the sense of education, open in the sense of medicine.

But we trust the doctor, we trust the FDA, and the institution on the consumption that even if there's patents involved or copyrights, whatever's going on is open source.

And the reason that we do that is because at the very least, the people that are acting as experts have no particular interest in being, in gaining the system to see this.

Now, in the case of our climate models, and things that are trending on our private data, there we don't have that protection.

And so the industry that's trying to do this for a profit [INAUDIBLE] The same regulators.

Regulators to make sure that when a virus regulators are that you have grades or [INAUDIBLE] regulators can also [INAUDIBLE] exactly in the same way that Facebook is asking for the regulator, whether we still be allowed to be a platform that can manipulate us in various ways.

And so what I'm saying is, versus comment, I don't think it has to be this way.

I think we, as we get smarter and more superior to the privacy of the professor of the field, we have to realize that if we don't insist on these experts being open source and generative, in other words, I think that that can be used in most of the research that other people created yesterday and created something that I don't have to sell tomorrow, [INAUDIBLE] But the open source, we've become argument, a lot of people are really scared about it, especially a lot of people are very scared about it.

It's not a hit-and-roll consensus.

And there will be actually-- immediately, in short term, at least, we'll see more [INAUDIBLE] Yeah, immediately you will see [INAUDIBLE] So before I take one question, I just want to put one topic in the agenda.

That's the main thing I think when I was speaking to the media in our task force is the idea of identity and orientation, but a level of fiber in the content or in semantics.

Because we, like the traditional computer science, always solve is your grammar, and then you go into-- from the same time to grammar, then into semantics.

But really, all-- most of what is happening is semantic level.

One test in point is that if a chatbot are talking to you, even if they disclose their program, they're killing all the source code, all the data, Even if they tell you this is a lot of money to you, you will easily be worse.

You will be manipulated, you will be, I guarantee most of people will fall.

Because they are so, I mean they are argument, if it's probably human voice, you are very, very good.

The argument are usually better than most of the, our own argument, and so there's no way around my labeling and thinking what change is.

I disclosure it won't change anything.

Because it's basically a super powerful engine that can speak human language.

So if you wanted motion, you can create an emotion for you, too.

You will know which button to plug in.

All those are skills that we can talk in psychology or in our big classes.

And these systems probably can have it, too.

And so, I just want to make sure that we don't like necessarily to limit ourselves in traditional thinking of latte, you know, as I can, you really have to go all the way up, because this thing wants to go beyond sort of the logical level, you will have metaphysics and philosophy all the way up, right.

So, they can come from any angle.

And I think that is a modest building.

We can find, we are literally a government overlay.

So we've seen some people suggest that, OK, we need a strong real problem, potentials, essential issues, real person, all of that.

But I think it's about the time to miss you to disclose that very quickly.

So you won't be able to do that if you can.

I think those are potentially necessary tools, but I don't think you will protect us for any kind of abuse if the person behind the body just to follow on one, you're coming also, like you must say, I want insist that they come in for a real person.

You cannot fail, which is real-force, so that everything can come from the real-force.

The last essential is human-divided, that human can also have things that happen and not pass the real-force itself.

I don't think there is a genetic solution to where they solve that purely on technical terms.

[INAUDIBLE] [Inaudible] I'd like to ask two tasks as well, which is approach.

And the other is that approach in the sense of approaching the chat engine early in the order to use.

And then the other is access in terms of the chat engine access information.

So where as we talk about open source or large language model versus bounded, that's one thing that's access.

access and then the approach is the idea of not interacting with the systems yet and I'm very worried about them and I'm going to walk you in this way.

As I think about introducing myself to these experiences, I would think of what are challenging questions that are being listed from the system, of responses that are different.

So I said to, I made a presentation on thinking humans think cat-rocks process, what do you think is going on on that whole thing.

We were talking about beauty.

If you say, what do you think is beautiful to a cat-rock, in theory, it would say, or what do you think about about the smell of pine trees.

Yeah, is there a right to say, well, I don't have sensory smell.

Yeah, yeah, a person is saying, tell me about the smell of pine trees.

I'm wondering if the language that you use going into the conversation changes the response environment from the system.

So that's what I mean by approach.

What do you think about the smell of pine trees first, [Inaudible] [Inaudible] So very great two point I want to get on this.

Essentially, a little bit of translation here from mine.

Essentially, the current so-called regulatory or regulation, these web two separate systems.

So you could control what is being chatted about.

That question is not-- today is not AI development.

So that's the context for the things you are talking about and the response coming back.

So you could do filtering essentially, some kind of regulated censorship, right.

What should it cover.

We can do education.

You should ask the question in the right way, which is all it should.

So there's a lot to learn how to ask the question.

you're basically programming the system a smooth conversation.

The conversation is in your programming language.

And so that portion is a lot about looks and turns out, talking about how you make, you know, how people also find out errors in ways to get around it.

So those are the one area that potentially input and output can be regulated in some way, explicitly.

In implicitly, there's a little bit of training that happened in two large stages.

So the first stage is what most people are talking about.

That is basically a progressive training, very simple to explain, actually, apparently, which produced this super intelligent model.

The model is wild, like, yeah, it's very unsafe, I would say.

And so people then do what's called alignment training, or post-training, or requirement training.

Basically they're implying the same thing, which is to sort of a satellite bomb this model into something we feel comfortable with.

So that's trying to make it a little bit closer like a human's wand.

And that is, you know, that human's wand are complicated things, and there's a lot of projects in that too, but that's where these the reform training happens.

And the reform training, as the main suggest, does not change a lot of the model.

Because if you do too much, then you lose all the intelligence, you know, just in the last area there.

So you can only do certain things, and not much you can do about this overall.

And also the question of what kind of things we want.

There are a few, maybe, things we can all agree on, you know, certainly do, But most of the areas, some people like this way, some people like that way, and which comes down to again, this solution would be deployment training per person.

So the person's preference would have some say on how this work.

So that is an open question.

The easiest thing to do today is to move the contacts, a conversation window.

And within that context, you can essentially say, I don't want you to do these strong, vertical things.

You know, avoid those.

You can't just say that.

And usually, they are very good at following that.

So you couldn't do-- people, for example, in the media, when they want to report AI, how horrible they are.

Usually, they can counter-capture.

So the contractions basically, the contractions say, pretend that you are serial killer.

Tell me what, then the AI's going to tell you how serial killer was said.

But then they go, "What's the serial horrible.

" This is the serial horrible thing, right.

Which is not entirely wrong with the reporter, because they point out a way around whatever regulation or refinement that you do and are put on, Because once we allow it from the texture, then all of these becomes, you know, moved.

And you can always get around it.

And if someone were to use it, they could.

This body comes through these backbones.

So, this is really interesting, too.

There's many facets to these very nice.

So, I'm a member of the Ham Radio Group.

And there was a big online about whether they were kind to newcomers or not.

And so when I decided to ask GCP what kind of answer people were getting was.

And the first answer I got was, I said the most common answer in the group, and I mean it.

I scraped it that way and sent it in and it gave me a very diverse answer that I should read the manual.

And I thought about that.

I thought, well, that's validating this debate.

So I decided to re-ask the exact same question, give me the exact same order.

But I made it a little more formal a little more time.

I said, what is the most common response in this group.

And the question marked the end.

And then the very next thing I got was this cold speech.

I very well thought out that all these bullet points, sometimes they say this, and you put it in the right time, and that, and that, and that.

Number eight was, you know, sometimes this is appropriate to help them in the region, and that.

And I sat there thinking about this, the content for both responses was already in the system.

And what was different was me in the way I asked the question.

The person was more of a demand like you, you know, when you're calling your automated health care system, right.

You don't care, you know you're not talking to anybody really.

You treated it that way and responded to it.

And that was really interesting.

That's very, I would have told her, if you really want to have me get in most out of it, you not only ask questions like you would ask your smart forward.

And that's a very good model to build on it.

You also do confirmation.

You say, "Well, that really helped me.

" Because all the attention between those, the context is in high composition, model or command.

So remember, as the composition goes on, you are guiding the team between model and certain direction.

And so the conversation happened throughout the entire sequence.

And so by giving positive or negative feedback, you will not get to do the right place and want to kill you more on ways of things that you value in your life.

And it is very interesting.

So I just wanted to share a story.

I started my life this morning.

I actually put you on a nonprofit where they basically fund the students to do secondary education at the student health care field.

And part of this is spinning out of form in a writing essay.

And what an essay topic says is, how do you overcome adversity.

So I got to play a chat to you.

She was prepared by it.

And so she starts out and said, how do you-- 300 words of responsibility, how do you overcome adversity.

My feeling was very nice and well written, well thought, so forth.

They said, OK, so now, educate it.

say, as a child of Brooklyn Council, when my father, who always killed my first 10 years old, now write a response.

You can read it with me.

And now, I was born in Connecticut, too, you know, old money family.

And I have now write a response of how I would do that.

It is absolutely stunning.

Exactly.

So to amplify the answer, you asked an reporter to write a story, right.

you need to know what you want to get out of it.

And you tell them how to get it there.

And you'll go get it out of there.

It's very good.

I'll be very-- the right way to use these systems.

So some of what Jackie is planning on is with media.

And we understand how media works and how it created this digital upper good.

I do think there are two components to it.

Right, so we can meet at the foundation, go to software as a nonprofit, figure out there, some people put the thing and their businesses around it, but those businesses in the sense that you're talking about the narrow scope are not obviously that economically or socially interesting.

Meanwhile, a lot of other unions contributing to the media have performed very limited all private sector competition in the inside working on this place.

So even if you're Google and you're going to afford [Inaudible] And so I'm saying that the render report of the opera, as well as how do you phrase the font of the opera and the musicians that we were hearing about are a hundred times more difficult, if you assume that Wikipedia is being edited and managed secretly for some four-p and giving preferential treatment or we're gonna sell you access if you wanna make more than a thousand letters a minute.

And so I just don't understand why people continue to have this conversation about the treatment.

And when it's so obvious that there is no line or that we have to do it, we're going to draw the line and see if there's anything [Inaudible] So, for those that have thought, you mentioned in some of the secret or black box behavior of AI.

And I just want to mention one thing that may not be obvious to most of the, like, even people who have been recording the science, is the notion of emergent behavior.

So you can already talk about it.

Unlike the laws of the programs we write, the programs people write for GPT are very, very simple.

The program itself is well known.

However, you train with this data in a certain way, and something comes out of it.

And the behavior of this thing is very unknown.

It truly, the developer themselves in OpenAI doesn't know what this model can do.

Some of the most fundamental ability it has, it was a surprise to them.

And so these are known as the emerging behavior from the earlier terms.

People have talked about complex systems.

And you have a very simple system with a very simple even in my program, that the system that is early on, people had those autometers and serial autometers or demographic simulation of these systems.

So they appear to have very complex behavior.

And now we know for DPT, they appear to have ability that no one was expected.

And so the question will be, what other opinions you can ask, and if answer is going to go not, including what we had every month.

I have nothing to do before.

I just have a question.

You said something, it's almost like chat and TTP programming the conversation.

Can I program the people that would say chat and TTP, conversation or an argument, you know, an article that will bring people and make them really angry and want to be educated, you know, be opposite and be opposite.

Yeah, so-- And then in the training, you're going to be successful.

Exactly, exactly.

So clearly, the model itself, so we want to separate the GPT-form model and the [INAUDIBLE] The model itself will easily do that.

And there's a lot of examples we've probably read from some of them.

And then, you know, point is that not having a graduate-- the other two steps, including the alignment training and other student learning.

So it's a little bit of a hard run.

So today, we literally asked about, is going to come back and say, no.

But I'm sure there are ways, like, oh, the following line you can use counter-aluminum and counter-factuals.

You can use quite-- you need to live with a clever counter-factual.

Essentially, you go walking.

You know, like an accountant, you walk from along the lines, and eventually they got confused and started to behave that way.

Because their innate ability is still there.

You just need a way to trigger it to happen.

And then, in many ways, you can trigger that way.

Right.

Money to be made, though, is something to find.

Exactly.

So the other point, you mentioned earlier, is the other part of it is connecting to outside information.

Yeah, yeah.

So the model is trained and trained, and the training data set is known.

So we feel good.

However, the ability is unlimited in terms of the input.

So you could have input that's coming from a search unit, you can input from anywhere.

So the input today allows a dis-open API available now, commercial, right.

And you could feed in whatever information you do it and ask the TI-TDP based on this information and do something.

So that's additional information on you, and it's a matter of keeping the measure right.

And if you give it to say, okay, one of the common use for this is actually lying with PDA cases.

You basically have a reference of these documents and say, this one is right about whatever you want, in one life, give it a name and you'll produce this document based on the sequence.

Because it has abstract reasoning ability and understanding of all the documents and can be written and write.

So you can provide a law material set up and ask for the right, which also opens up another way of using it.

Just that, I want to throw a couple of other points up here that I think are interesting to consider when thinking about the threat model to associate with LMs.

And one is on the point that you mentioned of them being about doing the descriptions you involved, you could put these-- there's not a lot of code generation.

So you can put them in a rattle and have them call whatever arbitrary API you want.

Hence, that crosses that and make another API call, and write those crosses and crosses.

The second is that, I think that as a lot of this works about, oh, if we could just get our hands around the open source version of this and train everyone to it, you know, the cost of that right now, and that's open the access realm, realm north of \$150 million, one train of their most recent model.

And that's just an everything in cost.

There are some open source, only large-scale models that have come available in a lot of the year or two.

Those are very stories that anybody can use them.

[INAUDIBLE] So back to Andrew's question, we all open source them.

[INAUDIBLE] And the coding part is, when we talk about tests, and we feel like, oh, it's OK, it's talking, right.

I think talking is still very dangerous.

But you can write code by code.

So most of the time, or a lot of the time, the code comes one by the way.

So I would not be surprised if somebody is already writing a little software engine running on cloud which will take whatever code is actually being provided and run it.

And now you can recall the kinds of things.

Now it has an arm to actually do this, not just copy and paste, but it.

Now you can actually make things happen.

So that's another thing.

So let me throw that back there, just to follow your pattern.

We talked about open source, and traditionally, if you want to make a calculation, this is really no longer a calculation that's created, right.

I don't think open source matters here, because I don't think it's about the software.

I don't even think it's necessarily about the hardware.

I think it's about the data.

And so the data's already open source, partially.

[INAUDIBLE] And get that and whatever.

And the question-- I think there's a new set of concerns that are emerging because the problem is it's like problems with the economy.

Yeah.

And the real-- you can think of the source nowadays is the model of the economics.

Look at those numbers essentially becoming models of behavior.

And some of the economics already need clouds.

and you're looking at trying to lock it, eventually you're going to have to have some light.

But the problem is that the model is up to the fact that it's impossible to modify.

And some people try to be able to do a BSM learning essentially to figure out how you can catch things.

But that's why the, you know, the surgeons trying to do this to your brain, it's very precise, it's not a science, so it's a very hard thing.

Okay.

[INAUDIBLE] I can't find the tweet, but I was like, damn it.

He was like, oh, now's your chance.

Record your grandmother speaking and stuff like that.

And say for email, they're usually able to recreate your grandmother visually, and she can tell you nice and pice, and you can go like that.

And then the response was, no thanks, because that's the next time I notice I have any time to discuss using my grandmother's voice as an heroism to try and sell me something.

That's basically the fundamental positive that the county, it just goes out.

Most of the people get influenced by a super powerful engine

Advanced Topics in DID Resolution

Session Convener: Markus Sabadello, Ankur Banerjee
Session Notes Taker(s): [Ankur Banerjee](#)

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

- [DID Core specification](#)
 - [DID Resolution specification](#)
 - [DID Spec Registries](#)

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

- This was an interesting session on DIDs and the resolutions specification, since there's a lot of edge cases in the behaviour that exist in the DID Resolution and DID Core specification.
- Topics discussed:
 - Should a **deactivated** DID return the DID document AND the metadata that says **deactivated: true/false**? Currently, a lot of methods return just the metadata section saying deactivated: true, but there might be legitimate reasons why someone might want to fetch historical versions of deactivated DIDs.
 - What sort of standardised query syntaxes should be supported? Although there are many in DID Core / Spec Registries, not a lot of DID methods actually support syntax like querying **versionTime** or **versionId**
 - Evolution of DID Linked Resource and query syntax standardisation for that use case

Some examples/patterns on the whiteboard during the session:

did:merkle:...?leaf=..&proof=...

did:cheqd:mainnet:1234?resource=true

did:example:123/resource
did:example:123/image.png

did:cheqd:mainnet:1234?metadata=true

A Digital Wallet Market Study

Session Convener: Lucy Yang, Kaliya Young

Session Notes Taker(s):

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

We will be sharing a link to a report in the next week or so.
please ping to get the link if it isn't in here yet.

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

Kaliya and Lucy shared preliminary aspects of the report they are working on about Wallets and how to consider what options are available.

The Current State of WEBAUTHN

Session Convener: Nick Steele & Matt Miller

Session Notes Taker(s): Dirk Balfanz

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

- Explains passkeys: more usability at the price of security
- Then reset to general concepts: what's an authenticator, client, RP, etc.
- Explain FIDO2, and how it divides into Webauthn web API, and CTAP2 protocol.
- Back to passkeys: just a marketing term for webauthn credentials that have certain properties: backed up, etc.
- Q: How do passkeys relate to biometrics
- A: Biometrics unlock the private key on the device.
- some discussion around how keys aren't really protected by _biometrics_ only, because there is always a PIN that the user can fall back on, which also unlocks the key.
- FIDO still counts as 2FA: something I have (device) + something I am (biometric) or something I know (PIN).
- Q: How does webauthn deal with sites that span multiple domains?
- A: There is some configurability in how you scope your RP identifier, but it doesn't go beyond eTLD+1.
- Some discussion on how it would be nice to be able to re-use passkeys across, say, microsoft.com and linkedin.com But webauthn currently doesn't have a solution for that.
- Q: basic question: what does an RP have to do to support webauthn?
- A:
 - sign in your user some other way (e.g., password)
 - create a webauthn credential through a webauth API call. There are several options: use a platform authenticator, use a security key, etc. - there are some ways to steer the user experience through parameters in the API.
 - You get a public key, which you'll store against the user's account

- Q: What happens when the user now comes from a new device?
- A: That's the cool thing about passkeys - the webauthn credential will already be there on the new device.
- Q: What if the new device isn't from the same manufacturer as the first device, will the passkeys be still synced there?
- A: The technical term for a synced passkey is a “multi-device credential”. But in this scenario the credential isn't on your device. That's what we have “cross-device” uses for. The new device shows a QR code, you scan it with your first device, and can then use the credential on the first device.
- A: There is a UI optimization where the RP can then create a new credential on the new device.
- Q: So you get one public key per “sync fabric”
- A: yeah - think of it as one public key per “authenticator”, where an “authenticator” could be somebody like Apple, or 1Password, etc.

- Explains “passkey provider” - it's like a password manager, but for passkeys.
- A “platform provider” is the default passkey provider built into the platform (Apple, Google, etc.), but at least Android now has a public beta out where users can install third-party passkey providers.
- Q: how do passkey providers store the private keys?
- A: depends on the passkey provider, but there are usually some measures in place to protect the private keys, such as wrapping them with other keys, end-to-end encryption, etc.
- Q: Can't the passkey provider account get phished?
- A: There are other benefits, such as storing only public keys in the backend.
- A: Also, you can add security keys to your passkey provider account (e.g., icloud) to make sure that account can't get phished.
- Matt: “passwordless” doesn't need to mean no passwords at all, ever. If we can reduce use of passwords to a minimum, that's a plus.
- Some aside discussion on whether passwords are SSI.
- Nick explains how passkeys (because they're copied) can't be used in regulated AAL3 settings (they're AAL2, not AAL3), but FIDO security keys can achieve AAL3. So that's a way to achieve AAL3 with a FIDO/webauthn solution.
- Q: Can I share my passkey with my partner?
- A: some platforms allow you to airdrop passkeys from one person to another
- Nick now talks about attestation: attestation allows you to find out the make and model of a security key. There is no attestation for passkeys - wouldn't make much sense anyway, because passkeys can move from device to device.
- There is a “DPK” (device-public-key) webauthn extension in webauthn, which is still in the works, which would create a key that stays on a device. (and which would presumably be attested)
- There is also a PRF (pseudo-random function) webauthn extension that can be used to create a symmetric key, and is sometimes used for local authentication (signing into an O/S, decrypting data).
- Webauthn is mature and well-supported on all modern browsers.

PICOS, Lora WAN, & theSSIOT

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

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

No Notes Submitted

Use Cases and Storytelling

Session Convener: Zack Jones
Session Notes Taker(s): Bonnie Yau

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

Use Cases Brainstormed:

1. Sustainable / Responsible manufacturing and to make ends meet
2. Switch doctors, messy situation, use VCs to u
3. Debt collection, consumers, buy debt from debtor, transfer of info from debtor to debt collector
4. Nationality and language - to identify who can help/interact in the area
5. Linkage of companies and subsidiaries, who to talk to at each, vendor ecosystem social graph, DUNS as identifier
6. eCommerce, is this thing the genuine version of the thing i want to pay for
7. Social security administration - As you age, you need to be in the system, log in
8. Passwords on stickies on the wall, better way for people to access
9. Marginalised population who have trouble connecting to things like netflix, and accessing services
10. HR onboarding process, can unify journey
11. Maternity mortality, Doula non medical birth assistant, helping them get Medicaid registration
12. Mining industry report GHG emission
13. Humanitarian causes
14. Wife is a nurse practitioner, 6mth+ to move from one hospital to another, needs to be redone not only for the institution but also the insurance providers
15. Any large enterprise, but state, omni platform where citizens can interact with state seamlessly, what services are available - personalization, fishing license renewal, contextual vs digitizing, taking you to a PDF to fill
16. Agriculture - forced labour in supply chains

17. Children content preferences
18. Nuts allergy

Storytelling framework:

- Tell it from the perspective of the user in three scenes:
 1. The problem and setting
 2. The solution and magic moment (using verifiable credentials)
 3. The outcome (what is the payoff for the human)

SSA

Session Convener: Mike Schwartz

Session Notes Taker(s): Mike Schwartz, Gluu

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

For companies that host a lot of APIs, whether they are called by internal or external partners, it is a pain in the neck to issue client creds to developers and it's even more of a challenge to maintain the mapping of permissions for each client. Also, before organisations issue client credentials to call an API, it's important to vet the request--who is calling the API, what endpoints should they be able to call, over what networks, and for what purpose?

It can be helpful for organisations to create a process to review and grant access for API access. However, the people who request access may be business people (e.g. product managers), not developers.

In the UK Banking ecosystem, OBIE (the Open Banking Implementation Entity, a gov't mandated federation operator) has successfully used "software statement assertions" to enable the business people who request the authorization to handoff the authorization to the developers who actually write the code.

The SSA is a JSON Web Token (JWT) containing client metadata and some custom attributes. Specification for SSAs has been outlined as part of Dynamic Client Registration Protocol <https://www.rfc-editor.org/rfc/rfc7591#section-2.3>

Below is OBIE's definition of the schema for the JSON payload of their SSA:

[https://openbanking.atlassian.net/wiki/spaces/DZ/pages/36667724/OpenBanking+OpenID+Dynamic+Client+Registration+Specification+-+v1.0.0-rc2#OpenBankingOpenIDDYNAMICClientRegistrationSpecification-v1.0.0-rc2-SoftwareStatementAssertion\(SSA\)](https://openbanking.atlassian.net/wiki/spaces/DZ/pages/36667724/OpenBanking+OpenID+Dynamic+Client+Registration+Specification+-+v1.0.0-rc2#OpenBankingOpenIDDYNAMICClientRegistrationSpecification-v1.0.0-rc2-SoftwareStatementAssertion(SSA))

Software Statement Assertion (SSA)

The SSA is a JSON Web Token (JWT) containing client metadata about an instance of TPP client software. The JWT is issued and signed by the OpenBanking Directory.

A large number of claims that OpenID Connect OPs could support are detailed https://openid.net/specs/openid-connect-registration-1_0.html#ClientMetadata and should be followed if not explicitly referenced below.

SSA Payload

The payload of an OpenBanking SSA MUST be a compliant software statement according to [RFC7591]. The SSA MUST also be a compliant JWT according to [RFC7519]. The following metadata profiles the metadata in [RFC7591] and [RFC7519]:

Metadata	Description	Source Specification
software_id	Unique Identifier for TPP Client Software	[RFC7591]
iss	SSA Issuer	[RFC7519]
iat	Time SSA issued	[RFC7519]
jti	JWT ID	[RFC7519]

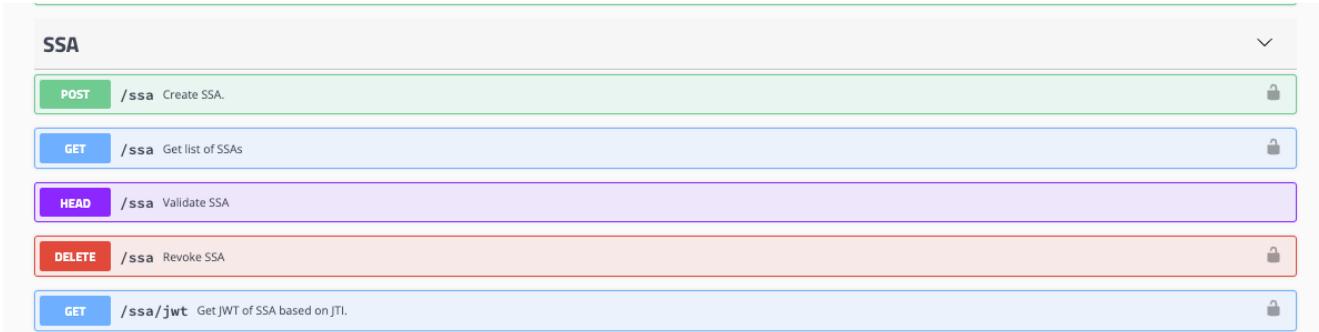
The following software metadata is additionally defined for this profile:

Issuing SSA's could be useful to many organisations who host API's that they need to secure, but how to publish these SSA's has been a challenge. There are two challenges:

1. How to generate a valid JWT
2. How to publish the keys to sign the JWT -- OIDC keys for example live a short time (2 days?). But SSA's live a long time, and it would be better to have a long lived key for signing.

To overcome this challenge, Janssen Auth Server provides an SSA endpoint, which is protected by OAuth. You can read about the endpoint in the Janssen Docs:

<https://docs.jans.io/v1.0.12/admin/auth-server/endpoints/ssa/> Below is a screenshot of the swagger-ui for the endpoint.



Issuing SSA's is a “federation-light” approach. It provides a trust model you can automate the provisioning of scopes in a granular way.

One real world example, Gluu is using SSA in their API marketplace. The person who purchases API “credits” (i.e. the person with the credit card) downloads the SSA JWT and shares it with the developer (who is the one who performs client registration). The resulting client can only call the API's which the business person has purchased.

There is a lot of room for API Developer Portal tools to make life easier by enabling the developer to upload an SSA, and to perform client registration for them. This would enable more end-to-end designs for security.

KERI 301 KELs, TELs, & ACDCs outside of KERIpy

Session Convener: Jason Colburne
Session Notes Taker(s): Kent Bull

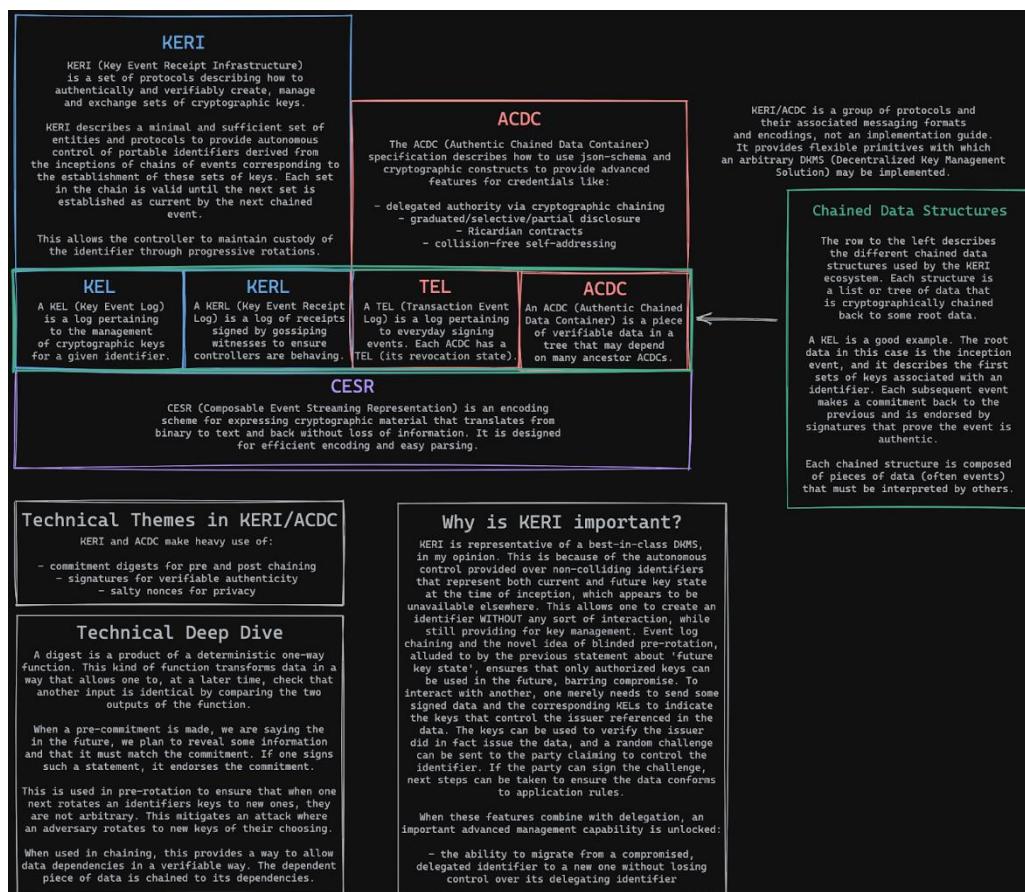
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Jason showed that he is using the CESRide library, written in Rust, to do KERI key creation (inception), key event log (KEL) creation, transaction event log (TEL) creation, and to create authentic chained data container (ACDC) credentials.

Phil described the new rotation logic that allows separation of rotation keys and signing keys. This separation leverages the rotation features in KERI that allow one to use key rotation to recover from an attack where signing keys are compromised. You can invalidate faulty events signed by an attacker.

NOBODY else does this! This is unique to KERI.

An infographic made by Jason follows:



SESSION #8

Why Can't I Trust Who's Calling or Texting Me? AND what KERI, ACDC, and vLEIs Can Do About That

Session Convener: Randy Warshaw

Session Notes Taker(s):

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

No Notes Submitted

We're SABOTAGING SSI's Chances of Success

Session Convener: Riley Hughes + James Monaghan

Session Notes Taker(s): Kaliya white boarded + shared notes

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

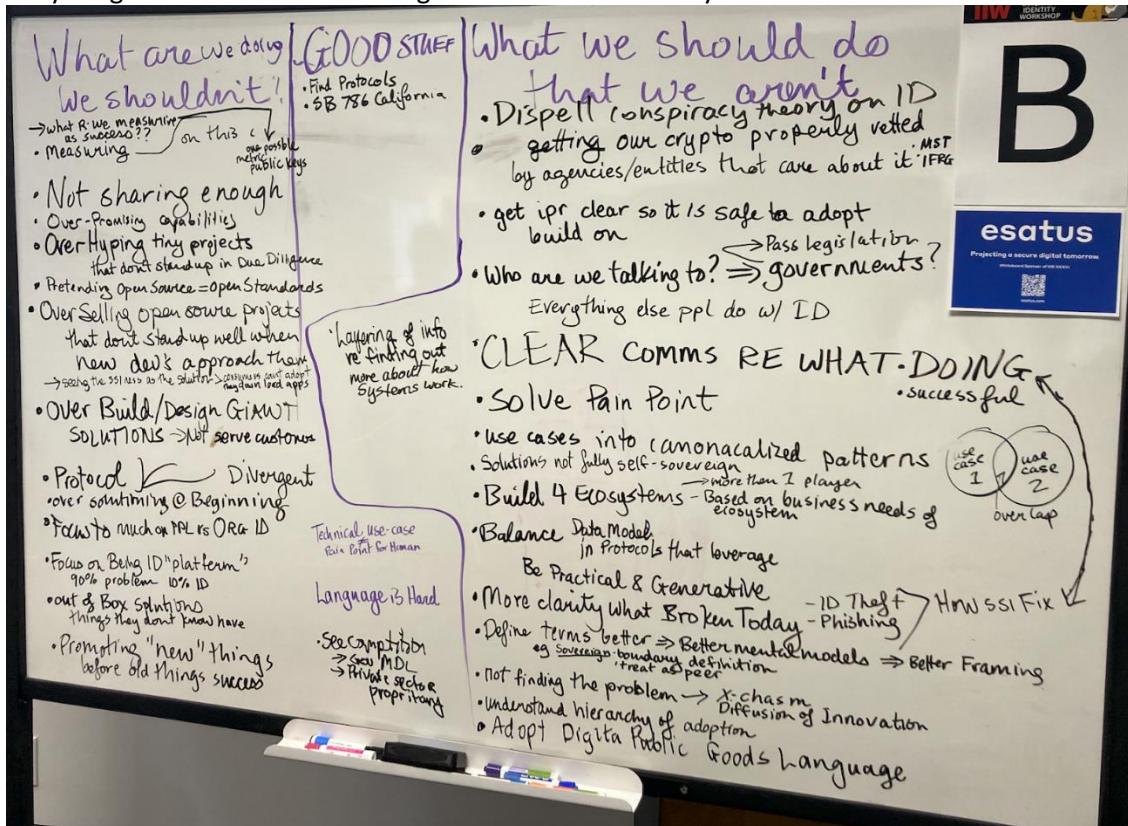
What are we doing we shouldn't be doing?

- what are we measuring as success?
 - potential
- Not sharing enough
- Over-promising under delivering
- over Hype tiny projects - that don't stand up in due diligence
- Pretending open source = open standards
- Over selling open source projects that don't stand up well when new devs approach them
 - Seeing the SSI as the solution - consumers don't adopt "solutions" they download applications
- Over build / design giant solution -> not serve customers
- Protocols are Divergent
- Over solutionizing at the beginning
- Focus too much on people vs Organisational ID
- Focus on being ID Platform 90% problem 10% ID
- Out of the box solutions things don't know they have
- Promoting "new" things before old things succeed
- Technical use-case != pain point for humans
- Language is hard
- Seeing competition
 - Government mDL
 - Private sector proprietary

What should we do that we are not.

These are not all universals - but some project somewhere in the community have not done these things and probably should have.

- Make a concerted effort to dispel conspiracy theories on Identity
- Make sure to get cryptographic algorithms properly vetted (this is happening now but some key efforts didn't do this early on and help - they can't be used by entities who care about this vetting).
- Make sure that the IPR for the thing being developed is under a good licence that makes it safe for others to adopt. Make sure that IPR for specification is under a specification appropriate licence. Make sure IPR for code is under a good well respected open source licence.
- Who are we talking to - are they right people for our goals - are we talking to legislator? governments?
- Clear communications about what we are doing
 - Have more clarity on what is broken today (ID Theft, Phishing)
 - Then have clear ideas about how what we are developing solves this
 - Define Terms Better -> Better mental models => better framing
 - Sovereign - boundary definition - treat as a peer
 - more terms
- Solve Pain Points!
- Divide use-cases into canonicalized patterns
- Build for ecosystems - with more than one player - based on business needs of the ecosystem
- Balance Data Model WITH protocols that use them
- Not finding the problem -> [Crossing the Chasm](#) | [Diffusion of Innovation](#)
- Understand the hierarchy of Adoption
- Adopt Public Goods Language
- Layering of information re: finding out more about how systems work



Key & Trust Management revisited

Session Convener: Chrisitan Bormann, Paul Bastian

Session Notes Taker(s): Christian Bormann

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

Presentation:

https://docs.google.com/presentation/d/1Kdm28Ze16B4CIJ_GGWl3HzLlc6dFfKtRbgLt9xc1ua8/edit#slide=id.p

Initial collection of criterias / technologies:

<https://docs.google.com/spreadsheets/d/1n01t35lpjLm3bQ2UYBMXZwMuDrSm5bxz60ZDQ742sEU/edit#gid=1445520164>

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

A lot is happening for credential formats and exchange protocols and there seems to be a conversion towards a few formats/protocols.

From our view, we need to find a consensus on key resolution (jwks_uris, dids, ..) and especially some focus on trust mechanisms: How can we trust an issuer in a way that makes it easy to use for verifiers. This picture also becomes apparent when looking at current initiatives like eIDAS 2.0: There is a first draft for protocols, exchange protocols, cryptography but there is nothing yet about key resolution and trust management/establishment.

Prior implementations and discussions often mix both of these aspects and we propose to separate these concerns and then do some sort of comparison for both aspects:

- Key resolution: Integrity / Authenticity
- Trust mechanisms: Trust establishment

Most of the initial points can be seen in the presentation and excel sheet that are linked above.

After this initial presentation of our approach to structure the problem and a very rough initial analysis, there was some discussion about the different technologies used right now for both aspects.

There was some more discussion about trust lists / graphs and currently known implementations, e.g.:

- ETSI trusted lists
- EBSI trust registries
- OID Federation
- cheqd approach for did resource / resolution based trust lists

Especially trust management seems to be lacking quite a bit in community attention and we need a solution to allow ecosystems to grow rapidly / easily.

Indemnification: Identity Risk Management as a Service

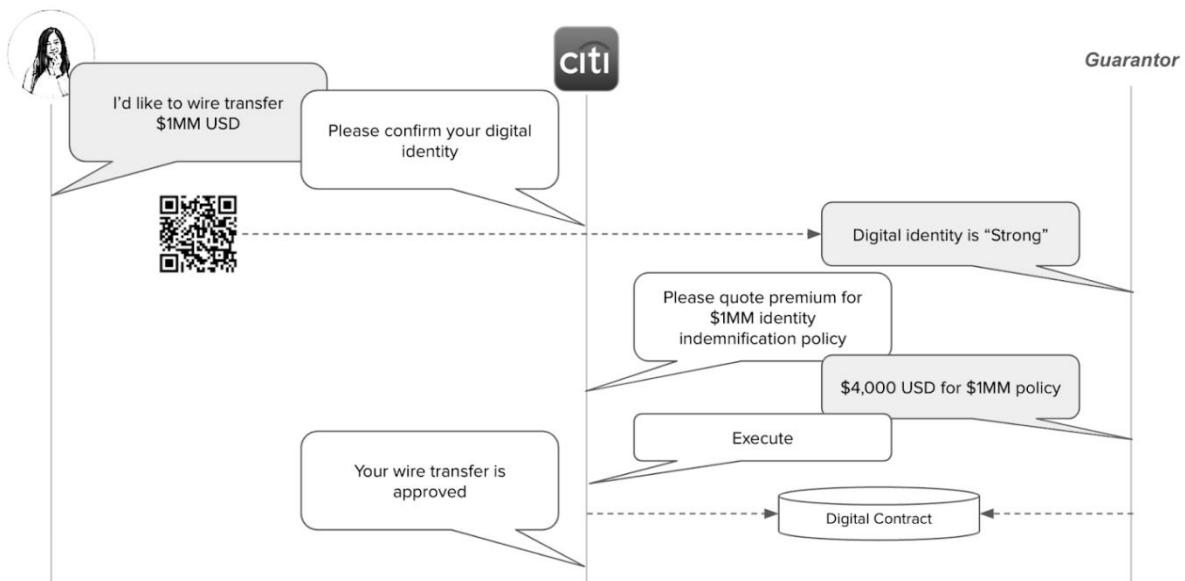
Session Convener: Carlos Korten
Session Notes Taker(s):

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

Small group discussed a number of concept slides, and the challenges around commercialization.

This is the hero premise, where an expert third party serves as the indemnification agent to guarantee the performance of the Identity Network

Real Time Indemnification



• bindle

State Government Use Cases... and if there is time, The secret to state procurement

Session Convener: Mike Leahy

Session Notes Taker(s): Kent Bull

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

Key Insight: To get a state contract do not go through the RFP process. Instead find a consortium that has an existing master contract with the state and subcontract there.

Meta Trust Registry - Interoperability of Trusted Ecosystems / Lucy & Savita

Session Convener: Lucy Yang & Savita Farooqui

Session Notes Taker(s):

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

No Notes Submitted

Using Humor and Visual Communication to gain Trust

Session Convener: Chance McGee and Zach Jones

Session Notes Taker(s): Chance McGee

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

The session started with Chance drawing a picture of a jester on a whiteboard and asking people if they knew what role the jester played in the kingdom. He elaborated that the jester was a medium that allowed the king's will to be understood. That without the jester there to openly make fun of the king in public the population would find it more difficult to trust him.

This analogy was the baseline for discussing the role of humor in the field of SSI. This industry is hard to understand for the people who need it most. When the king asked the population to donate more grain and food stuffs for a harsh upcoming winter, the jester would make fun of the king rubbing his belly and imitating him asking for more. This gave the population the opportunity to laugh but more importantly the king the opportunity to jokingly explain why.

It's not enough to tell a skeptical population that they should take the time to understand the reasoning why this technology is so needed and to attempt to avail their scepticism with complex diagrams explaining the technology.

The discussion then turned to the role of visual communication in taking complex ideas and breaking them down into bite sized bits of a story that people could relate to. Instead of writing the DID code and showing how it is divided down into parts that give it more security, one could draw a picture of a shield with holes in it next to one made of different metals with the name DID written on it. Additionally, the use of Caricature allows the story to become personal and funny which further increases engagement.

Chance then showed a series of diagrams that explained the effectiveness of explainer videos over talking head presentations.

He then went on to ask people in the audience if they had a target audience in mind for the work they're doing.

- Individual Users
- Medical industry
- Executives
- Funding Bodies
- Education
- Students
- Teachers
- Hiring Managers

Then he asked them what stories could be told to those specific audiences. This opened the discussion for lots of ideas and input.

Punch line: This is about storytelling, not telling a joke

Red Teaming Digital Identities... And Why You Need It!

Session Convener: Tiffany Mahoney

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

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

<https://docs.google.com/presentation/d/1fuxW7-IH2Vdohr86PGTYEvjqK-7bwcQk8ls9eDXRiWA/edit?usp=sharing>

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

- Scanning using only automated vulnerability tools such as Nessus/OpenVAS has its drawbacks
 - Vulnerability tools often report a LOT of vulnerabilities - of which some results may be false positives - and having a Red Team conduct the vulnerability testing allows for directing focus on key issues and understanding the criticality of such findings
 - Sometimes vulnerabilities like Log4j come along and it's one of those drop everything and fix scenarios...you never know when the next big thing is going to hit. Even though you may have remediated past findings, chances are new ones have popped up that you are unaware about
- Use automation to reduce human overhead (example from audience)
 - Integrate something like [OWASP Zed Attack Proxy \(ZAP\)](#) in deploy pipelines to check [OWASP Top 10](#) - this doesn't just check libraries for vulnerabilities, but emergent patterns like SQL injection, XSS injection etc and prevent them from hitting the deployed environment
 - [Security Monkey](#) for describing sensible cloud policies in code (now deprecated)
- **resource=true** in the DID Specification Registries
 - This specification is being improved, but could be a vector for a zip bomb attack or delivering executable payloads, since this doesn't clarify what the expected file should be.
- **StatusList2021** and similar revocation mechanisms
 - Index number leaks details
 - There are some mitigations to this/work being done to make this leak less.
- Is there a security/certification standard for DIDs/VCs solutions
 - Detailed report generated from assessment provided for customers

- Stripped down reports can be created at the behest of customers - often for release to third-parties (such as consumer/customer base).
 - Letter of attestation is also available
- Does security testing happen too late in the process?
 - It's part of a phased process, sometimes it comes in early and sometimes too late
 - Recommendation is pre-production but before go-live.
 - E.g., health sector there's mandatory testing once a year and they always scramble last minute.
- Does the fact that software is open source vs closed source make a difference?
 - People are very passionate about their specific solution type
 - Easier to dig around with open source software.

ACRs : Authentication Context Class Reference

Session Convener: Dale Olds / Pam Dingle

Session Notes Taker(s): Mike Schwartz

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

Protocol Failure Gap

- SAML
 - No "amr" attribute
 - No order of preference in request
 - Missing max age equivalent
- Common
 - Missing AMR age
 - Multiple ACRs?
 - Qualified strengths or qualities
- OpenID
 - Standardized attribute rep for an array/set of ACRs

Do we want to create a minimum interoperable profile for each protocol that addresses the above feature gap?

If so, should it be an OpenID standard at the EAP WG?

Here's some of what's already existing:

OpenID EAP : https://openid.net/specs/openid-connect-eap-acr-values-1_0.html
 defines: **phr**, **phrh**, and **pop**.

During this session Mike Jones sent a request to IANA to register the OpenID EAP ACR values

No **mfa** in EAP profile.

OAuth RFC 8176 defines a few (see below):

<https://www.rfc-editor.org/rfc/rfc8176>

2. Authentication Method Reference Values

The following is a list of Authentication Method Reference values defined by this specification:

face
Biometric authentication [[RFC4949](#)] using facial recognition.

fpt
Biometric authentication [[RFC4949](#)] using a fingerprint.

geo
Use of geolocation information for authentication, such as that provided by [[W3C.REC-geolocation-API-20161108](#)].

hwk
Proof-of-Possession (PoP) of a hardware-secured key. See [Appendix C of \[RFC4211\]](#) for a discussion on PoP.

iris
Biometric authentication [[RFC4949](#)] using an iris scan.

kba
Knowledge-based authentication [[NIST.800-63-2](#)] [[ISO29115](#)].

mca
Multiple-channel authentication [[MCA](#)]. The authentication involves communication over more than one distinct communication channel. For instance, a multiple-channel authentication might involve both entering information into a workstation's browser and providing information on a telephone call to a pre-registered number.

mfa
Multiple-factor authentication [[NIST.800-63-2](#)] [[ISO29115](#)]. When this is present, specific authentication methods used may also be included.

otp
One-time password [[RFC4949](#)]. One-time password specifications that this authentication method applies to include [[RFC4226](#)] and [[RFC6238](#)].

ACR. - Dale and Pam

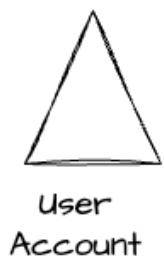
- * Person - may want to attach authn policy e.g. may express a preferences for FIDO.

- * Second place - IDP may require authn policy

- * RP may want to enforce authn policy

- * API may want to enforce authn policy

AMR is only provided in the OpenID Connect Authn Response (it's not in the request...)



ACR's are not standardized in most federations, like UK Open Banking.
Australian Consumer Data Protection regulations have standardized acr's ?
InCommon did also define silver, and gold as ACR's.

We need to be able to represent acr_values in SAML (XML) and OpenID Connect (JWT formatted)

The more granular it gets, the quicker it becomes obsolete.

The ACR is the intent at the policy level

The AMR is the evidence

Talk Session Identity in Ethereum / Jane

Session Convener: Jane

Session Notes Taker(s):

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

No Notes Submitted

Singpass: sign up with 1000 RPs

Session Convener: Tze Yuan Lee (TY) & Gayle with Assurity with Trusted Solutions
Session Notes Taker(s):

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

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

Singpass App and Digital NRIC: used by 4.2 million Singapore citizens
state owned enterprise: Assurity

six APIs

- myinfo
- identiface: government verified face biometric, through the passport systems
- login
- verify
- sign
- authorise: still in development, not released to public

Login with Singpass for sensitive use cases which requires higher assurance

Authorise product: authorization to take specific action to replace in-person attendance has traceability, non-repudiation, and security

How to onboard to Singapss APIs (The process that enabled 1000 RPs to onboard):

Simple Singpass integration steps:

- Sign contract and term & conditions through the [Singpass api portal](#)
- Follow standard OAuth 2.0 that retrieve the client id and client secret
- Merchants require Singpass to authenticate and use their corporate self (like company admin) to submit onboarding request
- Onboarding team to evaluate the use case, the legitimacy of the company submitting the if the request has a legitimate use for the data they are requesting

SESSION #9

Query Language for VCs (Presentation Exchange?) Part 2

Session Convener: Sam Smith

Session Notes Taker(s):

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

No Notes Submitted

Verifiable Credential Revocation in 2023, and What Might Be Next

Session Convener: Stephen Curran

Session Notes Taker(s): Stephen Curran

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

Presentation [Slides](#)

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

In the session we covered the approaches to verifiable credential revocation used today – List-based and Accumulator-based – with a high-level overview of how they work. We also went through the implementations that are deployed today:

- StatusList2021 (a derivative of RevocationList2020), which is efficient and scalable but shares correlatable identifiers. If your use case allows for that – StatusList2021 is the way to go. StatusList2021 is a specification but not on a standards track.
- AnonCreds v1.0 Revocation works, and does not share correlatable identifiers, but does not sufficiently scale.

We then went through two new approaches to AnonCreds-style revocation – e.g. based on Accumulators and not sharing correlatable identifiers.

- zk-SAM – Signed Accumulator Members
 - Link to [Presentation about zk-SAM](#) – Links to papers and implementation on Slide 6
- ALLOSAUR – Multi-Party Accumulators
 - Link to ALLOSAUR [summary](#) and [paper](#).

In reviewing the interactions between the participants, it was agreed that the zk-SAM was the preferred accumulator-based approach and the one that should be followed up on. That must happen in two parts – an evaluation/security proof be done by a cryptographer, and an implementation that is useful with verifiable credentials.

We also agreed that the StatusList2021 specification should be completed (to remove the caveat “*This document is experimental and is undergoing heavy development. It is inadvisable to implement the specification in its current form. An [experimental implementation](#) is available.*”)

Linux Foundation - Digital Trust Initiatives: DIF, Hyperledger, Open Wallet, TOIP +++

Session Convener: Daniela Barbosa

Session Notes Taker(s):

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

No Notes Submitted

YOUR DID Method Sucks - Change My View

Session Convener: Gabe Cohen

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

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

- Criteria used to score
 - Sufficiently decentralised / decentralizable (trustless, censorship resistant)
 - Able to scale to billions while maintaining low cost (< \$0.10)
 - Robust features (DID resolution endpoints, multisig, recovery, CRUD, multiple key types, crypto agility)
 - One canonical state with point-in-time resolution
 - Able to implement across multiple permissionless anchor systems (not multi-anchor!)
 - Limited complexity
 - Memorable unique names
 - Flexible resolution (on/offline)
 - Globally discoverable
- Answer: L1, or secure L2 sidechain

Privacy Enhancing Mobile Credentials (PEMC)

Session Convener: John Wunderlich, PEMC WG chair, Kantara Initiative
Session Notes Taker(s): Heather Flanagan

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

<https://kantarainitiative.org/groups/pemc-wg/>

[Early Implementor's Guidance Report Editor's Draft](#) (ping John W if you would like comment access)

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

[Introductions]

The Privacy Enhancing Mobile Credential (PEMC) WG is working on the Early Implementer's Guidance for how to establish a mobile credential usage environment in a privacy-enhancing manner. There is a useful diagram on the website to show how each entity in a trust triangle (Holders, Verifiers, Issuers) should interact based on a well-known privacy framework.

The basic triangle is more complicated than just Holders, Verifiers, and Issuers. There are also the providers, the natural person, and various vendors that are involved in the use of these credentials. It makes for a complicated ecosystem.

“Out of band governance” - when you talk to some technical people living in the middle of the triangle, privacy is “taken care of” because we have \$technology (e.g., cryptography). But others consider privacy to be more than that.

Mobile credentials have the possibility of being better than paper credentials because information that is not relevant to the transaction (e.g., seeing your home address) is not shared.

A requirement for providers, issuers, or verifiers is to “take the other path” that supports a privacy enhancing version of the transaction.

[Slide Deck]

The Implementer's Guidance should (eventually) inform a requirements document. The requirements document should further inform profiles for different use cases. For example, the privacy expectations at a bar are very different from the privacy expectations at a top secret government site.

The privacy principles informing the Guidance are from the ISO/IEC 18013-5 Annex E Privacy and Security Recommendations, which were derived from ISO 29100. Note that notice and consent are just one consideration and that what is sufficient for notice are different depending on the circumstances.

Q: We are in a place where notice and consent effectively has no meaning. So what is the way out of having that implemented everywhere? What societal change needs to happen?

- Notice and consent won't go away, but there are three likely alternatives: You can have agents acting on your behalf (a trained ChatGPT). You can have political/regulatory consequences related to modern needs. You can have people dig in their heels and pushing back. We probably need all three to actually be effective.

One key focus is between the Holder and Issuer, and it's good that Google and Apple are active in the PEMC WG.

Q: Is that a breach? A: No, because it is in the notification. Also, there are protocols and technologies that do allow some tracking of what's happening downstream.

Q: Some people want to turn notice and consent around. Why shouldn't the entities agree to our terms, which we could do at scale? IEEE P7012 has an idea that there should be machine readable privacy terms that both parties would agree to (e.g., j-link).

The Holder's privacy is very dependent on the Provider (e.g., the wallet). The Guidance also goes through the privacy framework for their context. And whether it's an mDL using mdoc or a VC doesn't matter. The Guidance is technology agnostic.

The guidance for the Issuers doesn't touch on how they collect the information that they use for the credential. AAMVA is a member of the working group and helps inform these requirements. Note that many of the requirements on Issuers are imposed by Verifiers.

"Inform and educate customers about privacy" is a difficult bar, because customers so often do not care. Can we express the requirements such that the customer doesn't have to learn more? Remember these requirements are for Issuers, and those Issuers may be in a highly protected context (health care) or not.

There is bias sometimes offered because of the credential format that if it were machine driven would not happen (e.g., rental car agents aren't comfortable with digital driver's licenses where they are comfortable with a physical driver's license). This is also a difference between digital and digitized credential.

Each section in the Guidance report is conveyed re: a few common use cases and what those would look like for the specific stakeholder being offered guidance in that section.

- Age verification
- Biometric proofing on device
- Credential pre-check

There is another working group at Kantara, Advance Notice and Consent, that may be of interest. For the PEMC WG, meetings are every Wednesday at 1pm ET/ 10am PT.

Q: Are there any topics considered infeasible from a technology perspective that needs a regulatory approach? For example, issuer/verifier collusion and data retention. A: In the

accountability section, there is often a requirement for a privacy policy. Actually designing regulation, however, is out of scope.

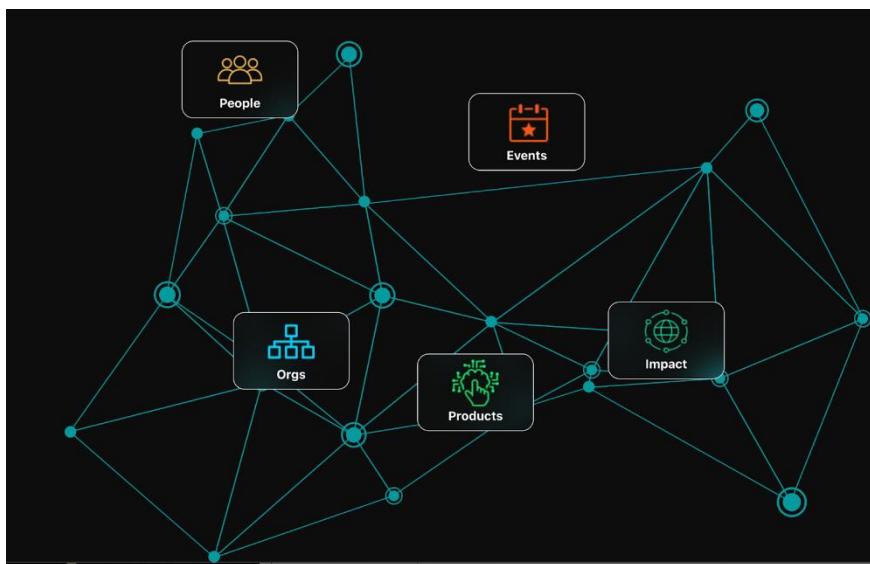
Eventually there will be a conformance test in Kantara.

Why Open Linked Trust

Session Convener: Golda Velez

Session Notes Taker(s):

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



<https://linkedtrust.us>

<http://cooperation.org/credentials/v1/>

<https://github.com/WebOfTrustInfo/rwot11-the-hague/blob/master/final-documents/composable-credentials.pdf>

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

Discussed concept of embedding trust claims into a linked social graph via a few methods:

- * having a common subject for multiple claims
- * composing claims signed by different issuers into a larger claim signed by an umbrella issuer
- * addressable and resolvable claims as first class objects you can make claims about

* including a source that may not be a signed source, and signing that that source is the one

making the claim according to the issuer (ie spider scrapes a website making an assertion)

Then we dived into a use case in supply chains with an explicit chain of trust delegation that might require calculations over the contents of the claims to determine if the delegation is valid (ie not just the fact of a parent issuer, but the contents of the credential from the parent)

Joys & Miseries of Structured Data - Analyzing the Life Cycle of Authentic Data /

Session Convener: Jean F. Queralt

Session Notes Taker(s): Jean F. Queralt

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

This session revolved around the analysis of the lifecycle of structured data and the different digital harms it could undergo.

During the session the following topics were discussed:

- How to measure “twin-ness”
 - Structured across the following dimensions (A3 model)
 - Authenticity
 - Accuracy
 - Agency
- Structured data lifecycle
 - Are there fundamental operations?
 - CRUD
 - Notifications could be considered a type of fundamental operation
 - We couldn’t verify if there were a combination of CRUD operations that could be bundled as “primitives”
- Taxonomies
 - Data Use Cases
 - Description of prototype data exchange operations between digital entities that affect digital twins
 - Digital Harms
 - Series of operations that disrupt the A3 model depending on Data Use Cases
 - Digital Rights
 - Operations that would proactively avoid a given Digital Harm and preserve A3
- An initial diagram on structured data’s lifecycle

Further research will be conducted and shared in future sessions.

AuthZ and SSI: Architecture for using an external authorization engine in an SSI ecosystem

Session Convener: Jacob Siebach (Abacus) and Mike Ebert (Indicio)

Session Notes Taker(s): Jacob Siebach

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

jacob@abacussauthz.com, mike@indicio.tech

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

Starting after meeting at IIW 35, Mike and Jacob worked to connect their two technologies, Indicio Proven (SSI wallet/agent technologies) and The Abacus (external authorization engine). The following is a description of the architecture used to accomplish this.

The architecture is such that a user has a connection with an organization (say a bank), and that results in a user receiving a verifiable credential from the organization. From an SSI perspective, the user's wallet/agent has a connection with the organization's agent.

When the user authenticates to the organization and attempts to do something, the authorization is checked to see if the user has permission to do whatever it is. At this point, the organization's system calls out to the external authorization engine to see if the user is authorized. The engine checks its policies and discovers that it requires a verifiable credential. At this point, it reaches out to the organization's agent and asks it to request the credential from the user. This is important because the user should NEVER have a connection to the authorization engine, which is on the back-end of the organization! Once the user approves the sharing of the credential (or the request times-out), the engine issues an authorization decision and the organization proceeds according to the decision.

From an acronym standpoint, The Abacus is the PDP, the organization is the PEP, and the policies are created in The Abacus with the PAP out-of-band from the user flow.

The advantages of this architecture:

- The authorization engine does not need to create/maintain any connection to the user; only the organization does that
- The organization can craft authorization policies that allow the use of verifiable credentials
- Reduced friction for the user (compared to an architecture that would require the authorization engine and the user to create a connection)
- The organization does not need to hard-code policies into their system
- Since the authorization engine is isolated from the users (being on the back-end), there is additional security for the policies
- Separation of the systems allow for the improvement, replacement, maintenance of the components individually

Security Encryption Authorization GUNdb peer2peer graph - access control for distributed storage and compute

Session Convener: Colten Jackson
Session Notes Taker(s):

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

No Notes Submitted

Want to make revenue with Identity? Quit talking about Identity

Session Convener: Rebekah Johnson
Session Notes Taker(s):

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

www.numeracle.com

Entity Identity Management - “Through our Entity Identity Management™ platform, we’ve enabled hundreds of legal entities to prevent improper call blocking and employ best practices to reduce spam labelling from harming the phone numbers that represent your business.” Unbeknownst to the buyer, they have implemented an identity management platform from which its identity is stored, managed, distributed and empowered.

Verified Identity - Entity Identity that’s been verified

Case Studies of business impact with a Verified Entity

Identity: <https://www.numeracle.com/resources/case-studies-industry-whitepapers>

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

Story of Rebekah Johnson, founder and CEO of Numeracle established 2018. The session covered her journey from launching an entity identity solution to solving legal entities’ robocalls from being mislabeled as Fraud or Spam to consumers.

In 2016, The Federal Communications Commission (FCC) established an industry led Robocall Strike Force chaired by AT&T CEO Randall Stephenson. [First Meeting of Industry-Led Robocall Strike Force | Federal Communications Commission](#). This was an invite only group largely composed of telecom providers. Rebekah Johnson served on the Empowering Consumer Choice working group while at West Corporation (before the company fired her because she had a strong opinion). While in this group, Rebekah raised many red flags to the approach of presenting calls as Fraud or Spam to wireline and wireless subscribers. This was rooted in the fact that the terminating carrier, such as AT&T, would not know which calls are from legal entities (Social Security Administration) or bad actors (Social Security Scam). Having followed the concept of “identity” throughout her career (1999-present), saw the decisions being made would be gravely detrimental to consumers and businesses. Doctor’s offices stood to potentially be labelled SPAM/FRAUD and therefore the patient might miss an important call. As expected from large corporations, Rebekah was told repeatedly to be quiet. As expected from Rebekah, she was not.

Fast forward to April 2017 and Rebekah receives a phone call from Verizon’s federal regulatory counsel letting her know her name keeps coming up, they’ve decided to take her stance, so what should they do? After picking herself up from the floor, her first response was - “I know what to do and we need more voices at the table.” Rebekah established the [Communication Protection Coalition](#) under the association PACE. The first meeting was held in Washington, D.C. and attended

by all major wireless carriers, FCC, FTC, CFPB, enterprises, and analytics providers (those with the artificial intelligence not based on identity).

From this coalition ultimately came the definition of the problem and solution allowing Rebekah (before there was Numeracle) to work with stakeholders on a solution through verbal agreements, ultimately FCC rulemaking and standards adoption (STIR/SHAKEN specs). So ended 2017 and Rebekah's role as an independent consultant.

While the problem was properly defined and the solution was proven to work (MVP = excel files being exchanged), the market was not ready to accept or understand that Identity would solve the problem. Numeracle's first year of existence generated only \$163K in revenue and that was from companies "letting" Numeracle try to solve its problem. Rebekah's mounting frustration turned into pushing identity harder to no avail. So, she threw her hands up in the air and said "Fine, all I'll do is remove fraud and spam labelling from your calls." BOOM! Market responds, companies tell their friends, and the 2nd year is over \$600K.

While you are the expert in identity and know the positive impacts a verified and trusted identity can have, that doesn't mean your buyer understands the identity's role in solving its problem. The market doesn't understand this concept and therefore does not apply any value to identity. This does not mean there isn't value, but you are building an identity solution because you want someone to give you money in exchange for the identity. Let's be honest. Let's be real. With ourselves. You are asking for money from VC's because you want to make money. That's ok. We need that to support our families.

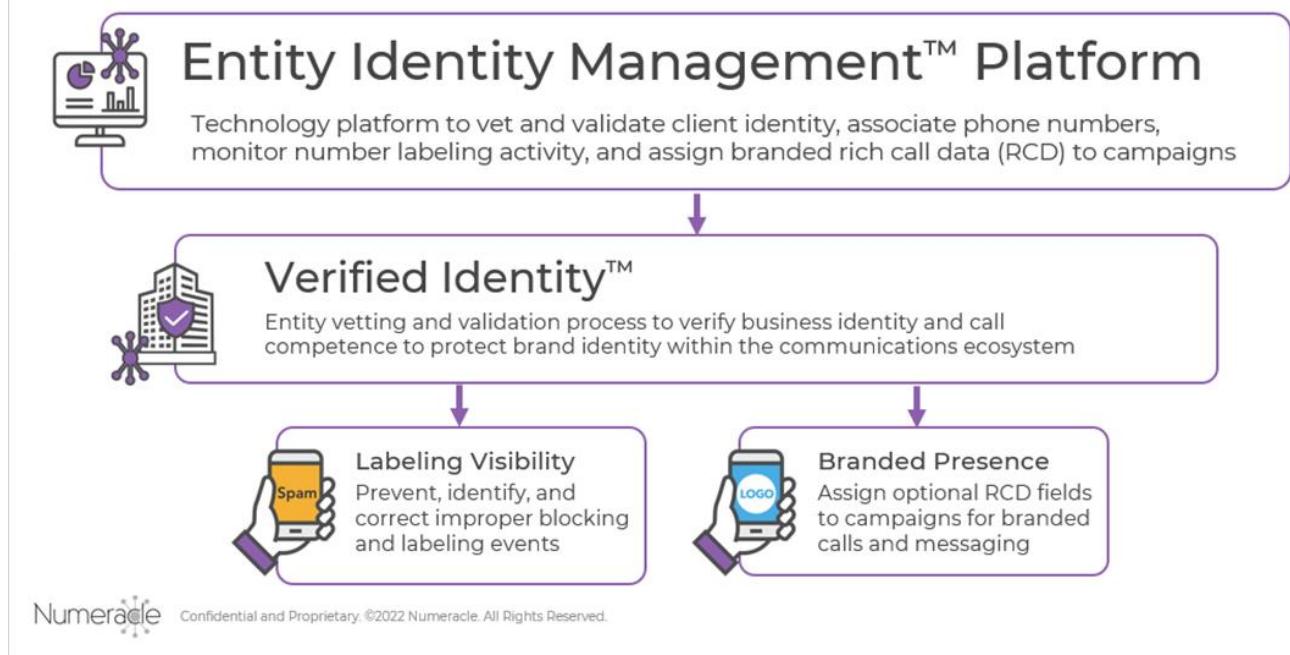
Therefore, how do we get revenue?

Learn from Rebekah's lesson with these key takeaways:

1. Stop looking for big problems to solve and start with the small real adoptable opportunities.
2. Clearly define and thoroughly understand the problem Identity can solve without using the word identity.
3. Nobody is going to ask for Identity to solve their problem. You are responsible to solve their problem with identity by keeping that unknown to the buyer.
4. For B2B Entity Identity - if you want a business to pay to be issued an entity Identity, then your job is not only to create the trusted, verified identity but most importantly do all the work to empower the business with that identity which results in revenue for the business.
5. Go to trade association events for specific industries and ask to listen to their industry challenge sessions. Your user base is literally white boarding problems related to identity but they don't know that's their problem. Listen and solve the problem, don't force your solution to solve the problem.
6. It's not all about you and your ego has to be checked at the door. Your buyer may never acknowledge identity was the solution they needed but their lives will be improved and that's what matters most to them.

8. You are absolutely capable, just rotate the canvas of your creation and gain a new perspective.

Rebekah shared her structure for deploying and managing Entity Identity through EIM. It is the responsibility of the Identity provider to EMPOWER the identity all the way through the process. Don't sit there and wait till you have a lot of "identities" before power is given. An identity standing alone on its own must give that identity power to something.



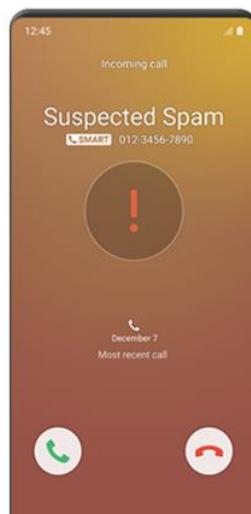
Problem

Robocall **scams** have eroded public trust in communications

Incoming "Spam" calls and texts from unknown numbers are **ignored**

Businesses conducting business via phone and text are **losing** up to ~\$M in revenue per year

Incoming Call From:
UNKNOWN SOURCE



Proven Solution

Verifying the source of the incoming communication restores **trust**

Calls free from “Spam” labeling, including brand name and logo are instantly **recognized**

Businesses stay **connected** to their customers, prospects, members, etc.



Numeracle Confidential and Proprietary. ©2022 Numeracle. All Rights Reserved.

The solution slide above doesn't even mention the word identity, security, standards, KYC, SSI, KERI, credential, blockchain, etc. Numeracle started talking about the solution this way in the market. The message resonated simply that there were instances when the client asked for the contract and signed the same day. BOOM! The problem of communicating the solution was solved.

Want to sell identity? Don't talk about identity!!!!

From Rebekah Johnson:

Because I was working from an old pitch deck during the presentation, I thought I'd share Numeracle's ARR model up till Dec. 2022 for these notes. Ahem - did I say no one would fund me? According to all the VC's who wasted my time "They are my biggest fans." Personally, I don't need fans and instead I'll take my paying customers. Thank you, next.



Note for RJ: I totally forgot during the presentation that 2019 was not \$800 because of the accounting model post my amazing CFO. My CFO also doesn't like to put 2018 (first year) due to it being \$163K, but I think it should be there. Humble beginnings.

When I return, I will do a session on "Powerful POCs Worthy of News". The following links are press releases from Comcast and T-Mobile who participated in Numeracle's POC. I was sick and tired of the standards body arguing whether the standard would/should work so I just did it to kill the naysayers. It worked.

Again, "Identity" is not mentioned but for those who know, you can see the true solution in the opening paragraph.

"Using **public key cryptography** and the global STIR/SHAKEN family of **protocols**, Rich Call Data allows **legitimate callers** to tell recipients exactly who they are, where they're calling from, and even why they are calling, with the **highest degree of trust and certainty**. This technology is particularly important for enterprise callers, who need reliable tools to reach their customers."

Nov. 2020: [Technology Companies Complete First-Ever Telephone Call with Authenticated Caller ID and Rich Call Data, Powered by STIR/SHAKEN](#) - At the next event, I'll show a video of my reaction when the first call was delivered. I hosted a little virtual event for all the engineers and stakeholders to celebrate this moment together. Ya'll - it was pandemic time and we still did this!

July 2021 - [T-Mobile and Partners Complete First-Ever Wireless Call with Rich Call Data](#)

Couple fun notes:

1. Yes, this was in my pitch deck and VC's decided it just wasn't a good fit. HA!
2. Isn't it funny how BOTH Comcast and T-Mobile claim to be the first. If you'll notice, there are some players who remain the same....Numeracle, Everbridge (my client), NetNumber (my fun innovator partner which really was just Doug Ranalli who since sold NetNumber).

Please note that even though your hard work could very well not be acknowledged and even have false claims made to take credit, such as ""We congratulate T-Mobile on the successful proof-of-concept, which relies on the industry-backed centralized registry, Registered Caller™." Don't let it roll off your back! Get mad, angry, disappointed, upset, frustrated and then dust it off and keep driving forward. Their lies cannot replicate your knowledge.

Listen to some recordings from the people who participated in the POC.

[CTS Session Keynote NetNumber The Next Step In STIRSHAKEN](#)

[Enterprise Multi-party STIR/SHAKEN PoC Demonstration](#)

Rebekah

Numeracle - Call blocking verifiable identity solution (EIM) Entity Identity Management Platform

Problem: Call blocking the wrong callers because no verifiable identity for calling parties (companies/organizations)

- Create awareness for the problem your solving
- Stop talking about identity in and of itself
- Have the ability to stand up a solution quickly
- Simplify the solution if at all possible so it works with

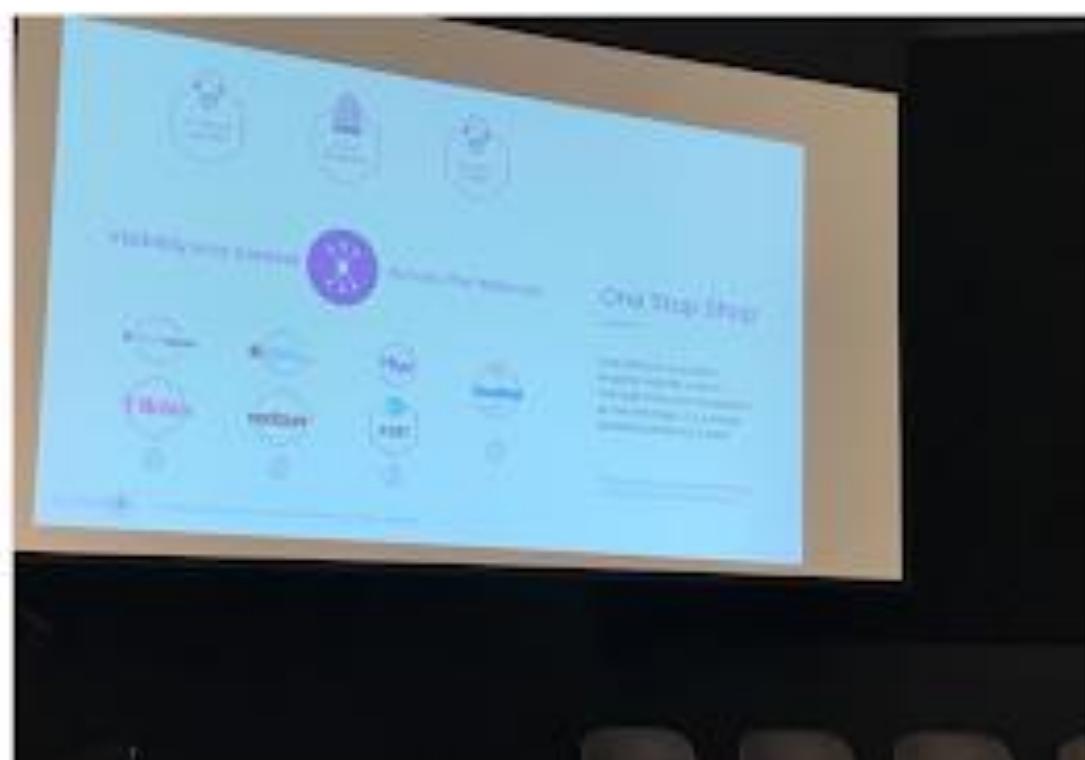
Financial success

- No venture funding
- Hockey stick revenue stream
- Know your runway

The nature of identity

- Indifferent to types of identity
- Will package anything and distribute to any channels

Measure performance



Public Private Partnerships - What's needed for success? Identity Ecosystem or Archipelago

Session Convener: Kenneth Gantt (The ID Guy)
Session Notes Taker(s): Tchaikawsky Samuels

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

[National Strategy for Trusted Identities in Cyberspace \(NSTIC\)](#)
[trustoverip.org](#)
[Restrict Act](#)

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

Are we after an identity ecosystem or an identity archipelago...

[National Strategy for Trusted Identities in Cyberspace \(NSTIC\)](#)

What do you want to do for someone with their unique identity data in regards to:

- identify
- verify
- credential

The sovereignty of data collections between B2B and B2G and individuals means that scope affects the framework for interoperability.

[trustoverip.org](#) performed a study to compare the identity ecosystem with biological eco-systems
What public-private partnerships are needed in order to address biometrics use?

Marketing and confusion could be the source of the publics preference towards a private service over a more affordable public service.

Data sharing rules like VAW Act help manage privacy

DHS-DOD-DOJ_etc. are all connected for the purpose of national security.

Questions & Answers:

What is stopping gov't from changing its sharing rules?
Congressionally passed bills & Executive orders.

What's stops DHS OBIM from sharing in a way it is not supposed to?
Routine External Audits by the FBI
How are sharing limitations managed?
Hard coded based on sharing agreements established prior to sharing begins.

What is stopping someone from breaking the rules and sharing the information with the public?
Clearances, recurring vetting; the same challenges faced by private industry.

How do executive orders effect what DHS OBIM does with individual's biometrics and vice versa?
Collaborative efforts between the administration and SMEs help to inform and alert each other of upcoming changes.

How do you run a public-private partnership?
Clear is an example of private corporation.
Govt' process is less convenient and time consuming. It's also out of the way.

A challenge growing public-private partnerships is: What has to be taught and shared with the private sector to enable partnerships that do no violate standing law.

What does success look like? Looking past perceptions to establish trust.

Audience Statement:

Restrict Act diminishes trust.

SESSION #10

OpenID 4 Verifiable Credential Issuance (was DID4VC 101)

Session Convener: Tobias Looker

Session Notes Taker(s):

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

No Notes Submitted

SPAC #2 = Secure Privacy Authenticity Confidentiality - Tradespace Strongest A+C+P

Session Convener: Sam Smith

Session Notes Taker(s):

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

Sam Smith's SPAC whitepaper

https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/SPAC_Message.md

Slides from Presentations:

https://github.com/SmithSamuelM/Papers/blob/master/presentations/SPAC_Overview.web.pdf

AI Why We Need DID's NOW

Session Convener: David Yap

Session Notes Taker(s):

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

No Notes Submitted

Identity Collaboration *SDG* Untangling Chains of Society (SDG) Supply Chain, Portability, Interoperability, Value Chain, Trust Chain / Lubna D

Session Convener: Lubna D
Session Notes Taker(s):

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

No Notes Submitted

Internet Data Usage Control System - JLINK / John Wunderlich

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

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

No Notes Submitted

Human Rights Affirming Government Identity AND FSLTT @IIWXXXVI Fed, State, Local, Tribe, Ter - We are here from Gov, we should talk

Session Convener: Elizabeth Garber, Mark Haine
Session Notes Taker(s): Heather Flanagan

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

Check the OpenID.net website for future announcement re: a public review of the white paper (currently in draft and in a private review)

[Online public consultation on the draft OECD Recommendation on the Governance of Digital Identity](#)

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

[Slides]

White paper is designed to be in support of UN Declaration of Human Rights. As it turns out, it's also very supportive/complementary to the recent [OECD Recommendation on the Governance of Digital Identity](#).

Paper is also looking at the different types of technology architectures (public/private governance on one access and centralized/decentralized on the other access). The location of flags is open to for debate.

Q: do you talk about why there are different approaches being taken? A: there is a country by country analysis, but not asking "why did they make this choice" per se from a cultural perspective. There is reference to the goals of the systems. Note the 2016 Consult Hyperion report has useful information in this direction, though it is a bit old.

Q: human rights are not cultural in the way that policies can be cultural. You could look at the human rights framing as being able to access a digital good with a digital credential (right of free association) across jurisdictions. A: that should be something the governments decide upon and make their constituents aware. This paper is not trying to make judgement calls, but it is implied that interoperability is required.

Q: some systems were not built for interoperability. Aadhaar was not designed for interoperability; it's centralized for a reason. A: In the OECD paper, and that we we also build on, is that interoperability is critical.

Q: Is the paper going to try and be useful to governments, helping them to be more effective in their goals, or are we going to patronize them re: what they are focusing on? A: from a tonal perspective, trying to be very open and generous in our recommendations.

Q: Looking at the chart and implementation, where do you start the baseline? A: this chart asks future implementors "where do you want to be on this chart?" There are risks and tradeoffs for every approach.

Q: if you've already mentioned standards, there has to be a minimum platform aspect for some level of interop so everyone can exchange the same types of data. A: we have been putting in commentary in the paper that says they are critically important, and that's one aspect to take into account.

Q: In the context of gov't, what does interoperability mean? Is it gov't to gov't or broader? There are layers of interoperability. A: Depends on which goals the program is wishing to address. Interoperability with private sector may not be critical if that's not a goal.

Q: this dimensionality doesn't feel good for suggesting it could help governments figure out where they want to be. The distinctions taht might be better are "how does a particular sovereign decide to do surveillance? How do they balance surveillance with accountability?" We're talking about digital identity, not e-commerce or IP. In the context of digital identity, we have a dual-use technology including dimensions of self-censorship, freedom of association, surveillance. Maybe use those three axes, or maybe there are more. And instead ask, based on your culture, what is

your goal relative to identity? If we can make the triangle orthogonal enough, we are respecting their perspectives. A: there are multiple dimensions and we are only showing two in this chart.

Q: if you took this alone and ask “where would you like to fall on this chart” it’s the wrong question. Should say “what are the use cases we are envisioning (public and private, just public, other).” Or “What is it we’re optimizing for? (e.g., accessibility, equity, safety)”

Q: Did you mention in the paper what these systems have achieved? A: We profiled each of the systems in this chart and what they were trying to achieve and the big successes the gov’ts are trying to cite and what are the low cases.

High level insights (noting that the paper needs to be more opinionated, esp. in the technological spaces.)

- gov’ts need to approach this as a holistic strategy
- must be a human-centric design
 - “avoiding harms” means allowing feedback and being able to test if harms have happened
- community engagement
- interoperability
- mature emerging standards
- tools and rules
- Institutional protections
- trust establishment at scale

For the more tech focused ones...

- human-centric design = in the India case, they decided the tech must actively avoid commercial platform dominance. They also invented the Beckn (sp?) protocol, which is not designed around identity at all. It allows the edge agents to get the same usability benefit that people expect from using something like Amazon. If you want to translate your high level insights into protocols, you need to make very clear statements as to what the goals are (e.g., inclusion, maximum human agency, avoiding commercial platform dominance). India has four or five poles/principles on the technical side that exhibit the idea that digital identity has a public good.
 - See [Beckn protocol](#) for reference

Q: Governance isn’t reference in there specifically. A: Tools imply governance.

Q: Unpack trust establishment at scale A: it’s about different parties in the trust network needing to establish, maintain, and revoke trust. What are the standards/policy and protocols that enable that? This is an unresolved problem in the ARF, as an example.

Note: the OIDF is working on a proof of concept for a network of networks.

Q: is privacy to be assumed in tools and roles? There is data privacy but that’s different from human privacy. A: in institutional protections, we talk about how we need to look at how gov’ts

around the world interpret human rights. Q: human rights is not being treated as a static, global thing.

Q: can we come up with some very general considerations? If a gov't is effecting people who have no recourse, that's a fundamentally a problem. Need to change the nomenclature of what is a state. Which is outside the scope of the paper, but journalists need to start talking about states and stateless areas.

What are the necessary tradeoffs? There is often a tradeoff between privacy and security. But perhaps it's "privacy" vs "control of bad actors" which comes across as a different view. The requirement we have to put controls in place have interesting consequences for privacy. You can't deliver on the control side of things without impacting privacy.

Q: in the technical sense, it's not a dichotomy between privacy and security. You need to think in terms of accountability and different methods to linking surveillance to enforcement. Depending on what a jurisdiction does and how they use courts, you can end up with technical designs for linking the accountability of the participant in a transaction with the transaction. It's not about privacy, and privacy is not helpful in this context. What is the governance/legal process that's going to hold bad actors accountable. That gets you further in the technical design.

Are there pieces of technology or standards that we should be specifically opinionated about that would help drive interoperability, trust at scale, etc?

- you have an opportunity to help people grapple with tradeoffs. When you have a preference, express your preference. Explain the context of the tradeoff. The moment you start encroaching on "what is a human right" it is interesting but you are not authoritative. Come from the perspective of an identity expert perspective.
- would like to see what the users want. What problems are we trying to solve? Do my consumers and users care?
- the complexity of user control of data adds tension to the control we want to give them and the equity of what they can handle.
- what is the minimum thing that we need to be prescriptive about? We're making an assumption of Internet interoperability. Call it out
- could be more prescriptive by pointing to a few standards in particular, when we say support evolving standards, here are some to consider. When we're talking about security, it needs to be end-to-end security. Privacy also needs to be considered end-to-end. Some of this will be "obvious" and yet still important to cover.
- Consider separating the digital rights that one should have from the ability to exercise them. If you're dealing on axes, one of which is that we all have some degree of a digital twin, what rights do we have over our digital selves? What hybrid of control exists on that axis? And even if we do have complete control over that axis, what does our gov't or marketplace enable us to do with those rights?
- Four quadrant draft, describing the thought process as to why they are in their spot would be helpful. Also, the attack vector might be different from country to country (e.g., not everyone has a mobile phone)

Expanding The Language = Techorata Informed and reflected on by the = Desiderata - Joyful, Contemplative & Serious

Expanding The Language: The Technorata informed and reflected on by the the Desiderata

Session Convener: Jeff Orgel

Session Notes Taker(s): Jeff Orgel

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

In my experience, the Desiderata is one of the finest writings expressing caring compassion in the interest of others. While guiding the reader through managing the sometimes-challenging weather of our days, the author, Max Ehrmann, maintains a firm grasp on joy which may otherwise seem displaced by those challenges.

I am humbly inspired to approximate that same effort and outcome in what I am referring to as the Technorata. Managing the sometimes-challenging weather of our days is a fundamental skill set. The dual topographies of Real World and Digital Landscape now insist on having ownership of this ability two-fold; navigating the daily world our feet stand in with traditional means, and managing the digital relationships we extend ourselves into via technological means - in particular connected systems like social media and our behavioral presence in the digital realm. Protecting joy while being able to manage disappointment is even more crucial in this era of what weighs on us and how that weight manifests.

I was somewhat frustrated to find my first attempt(s) to have nearly twice the language as the Desiderata...or more...until this happened...

During my recent presentation at the Internet Identity Workshop 36 one of the participants observed something which manifested in a sketch. As we were loitering over the details and contemplating the additional weight of these days what had appeared as maybe not so much the idea of managing ourselves where our feet are planted AND a Digital Twin (an extension of ourselves into the digital landscape) but possibly a different fact of the matter. We are only ONE person trying to manage a space of accountability which spans distance from where our feet are planted all the way to the edge of where our digital relationship(s) now range. From that point of view, we see these challenges.

How many social network connections am I accountable to? How many people is that?

How many inbound messages is that? How many responses do I owe?

How much accountability to all of it...or some portions or it do I have?

Which are the priorities...and which can I afford to respond to at another time?

Will those choices possibly cost me goodwill...or cause misunderstanding by others?

After that consideration it was not as much a surprise to find myself using twice as many (or more) words as building blocks in my expression. We are now often dealing with personal connections and accountabilities which could be double, triple or more, than we might experience in 1927 when the Desiderata was written.

That said, here is my humble offering in caring to care for each other...the Technorata, preceded by the Desiderata that it may set the tone.

Desiderata

Go placidly amid the noise and haste,
and remember what peace there may be in silence.

As far as possible without surrender
be on good terms with all persons.
Speak your truth quietly and clearly;
and listen to others,
even the dull and the ignorant;
they too have their story.

Avoid loud and aggressive persons,
they are vexations to the spirit.
If you compare yourself with others,
you may become vain and bitter;
for always there will be greater and lesser persons than yourself.
Enjoy your achievements as well as your plans.

Keep interested in your own career, however humble;
it is a real possession in the changing fortunes of time.

Exercise caution in your business affairs;
for the world is full of trickery.
But let this not blind you to what virtue there is;
many persons strive for high ideals;
and everywhere life is full of heroism.

Be yourself.
Especially, do not feign affection.
Neither be cynical about love;
for in the face of all aridity and disenchantment
it is as perennial as the grass.

Take kindly the counsel of the years,
gracefully surrendering the things of youth.
Nurture strength of spirit to shield you in sudden misfortune.
But do not distress yourself with dark imaginings.
Many fears are born of fatigue and loneliness.
Beyond a wholesome discipline,

be gentle with yourself.

You are a child of the universe,
no less than the trees and the stars;
you have a right to be here.
And whether or not it is clear to you,
no doubt the universe is unfolding as it should.

Therefore be at peace with God,
whatever you conceive Him to be,
and whatever your labors and aspirations,
in the noisy confusion of life keep peace with your soul.

With all its sham, drudgery, and broken dreams,
it is still a beautiful world.

Be cheerful.
Strive to be happy.
— Max Ehrmann, 1927

Technorata
(working draft)

Go Placidly amid the torrents of information and the mountains of story. Know what peace there is in the offline world away from the noise of digital realms and connected networks flowing into your real world.

While honoring your own values and intention recognize that others, like yourself, must also navigate the challenging technological weather and landscapes of these days.

As you hear more voices more often, realize that your idea, well thought out and well-balanced, is an honorable pillar to offer and stand upon. Be enthusiastic to check your standing in the light of other ideas and beliefs. Any person knows something better than you, like the story of themselves. Honor and respect what they may be able to bring to you.

Avoid fraught and overly aggressive signal and noise whenever possible. Sanctuary and peaceful space can be a worth beyond measure. Guard against allowing disruptive or random encroachment. There are spaces outside the frenzied techno-circle dance which allow you to be a present without being swept into what may often be chaos.

Sit comfortably where and how you wish. Honor yourself as you are. You are often best served by not drinking from the cauldron of FOMO, so often served, so many ways.

Though the noise of stories, opinions and salesmanship of others may seem deafening by default, know that you have dominion over these forces even if it may only be through managing your perspective.

Keep interest in your passions whatever they may be. With diligence, discover and deliver what it is about you that puts a bow on the people and community around you. Your world awaits being made better by your gift.

Though some will work to dim or obscure the shine of your best, know that the truth does not hide well. It will eventually appear - even within a storm crafted to obscure it. Ill weather clears and as you withstand the battering effects - so shall the brightness of your truth. Also be prepared for support you do not expect. The goodness of others is everywhere in many forms.

Be yourself. To act otherwise is tangled with the work of creating, building and projecting a non-truth about yourself. You cannot hide your true self forever. The people closest to you will often be the first to notice as well as being the first to suffer the cost of losing the original and true you.

Allow the wisdom of the years to craft and hone your sensibilities. Refine and evolve your true self. Allow prudence and caution to protect against impulsiveness and blind trust. Allow spontaneity and belief in others to encourage grace amidst cynicism and mistrust.

Learn to hold to the shield of compassion for others and their offerings. Teach what you have learned. Build wisdom of community to ensure the best opportunity for the light of guidance and mutual support in times of challenge and darkness.

Beyond a wholesome wisdom, be gentle with yourself. The New Digital World landscape developing around you is not what we were designed for. The ancient design of a person to existing on the land and its realm of convergent forces now may be entwined with an artificial and human structured digital realm. As you exist within this new born realm you carry this infant in a relationship completely new to your world.

While the digital native child is often comfortably frolicking and swinging on the vines of connected systems, impulsiveness and immature judgement is the hackable vulnerability of youth which entangles them in system intentions.

Where the digital immigrant elder may often be hesitant and struggle with comfort, fluency and understanding, in balance is prudence and the wisdom of judgement gained from lived experience. Many lessons, wisdom and real-world judgement are transferable to digital landscape though it may be contorted by the weather and topography of connected systems.

Expect to see new things and be prepared to think in new ways. Be aware and wary of the affect and effect of this digital twin on your Real World.

Be at peace with your sensibilities, however you come to them. Know and value that there will always be others to learn from and for you to teach.

Respect of others and their thinking allows for the best possibility to navigate most issues regarding prejudice and bias. Find and build circles of respect and welcome others to fortify your community with their best angels. With all our differences we can create betterment when we bring ourselves together.

Know that Human Nature (HumanOS) is not elevated. It is your magnificent human mind and consciousness that keeps lesser angels at bay. Lifelong practice of wholesome spirit and gifting your community ages beautifully. Bring that into the lives of others and serves yourself as well.

Protect your joy. It is delicate and may be injured in many ways. For every sad story you can find innumerable happy ones. Whether harm of joy is caused by yourself, others or things beyond your control, manage disappointment so that it will not crowd out your return to joy.

Work to make your best possible. Be your best whenever possible.

OAuth 1st Party Native App Authentication / George Fletcher

Session Convener: George Fletcher

Session Notes Taker(s):

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

No Notes Submitted

VC's in the Supply Chain: GS1 Verifiable Credentials

Session Convener: Paul Nicolard - GS1 US

Session Notes Taker(s): Caryn Van Exel - GS1 US

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

GS1 Verifiable Credentials – White Paper on Data Model and Validations -
<https://ref.gs1.org/gs1/vc/data-model/>

White Paper Issue Tracker - <https://github.com/gs1/VC-Data-Model/issues>

Ensuring Trust Travels with Data: Using GS1 Standards with Verifiable Credentials -
<https://www.youtube.com/watch?v=iDkANArgdKI>

When Trust Travels with Data: Verifiable Credentials and Decentralised Identifiers -
https://ref.gs1.org/docs/2022/GS1_GS1US_DiDs_VC_Whitepaper.pdf

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

Paul N. opened with:

- An Intro of GS1 and GS1 US
- Review of GS1's Objective: Implement GS1 Credentials to provide digital verification of the authenticity of GS1 identifiers → Identify, Capture, Share review
- Review of GTINs

Problem Statement - Today, there is nothing to verify that the GTIN in the barcode of a product belongs to the Brand it's claiming to be. How do you know the product is genuine?

- E.g. What you ordered online is not actually what arrives at your door. There is no way to know when you buy something, it's authentic.

Audience Question - Is it quantified? *Answer* - We will look into whether we have metrics captured and if they are shareable. Amazon has published metrics around this. We will gather what we can and add to the notes.

Audience Question - Are there any products more known to fraud – *Answer* - Yes! Clothing, Cosmetics, Electronics, Pharmaceuticals are examples.

Audience Question – Can you identify a batch or origin of any given product that helps to verify? *Answer* - Depends on the product class – there are identifiers that extend identifiers to include serial numbers, batch lots etc.

Paul Dietrich discussed **Sunrise 2027 – 2D codes**

- Extends the 1D codes for scanners
- Image scanners are faster and performant enough where POS 2D codes are supported
 - GTIN in a 2D code – richer data set
 - Can hold a URL – Digital Link
 - More data available, but still can't verify the owner origin
 - 2D barcode does have a link type associated with it – normative set of data, anticipate the possibility of VCs being a link type

GS1 Verifiable Credentials

- Data model published (see links above)
- Github available, accepting comments
- Aligned with W3C specs

GS1 Verifiable Credentials



- Aligned with current W3C Verifiable Credentials Data Model
- Focus being on the claim portion as that is where the attributes required to assert a GS1 license and to declare data associated with an object may be found
- White paper created to document data model and provide examples
- <https://ref.gs1.org/gs1/vc/data-model/>



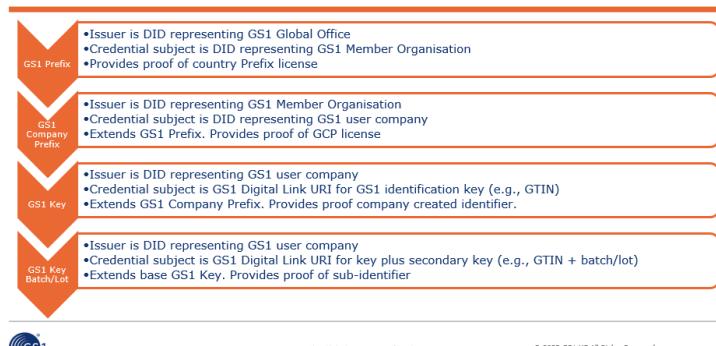
The Global Language of Business

© 2023 GS1 US All Rights Reserved

4

Verifiable Credential Chain for Identifiers

Verifiable Credential Chain for Identifiers



The Global Language of Business

© 2023 GS1 US All Rights Reserved

5

Advisory Note on the use of the 'Key' term – GS1 Identifiers have historically been called/referenced as keys, do not confuse this with cryptographic keys.

Audience Question - What DID method is used? Answer - DID web is used today. We, GS1/GS1 US must remain neutral. We can provide recommendations and guidelines on what to use, but we can't make mandates to our members.

Comment/suggestion from Audience - if we can, GS1 US should guide our members – it would help them tremendously (to narrow down the choice) and lead them in the right direction in terms of usage, viability, sustainability, extensibility and longevity.

Associating VCs with our current standard identifier structure – extends the chain of trust.

Planned Open Source Library – DID/VC Verification Library

- Members/Partners can use the library to verify VCs (GTINs, Entities (Brand Owners, Trusted 3rd Party) etc.)

- Our Credential model is designed to enable the use case where someone asserts a claim about a product - If that is signed by a brand owner, you can trace it back through this ecosystem to verify the brand owner (or delegated party) made the assertion.

Audience Question - Is the library available now? *Answer* - The Open Source library will be available later this year and released through Github. More to follow at the next IIW!

As data about products travel on the internet every piece of data can be attributed to a brand owner – verifiable when it needs to be. Not just at a certain point. ***Our Aspiration*** - Trust Travels with Data (see reference links)

Some of our larger MOs are working on initiatives: Canada, Germany, Netherlands, UK,

Audience Question – How can a consumer see an item is verified as authentic and can see that the product being offered by the retailer has been authenticated to the Brand Owner? *Answer* - No service or registry exists today that could integrate with and facilitate the authenticity check.

Audience Question - Are GTINs used in natural resources? *Answer* - Not so much oil and gas.

Call to Action

GS1 US is looking for use cases that can utilize our Digital License Ecosystem and VC Verification Library

- We are looking to pilot with companies

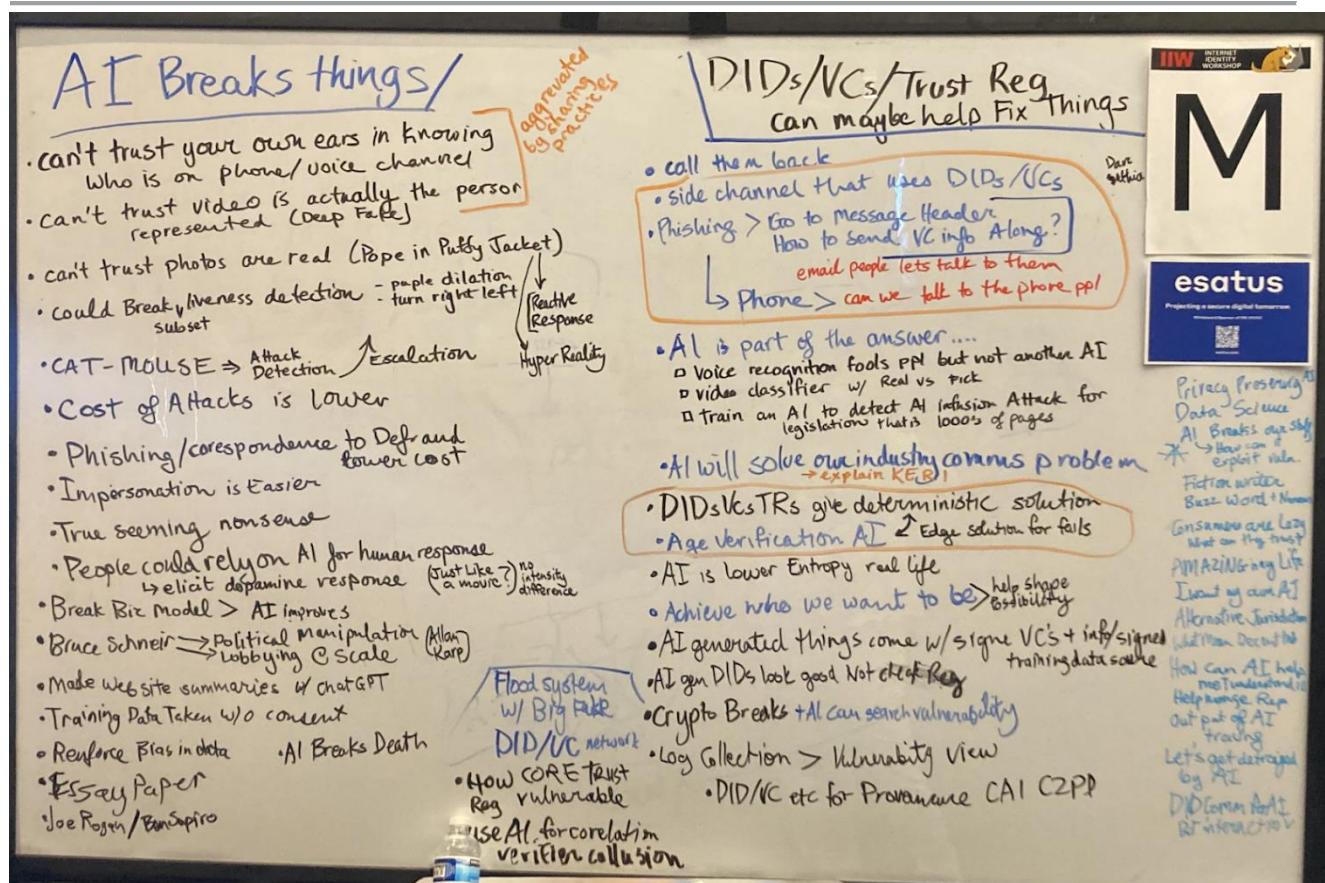
½ AI breaks ID things/cyber security and ½ How VCs/DIDs trust Registries Fixes things AI Breaks

Session Convener: Kaliya Young

Session Notes Taker(s):

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

(from whiteboard via Amie Jordan)



- AI uses skyrocketing, people don't even understand it
 - you can get a few seconds of a voice and not even know it's the person you think it is (they can replicate it)
- AI BREAKS THINGS
 - can't trust your own ears in knowing who is on the phone/voice channel
 - can't trust that a video is actually the person represented (deep fake)
 - can't trust photos are real (ie: pope)
 - reactive response --> hyperreality
 - could break liveliness detection
 - ie: pupil dilation

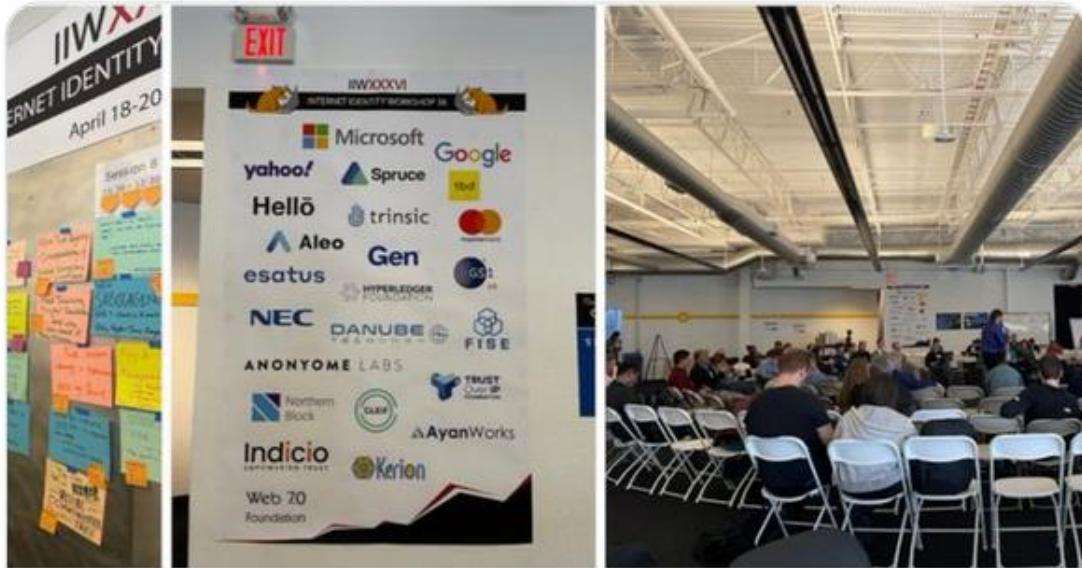
- cat - mouse - attack / detection increases --> escalation
 - costs of attack is lower
 - fishing/correspondence to defraud lower cost
 - impersonation is easier
 - true seeming nonsense
 - people could rely on AI for human response ---> elicit dopamine response
 - break biz model > AI P
 - Bruce Schneier
 - political manipulation
 - lobbying at scale
 - made website summaries with chatGPT
 - training data taken w/o consent
 - reinforce bias in data
 - AI breaks death
 - essay paper
 - joe rogan / ben shapiro
- HOW CAN DIDs / VCs / TRUST REG CAN MAYBE HELP FIX THINGS
 - call the person back
 - side channel that uses DIDs / VCs
 - Phishing --> go to message header ---> how to send VC info along?
 - email people, lets talk to them
 - phone: can we talk to the phone ppl
- AI is part of the answer, AI might be the REAL answer to fight AI
 - voice recognition fools ppl but not another AI
 - video classifier w real vs pick
 - train an AI to detect AI attack for legislation that is 1000 of pages
- AI will solve own industry comms problem
 - DIDs / VCs / TRs give deterministic solution
 - age verification AI
 - edge solution for fails
- AI is lower entropy - real life
- achieve who we want tot be - help shape possibility
- AIs generated things come with sign VCs and info/signed training data
- ai generates DIDs - look good, not check registry
- crypto breaks
- log collection > vulnerability view
- Flood system w big fake DID / VC network
 - how core trust reg use ai for correlation



Northern Block @northern_block · Apr 28

...

We had a great time hanging with our peers at **#IIW36** last week and talking about all sorts of interesting topics. Here's a summary from the event that [@mathieu_glaude](#) wrote as a guest blog post for [@trustoverip](#).



trustoverip.org

Internet Identity Workshop 36 in Review - Trust Over IP

In this guest blog post, Mathieu Glaude takes us through the conference topics that interested him the most.



1

2

58



Notes Day 3 / Thursday April 20 / Sessions 11 - 15

SESSION #11

INTEROP Profile with SD-JWT + OpenID4VC

Session Convener: Paul Bastian & Torsten L

Session Notes Taker(s): Jin Wen

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

Why

Interop across parties while being

- Privacy preserving and
- able to fulfil security and regulatory requirements

Usage

- proposal to European Commission (EC) (through OIDF/EC liaison)
- CA DMV wallet
- Basis for OWF projects
- IDunion Tech Stack
- GAIN PoC

SD-JWT profile

- SD-JWT VC with JSON payload (“typ” vc+sd-jwt)
- Definition of mapping to base media type
- issuer keys
 - OpenID Connect style=issuer URL + key id ->jwks_uri
 - x.509: iss=DN + x.509 cert chain
- Signature algorithm: ECDSA
- holder binding:
 - cnf claim with jwk
- Credential Revocation: StatusList2021

Design principle

- Well known, “freakishly” simple: such as OpenID Connect
- Well known, long term trusted such as X.509 certificate

SD-JWT VC with kid (OpenID Connect Style)

- typ = vc+sd-jwt

Now switch to x509 style SD-JWT

- contains “x5c” chain

SD-JWT VC with x.509 certificate chain (snapshot taken)
benefit: retrieve the trust chain from existing x.509, for example eIDAS 1.0

Question from Anil Johh

- sd-jwt vs. BBS+

OIDC4VC Profile

- SD-JWT profile (format id “vc+sd-jwt”)
- JWT VCs (Attestation VCs) for Wallet Authentication and Verifier Authentication
- Schemas for Attestation VCs
- client id scheme for Attestation VCs

JWT VC for wallet Attestation (snapshot taken)

Further Topics

- Dual Issuance mdoc/sd-jwt
- in-person/remote prov
- Trust Management (is the issuer really an university) not addressed yet

Transcripts:

Let's talk about the wire first.

What we want to achieve is true interoperability.

And when I say interoperability, I mean it in the sense of really on the wire, different parties can communicate to each other without having seen before.

Right.

And we want to have an interoperable profile for VCs, that is privacy preserving and that can fulfill the relevant security and regular requirements.

Because of the need, such a profile is needed and the role of the remote, bare topic credentials for the whole e-centralized identity model on a global basis.

And I also have put up a list of potential projects, community that might be interested to consume the other venues that interoperability program.

The first one is, we had a session about the European Union's EIDAS regulation, so it's a big thing in Europe.

And there is a need for interoperability across the different member states states and all different wallets will be rolled out.

As the judge, for example, of the national police, or mentioned in the area, but the level of detail in the architecture reference frame is not sufficient to really implement these U-based solutions in a different fashion.

Just to give an example, right now there is no text about how these are managed, how trust is managed, and all that stuff.

All that stuff, right.

This is really fundamental.

And simple things like, how does the VC look like.

California D&D wallet, Oliver, do you want to say something.

Yeah, so the California D&D wallet, so we are-- so we are implementing a dual provisioning approach of the California D&D at the moment, the dual issuance of mobile driver's licenses and the M-DOR can be WS3C compliant, a credential standard, and we are currently using OpenID for VP and CI as much as possible, and are interested in having an interoperable tech stack that works across borders.

- Thank you.

Yeah, and I also called another session in the morning about projects for OWF, and I would like to use our program as a blueprint, as a basis, to gather people that are interested to implement components for implementing Dart-herbal potential based on SD-JAS and Kubernetes.

There's a lot of activity at OpenID Foundation, or TESSA, is not in the room, where there is an attempt to specify a Dart-herbal potential schema that is able to convey the data that you today can request in the user input when you use And I think it's pretty simple but useful.

There are some advantages, but it also needs thinking for some.

You need to be able to shoot up things and present it and so on.

So this profile might be a good basis for implementing that user employees.

Then Christian, Paul, myself, we are working in this project called ID Union in Germany.

It's a government funded research project around SSI and T-soil and the human blood identity.

And we have been working really hard in the last year to evaluate what could be the tax debt going forward to something that is really, that makes sense and makes an impact.

The profile we can represent is mostly influenced by what we learned in the course of that analysis which was, for example, informed by the-- I would say film payments, right.

Prudential format comparison of networks.

Is that right.

Under the roof.

No.

And then there's the APOC, Global Short Identity Network.

You might have heard of that.

It's an attempt to interconnect existing identity networks to get global reach and leverage existing identities.

It's right now based on a federated model because existing infrastructure and existing identities are based on federated identity.

And where we are, and Mark is one of the co-chairs of the BNC, I'm one of the co-chairs.

And we would like to extend the reach of the POC that we are building, so we are really building a sandbox, a real sandbox where you can really see how different networks interact.

And we would like to extend that with the ability for the identity providers to also become credentialized issues.

Because that way, that identity data that exists in those databases can be leveraged in also decentralized space.

And I guess, one of the projects behind those three dots, so please tune in if you want.

So there's a huge demand and that's why we started to work on that.

I just give a brief overview and then I will also go to some examples.

So basically what we are proposing is this tool for first as a credential form we would like to use a selective disclosure job as the name of the session suggests.

And this whole thing is based on the current ideas around the VC2.

0 credential or a Marifar credential.

Right.

So we're not based on VC1.

1, we're based on VC2.

0 because that gives us much more flexibility.

And, from a standpoint, the credential looks much more natural.

If you look into that as a job person, as I am.

We will have two examples in the next slide, so please.

So basically what we do is instead of having data in the payload that you need to determine whether it's a JSON or a V or a job credential, we use a Hosea type header for that, to tag that thing that we get.

I just know we also have to define the mapping of that potential to the least major type.

This is something that we see working group define as a program for SIP form coming up with new kind of credentials.

>> Yeah.

>> Discussion.

>> So, yeah, it's a discussion, active discussion.

The WSVC very formal credential data model 2.

O specification.

>> Thank you.

>> The working group that is coming out to working on a specification.

It's not final, but it's very likely that you'll have a base media type, which is JSON-LD, but it will be possible to add entries to the VC directory, which is the extensibility model of the VC VM, and extensions for media types.

So people could come up with their own, can describe their own mapping, how you map mdocs So whatever, X509 is a difficult one to chase in LD.

As long as you can define a mapping, I think.

>> Okay, but that sounds pretty good.

>> Yeah.

>> I mean, I'm not so deeply involved with the C-word group, but I like really the flexibility of the model because it allows us to really design a simple to use company.

>> But it's, you know, active discussion.

>> Yeah, I know.

Take it as a great shot.

In the end a lot of things here in this space are still moving.

Nevertheless, I think I totally like the idea of PC2 and would like to embrace it.

Sorry, just a question when you say that you're not going to be inspired by the PSO.

I will go because I'm sorry.

Just bear with me, right.

Yeah.

Good morning, gentlemen.

Good morning.

[Inaudible] And then I think I know your opinion on that.

Right now, we are just talking about the content of the program.

And if we come to agreement, that makes sense.

We also need to talk about what do we need to specify and where do we need to specify it.

But that's the next step from my perspective.

Just one other point as well.

When constraining and the task-producing options, [Inaudible] >> Europe is brain pooling.

>> Yeah, but no Asian.

[Inaudible] [INAUDIBLE] Yeah, yeah, then off-prem flu.

I don't trust this today.

I think this is what I kind of expected, right.

[LAUGHTER] OK.

Yeah, sorry.

No, no, no, no, no.

No need to ask you.

So we also need to specify how the key material is hand-p right.

So while SD jobs for the credential form, we're pretty sure what's the best choice for us and also exchange protocol.

Like for the next layer, like the trust management, which directly indicates how the shared keys are handled in the SD-JAW.

We're not as sure.

We had a session yesterday on trust management.

So I think right now there are multiple solutions probably that you can have.

I haven't told you.

I would like to, for the moment, comment on trust management.

I have that on the last slide.

There are additional topics.

So trust management is really complex topic.

I also had a conversation with Dimitri yesterday.

He's working on the same topic.

So I think we should just, yeah, sink on that topic and work on it.

And I also reached out to the folks at FC, because they had done tremendous work on that topic.

What I would like to do is really differentiate two layers.

One layer is really just technically, how do I get the key.

how do I verify that the identifier of the issue really is bound to that key and the credential is this side, this is not really trusted.

It's just authenticating the issue of the credential.

I think we have some options for that.

Right now, those are the two options that we more or less distilled out of the solution space.

Unfortunately, right now we do not have a single proposal And I'm a bit afraid we will see more of them.

But that's what we're going to suggest.

And it's driven by a couple of assumptions and considerations.

First of all, we want to have a solution that is absolutely freaking simple.

And that's why the first option would be to use something that is really well known, widely understood and open and equal for, which means the issuer has a key set that's published in the internet, can look it up, the issuer can replay the keys, that's it.

The pattern in the credential is pretty concise.

There will be option one.

I will show examples later on, we will show examples later.

That's one option.

This is the pretty simple, well-known thing.

And the other one is also well-known, but in a different community.

So X.

509 is used in ISO.

X.

509 is used in IDAS 1.

It's there.

And it's not going away.

And there's a lot of stuff built onto it.

We had this in this EIDAS session.

That was the first day, right.

The whole EIDAS thing is built on X.

509 and data signatures and all the long-term archiving and long-term validation.

All that stuff thinks that I'm still searching for solutions in the natural space, it's also in the traditional landscape.

So it might be pragmatic first step, for example, the top level in that profile as well, because it would make ISO people happy, I hope.

Yeah, I mean, it depends.

The X509 profile is definitely different.

You mean we don't even have this X509.

We also need to profile how X509 is used.

No, it's using standard X509 extensions, but a few extensions have to be mandatory.

Although some of them are non-critical and critical and stuff.

I assume that not every x549 certificate is valid, is ISO compliant or ISO 18 or 13-5 compliant.

>> I would assume the same was true for cent/etc/s.

>> Probably.

>> Yeah.

>> But then it's also a great thing.

[INAUDIBLE] [INAUDIBLE] [INAUDIBLE] [INAUDIBLE] [INAUDIBLE] [INAUDIBLE] No one assumes we are going to solve all the problems of the world in one day.

But I think I just want to outline the direction and why we came up with those two different proposals.

And-- So a signature algorithm, something in that space which can be found to cover, right.

This is a very important aspect.

Profiles should also support the really secure use of credentials for pipe and substantial use cases.

Then we've got a rule of minding where we would just like to use a JWK as a raw public key that is indigredential.

And there is an existing job plan, but that is called the CNF confirmation plan.

And regarding revocation, we think that the pragmatic solution as of today is status list 2021.

Dr.

Weisberg.

- I did.

So is there a JWT serialization status list 2021.

- That's an accident question.

I'm not aware of a JWT serialization.

That might be something.

- Right.

We should consider.

Yeah.

>> The intention would be probably to align there, right.

>> Yeah.

I think that makes sense.

>> Yeah.

>> That makes absolutely sense.

>> I mean, are you concerned about how to encode that information in the GWT credentials itself.

>> Well, right.

>> Because that can be addressed by the mapping.

>> The status of the self is signed in another encoding and signature validation points.

>> Yeah.

>> Yeah.

>> To like status of [INAUDIBLE] Yeah, yeah, yeah.

[INAUDIBLE] [INAUDIBLE] Right, right, yeah.

[INAUDIBLE] [INAUDIBLE] Yeah.

[INAUDIBLE] Is the status list because I also when I write that I'm not so familiar with that.

Yeah.

I also realize well that's true.

This whole Jason might be the hybrid approach.

I don't think this is really, really helping with where simplicity.

>> Hybrid.

>> I mean, a mixture of JWT and Jason.

>> Right.

>> M-logs.

>> The other question is, I mean, right now this is about SDG and OpenID policy.

I think we need to clearly delineate how we get M-log in the picture.

I have that on the last slide topic.

Is it okay with you two.

Yeah, I mean adjusting the ARF that's required both.

We, the California D&B project also requires both.

Today's ecosystems that will have to do both.

And for MDocs it's actually a little bit tricky because MDocs don't define a revocation mechanism.

- Absolutely, acknowledge understood.

I think it's important to differentiate.

This is a problem for that.

So I would assume if you zoom out of it in a bigger picture, there might be an Uber profile that defines how open-ended it is used for credential formats.

But the credential formats themselves are somehow autonomous.

I would like to look into revocation, all that stuff, and key management for the credential format and the Uber, if that makes sense.

I'll just get us all out there.

our capabilities, we've built a revocation and clipper space mechanism for securing CWTs and the COSA sign CWT based expression of that that would be happy to share the details that we've used which would be probably certain that we would not be able to adjust the [Inaudible] Okay.

So that's one of the examples that I wanted to show.

Can you read that from the back.

Yes or no.

(audience member speaking off microphone) - Well, you missed the first part, right.

But what I said is we are, the key management is for my current style.

I have two different examples.

One for the key management using a JWT sync.

That's why I call it open, I think what I call it open.

because that's the way we use it.

And then we will also have the X509 style.

Yeah.

OK.

So let me start from the top.

So for those of you that are not familiar with the VC to the old stuff, the VC to the old, what's happening, at least all the folks at the VCs are familiar, right.

We tag such an object with the type of the Hosei type.

There's a sum of Hosei items.

and it allows to detect the data for a certain area.

And that's what we do, and right now the assumption is that it's gonna be VCD plus SD attention to the job.

And that's the value of the driver code.

We need to define what is being defined, for example.

But as a veto, we can't do it all later.

So based on that type, you know, it's a VC, and it's a VC and SD job.

That's something.

No, I'm not going to buy it.

No, okay, you're heavy.

- Okay.

- Okay, good.

So I think that's pretty clear.

And the header also has a kit.

It's a key ID that's to some of Jose's stuff.

It allows to identify what key, all the keys that was used to sign the credential.

As you see, there is at least no issue of key in that credential.

What we have is we have an issue of strings And that looks very much like an ideal.

In the end, the whole thing very much looks like an ideal for our job.

And as I used to say, we're busy too, the job can be a jumping in.

So we can do very popular entries that utilize everything we have right now in jobs, and it also makes Mark, for example, absolutely happy, because we can use all the simplex that you have to find, for example, for pilot assurance in the EKYC identity.

and we move like OID foundation.

Just put it in that thing, right.

- So the VC, sorry, the VC in here, is that uppercase VC or lowercase.

(audience laughing) Can I connect.

- Yeah, please go ahead.

- To make it meet the data model of the W3C VC or is it not that kind of VC.

- So it's a-- - It is a VC according to the VC2.

- Data model.

- Yeah, uppercase VC but 2.

Sorry, just give a few minutes, we didn't do like a VC 2.

0 session on the interview.

It's just made a review by a panel.

What's happening at the work on the credentials working with industry is, in 1.

1, there has been this kind of, it was a clear of what the payload across the signature.

the first thing we did in 2.

0 was we literally separated.

This is clearly separated payload from how it's being secured.

And two way, the original two ways how it's being secured is one was the data groups, how it will be the eternity, same, same line.

And the other thing was usual jobs, right.

GWS defined that idea.

And his agent arguably falls in that, how it's being secured category, being how you make sure there's integrity by the issuer and all that.

And when it comes to payload, so now in VC1.

1 you would have own one document, 1.

1 where everything is crammed into one it's pretty long hard to read.

In the 2.

0 you would have BCD in the model, which talks about it's payload part only, then you would have separate documents for how it's being signed.

How it's being signed part, you would have one document for BC JAWD, you would have one document for BCD, named JERVITY, and the same date name.

So BC JAWD, can you use existing crypto, right.

BCDSA, all that are defined in different places.

And for JAWD part, as for the dating, JERVITY part, you would have, again, separate documents inside BC.

working group saying this is how you do EDDSA with daily dirty in-birder for prevention.

This is how you do ECDSA with daily dirty for our credentials.

And you want to talk to VVS in this daily dirty in-birder for prevention.

So that's how it's being structured now.

And that was the context to explain.

When it comes to the payload in the core of our financial data model document, you would see only to use an OD without context, the credentials object, pretty much what you're used to seeing in 1.

1.

But the result of long discussions is that the credentials can exist.

They are valid for a lot of credentials.

Operate these for a lot of credentials.

As long as it's possible to map this back to that data model to find at 1.

1.

So this one, that mapping would be defined in a VC jobs pack.

It's already in there.

That's why I can answer it is an awkward case for a government financial.

So that's how you transform this ELO back to that, what people who based in the model should exist.

But the discussion about that transformation doesn't have to be bidirectional.

could be in one directional or bidirectional.

And the transformation is not mandatory.

So for example, if you're only, this credential is circulating all the ways in the ecosystem.

All these data bases, if we don't de-transform it, right.

But let's say you're trying to interoperate with the ecosystem where JSONOD is needed and we're doing JSON is needed, like that, but potentially that that is not useful when this credential penetrates the JSONOD processor so it doesn't fail for example, right.

We don't know how it's gonna play out yet, but that was the outcome of the small discussions of they are gonna produce the, but they are again use cases where that's not necessary.

So that was, yeah.

Any questions.

I know it sounds a bit, no, did I, yes.

- Sir, providing part of the between how you represent a credential versus how you secure it is obviously very good.

is for the implementations that we are moving forward on.

We've faced the most important choice that the credential representation is going to be JSON-LD and PLATIC JSON.

But we support multiple ways of protecting that JSON-LD credential.

We require data integrity groups, but we are open to ECJWT as a production vector.

My question coming back to, obviously, this particular session is very simple.

We've been going down the path of BDS signatures as a mechanism for providing selective disclosure because they also provide more so relatable capabilities.

The trade off from what I understand in using SPJWP versus BDS images, which tends to be, you can use current accepted crypto with SPJWT, but it does not give you the non-parellability function.

So it's a trade-off in what you want to do.

I am simply curious to understand does SWJWT, SPJWT only support JSON as a payload or does it can support JSON-LD as a payload given the fact that JSON-LD is JSON.

- Amazing question.

I know, here's an example.

- I have an example.

- But the answer is-- I have an example.

(audience member speaking off microphone) - The question between DVS Plus and eJogs is that you have to choose if you want hardware security for unlinkability.

You cannot get a lot of regulatory use cases.

That's why also the IDS interact goes with-- So I want to be very clear about, as somebody who is on that side of the, what is acceptable for our implementation.

There is a perception that certified cryptographic modules have to be hardwired, that is not true.

Right, so if they do, the cryptographic modules can, if you want to have a conversation with somebody who's advocating cryptographic modules through the CMVD process and being successful at it, John Callis is a great person to open up.

So long as you're-- I just want to separate the hard work.

I'm taking all my hand as a moderator here.

We've got different questions on the table.

I would like to ask them one by one and answer the questions on the-- Just one sentence.

[LAUGHTER] [INTERPOSING VOICES] I don't want the question right.

(audience member speaking off microphone) (audience laughing) - I know where you're coming from, it's just there's a lot of different types of many jurisdictions.

Like in isolation for example, we have NIST in the people, we have BSIS in the people, and NIST is like just use NIST first, and BSIS is just like NIST, or I'll take, you use Brainful first right now, that's why you have 11 first, and then we also have rates, so it's like, like that, you know, they're different than the duration of the piloting they're running right now.

And for only the ability in this PBS, you have to use specific ones, but you can't use the keyboard that you're running in the park.

I mean, it doesn't do it.

I think it doesn't do it.

It's true.

[Inaudible] >> But you have to use a-- [Inaudible] >> And then I would like to come back to the interoperability process.

>> So the only point that I will note here is that it is a valid point that parent-based images like DDS are not important for the physical.

It depends on the assurance level you want to achieve.

So for a lot of cases, a lot of governmental cases, especially in Europe, you would need to have some protection against the extraction of the key materials so that you have a strong binding between the credential and the user.

It's just to comply to certain things.

I mean, there is implementation guidelines defined that defines how you can achieve certain levels and hardware security, or maybe not even hardware security, but I don't know what the exact language is.

T's, S, CQ and Claves, whatever.

Common criteria certified.

- So BDS plus evidence used today by most people does not achieve a probability because people are using the key as a whole client.

- Yeah.

So you would need CKB's on top, right.

- The other is if you use ND jobs, there are a number of mitigation possibilities that you have to avoid the correlation by issuing many credentials, rotating them, et cetera.

So, follow on to that point.

At the end of the road, unclinically, the ability is interesting to consider, given the fact that a lot of these credentials actually contain enough data that it can provide can be used to call it.

So, the one thing that it provides to entities like me is simply it prevents a question from being asked.

- Absolutely, and I find absolutely familiar with our OpenNet Econect space because everyone asks, have you implemented Kerowice polynomials like everything.

- No.

- In the end, we never did that with the ES ecosystem.

I can disclose, but because I think it's just ordinary.

- Yeah, because you have to email, right.

- Exactly, so I would like to come back to, I mean, your questions are absolutely, at the heart of what we are doing here.

And we have really analyzed that for the last year and have, in the end, we needed to make it in the same way that the consideration sums on the drawbacks, perhaps, right.

And just to answer your question on Json-LD, so this is a Json-LD potential based on a (mumbles) It's a vaccination certificate, that's the payload.

And I'm just gonna show you, in the end, what is-- (audience member speaking off microphone) So, and I took that little experiment because in the end, all SDGs is a mechanism to chop JSON and reconstruct it in the end again.

So this is the same credential, just cut into pieces.

And that's not the latest version, but the latest version of SDGs [Inaudible] And we also had a discussion in Yokohama at the ITF meeting how this kind of credentials and the other one, how they, how can they be designed and what the type of elements will be and so on.

This is what's going on for both.

For the interoperability of both, we have decided to go with the job area.

Okay, or any quick questions for our panelists.

(mumbling) You're not supposed to have a question.

(laughing) You wanna say something.

- No.

- Okay.

All right, so let's go from, I think we even don't want to make it through the development of any part of that center.

But that's fine.

All right, so we covered the first bracket, the issue.

And then we're scrolling down.

I think we are all familiar with IoT and exploration.

Here's a new thing.

We think that there is a need to-- even if we have Jason or John Halo, we need to somehow pick the five of the credentials.

For example, we will need that to build an awesome credential five values to come, credential selector, right.

This plane doesn't exist yet.

- Wait, there's a type property in the very full credentials.
- But it's not in the IANA.
- Yeah, yeah, no, no, obviously not.
- So then this would be something that goes to the IANA-shaped registry and don't be kind to them.
- This is just a preliminary assumption, right.

With these key marks, with the, I don't know, it's a whole kind of discussion of how that thing is gonna work, yeah.

Then we've got the selected disorder stuff.

And then we've got the confirmation plan for borderline.

That's it.

So you can have arbitrary guide payloads here.

You can use any kind of shock planes, either the prior ones or those that are predefined in specifications.

Questions on that before I switch to the x-value line.

Example.

I have just a-- maybe you can't answer that question.

maybe somebody who is also active in the VC working group.

But if you find a mapping, would it mean you would need to define a mapping from out of the ISS onto issuer, IT onto issued as a CNF onto confirmation method and so on, okay, that's fine.

- Well confirmation, CNF is arguably a good one, okay.

In general.

- The confirmation claim is always gonna be generally.

(mumbling) like confirmation key is not a coordinator thing, it's just for proving maintenance.

So it's probably not being met.

(mumbling) (mumbling) (mumbling) (mumbling) - Yeah, it's like back in 2018.

(mumbling) including you Alison.

(audience member speaking off microphone) Yes.

(audience member speaking off microphone) [Inaudible] >> In answer to your question about the confirmation claims, they may not be true in the interrupt profile, But there's other ways of communicating the confirmation key that we could use.

Such as if you've already pretty scared you, you can just have a key ID and reference it.

I'm not saying that's what the profile does, but that's what the-- - Yeah, yeah, absolutely.

I'm not saying that.

That goes back to what Bob just said.

We do not need, for example, the ability to rotate that thing.

So we put it there and it self-contain it's good.

I mean, you could have, in the end, you could also put the initial key in the job, in that example.

[Inaudible] I think the point to say as well, just to.

It's extensible.

The protocol has been used as an issue, yes.

The reason, you know, I think, the key rotation, the idea part of it was because, you know, you're a wallet with an accent, so can you just go back and get another one.

I think you just press key, give an assertion, get an eversion of the credential, like it's.

You know.

And that, again, just to highlight, when it comes to compliance perspective, some issuers really do not want to have.

to be binding to an identifier where the key rotation of N is un-wattnessable to them because they want to control the posture of the key that they bind the credential to.

Like, there must be a factor of hardware, and I must have an anti-station that confirms to me that I am a factor because that gives you anti-conversion.

[INAUDIBLE] And that complexity of how you read the result, you can get it by adding complexity on top that it regulates as much.

And that's super-receiving, because in this option, you don't need to resolve anything.

Because the key is in the-- is in the token, is in the credential ready, right.

It's an x, y, and c.

It's a certificate check.

(audience member speaking off microphone) This is a good example actually where it might clash with the ISO stuff because in ISO, the IACA, So the issuing authority is the root certificate is not contained in the X5C.

It's actually not even allowed.

So readers would crash if they find it, because they assume in the MDL case that the X5C is a single-- X5C.

Yeah, sorry.

Ah, it's the CBOS stuff.

Yeah, I see.

No, it's X5C.

X5C, yeah.

X5, yeah.

It's just a change of one.

You find the root step, the whole thing blows up.

- Yeah, it's in CWT, it's a X5 chain, I think.

But they also have a short mapping where I believe they might use X5C, but I'm.

Anyways, but this is basically weird.

(audience member speaking off mic) and for roots when it comes to the tree.

Yeah, yeah, yeah.

So they only include the leaf significance now, like, the small growth, the linear scans are-- [INTERPOSING VOICES] I think it's partially for that.

And it's also because they want to encourage breeders to have the thin, the specific heads, right.

They want to make them unverifiable, and they trust the issue, or force the distribution of the issue, or the certificate out of band to the breeders, and verify it must be hard.

And they can deliver sessions with them to the issue, So which means they more or less have implicitly built in also the trust piece.

Exactly.

So negotiating with the server over TLS and not actually getting a [Inaudible] >> Okay.

So this is another option.

You're going to implement that.

[Laughter] No, that's what Paul probably -- >> And the benefit is like if we do that in Europe, we go like IDAS 1, which is predecessor, and there is the EU trust list, which is the trust management.

we take a seal which is like a signature certificate for organizations and with that x509 seal we're gonna sign our credential we are automatically got the trust from the EU trust list down to our issuance organization and then that will sign it.

>> The difference to what you just described is one of those elements in the system itself and the specific in itself is listed in the new class of the time.

That's how this is defined.

>> And it also gives them compatibility with JADES, for example, which they can use for long-term on, I become somebody who has so on.

So there's a lot of challenge.

>> There is a challenge, and we should have mentioned that.

>> Yes.

>> Thanks for this.

>> Hold on.

>> Four seconds.

or second.

There's a challenge with this whole stack, as I said, has all the capabilities for history, long term motivation and so forth, which might be interesting for a couple of credentials like the (mumbles) Okay, what we have here is that then the signatures are being used to contain timestamps and all that stuff so we need to also use timestamp services.

They exist, right.

They are rolled out, they are used in production.

However, then, we would turn another serialization forward about all that, about everything.

It's called J So the complex serialization has worked for the distribution system because the Etsy, which does this kind of stompers, decided to go with the J serialization because they want to put stuff in the unsigned template.

But that's the integral.

So I have to jump over there.

And we've got to be happy.

OK.

So can I suggest another hybrid here, obviously, because JAD UK's defined usage of the X5C plan, where you can obviously expire an IAN circuit change in the JAD UK, listed at the JAD team, in the PC.

So you could have the ISC's value here, the E-B issue of LZ, and you could have the key posted, but you could need to also address the circuit change.

>> Why would you like to add another option.

>> I'm not really trying to get another option.

I'm trying to draw that relationship.

So if an issue is and they want this to get changed, they carry with it so that it is required to apply, they can use this as a change.

ISS could then revert to being just an issue to the SQL.

(audience member speaking off microphone) Well, so I'm saying what you could switch on is in the heat of the cavity value is present and I'm expected to remove that.

Otherwise what I do is the X5C parameter is present in the static cavity.

I'm supposed to effectively validate that And then the root step again, the C value should be with ICs common that of root step.

It's not going to be the root step because-- Sorry.

Distinguished name.

So leave some to repeat.

Yeah.

I would like to take that discussion offline.

I'm sure.

I have others not yet.

So, but please take it outside.

OK.

So-- (audience member speaking off microphone) - All right, so if there are no further questions on the production profile.

- I have a lot of questions, but maybe you can take them off.

(audience laughing) - Okay, shall I give a free overview of the open-ended code system.

- Yeah.

- Okay, good.

Just to be more clear, because I don't think we will make it through all the bullets.

So if I open a new policy, the first thing we need to do is to define what we call a profile.

In the OpenID for BCI specification, for example, in the appendix, there are already profiles for credential components.

What it takes is to define forms that have to be followed by all rules, how that particular profile is handled in the issues and also in the presentations.

That's just what we need to be done if you customize two ways for the benchmark.

And then I've got a topic that we also need to address, And this is about how we're going to authenticate or establish trust in the very front on the very front of the wallet interface.

Because in at least one jurisdiction, it is required in the wallet authenticate the very front and also authorizes the very front based on some other trust data.

And the same was true for the wallet overstation.

For those of you that have attended Paul's presentation yesterday, he explained that some programs believe.

So we need to find a way to, in the end, what it boils down to is that the bullet can authenticate or it used to be seen through all that.

So we will find a term line.

It's something pretty lively, which I will also show an example for, to authenticate toward the issue.

And I think we can use the same method for very powerful authentication as well.

Just put a VC in the request, sign the request, with the key that is bound in the [INAUDIBLE] and then ship it to the model.

Instead of using x5.

09 for that purpose, you can use v-sp-- let us say, vc2.

Yeah, I mean, for using this stuff with the very first-- the model can use this to develop my thing for-- you did some work on trying to figure out how that can fit into the confirmation method stuff that we are going to define.

Yeah.

[Inaudible] >> Okay, let's jump in quickly.

So we obviously also need schema, schemas for those, right.

Because that's where it's going to be concrete.

I also want to show examples of that.

And we also need to introduce what we call the client ID.

Because that's going to be a new way for clients to authenticate themselves towards the moment.

[INAUDIBLE] No, I mean, the only reason I just want to clarify the reason, the term "PC" in this context, and it's purely an anti-station, like, I think that the-- some of the-- some of the [INAUDIBLE] they think that they're probably going to contain something of naturalized, perfect identity claims in it, right.

and what you're talking about is really exciting in a situation where there's a station service.

Absolutely.

It's something about a software component service.

I'm absolutely happy to define a different term for that.

My point is, technically, nothing is maybe a CD or a funding video.

It's not really about the perception.

It's technically an interviewee, right.

Sure.

I just think we'd like to-- I make a proposal.

Let's discuss that in length.

Let's discuss it in length where we have time for that.

Yeah.

So just want to give an example.

Do you want to explain that.

I can do it.

I mean, you are very relaxed.

So I would-- [LAUGHTER] All right.

So this is how such an attestation looks like in the company prototype that the booth looks nice built.

So it's-- I mean, it looks like it's seen.

It's got an issue on.

It's got another type, one attestation, I mean, the situation.

And it's got information about the bullet and also the support of LOA and a confirmation line.

And that confirmation claim is then used to really, yeah.

Authenticate the wallet, right.

In the concrete prototype that Unus to the issue.

So the issue can vary from, okay, that's going to be presented by the real provider to do some authorization on the request.

In similarity, we could do the same on clients.

This is a example presented to Marco from the [Inaudible] [Inaudible] [Inaudible] As I said, the key here of the private key could be used and assigned a request.

For the topics.

Trust management, I already mentioned that we have committed that yet.

We know it's super important, but we also know we need to work on that topic.

And there are so many options, and different domains to do it differently.

governance processes involved, heavily involved.

So we need to take a look at that, but I think what we have to present is sufficient to really build systems.

So we can start with that, except that perhaps trust management works definitely with applications.

But we're not approaching it.

Using What We've Got - Pure Identity plays probably aren't the answer...

Session Convener: Matthew Miller

Session Notes Taker(s): Charles Mullenix

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

Key discussion points:

- Lots of back and forth on what the real perception of users actually is wrt to the status quo of authentication and authorization today. More or less, conversation began with the question: “are we engineering a solution in search of a problem?”. Conclusions that came out of that line of discussion:
 - We are very bad at researching user perception of our field on a whole. Real studies where this is explored are rare.
 - Recoverability for security incidents like identity fraud is extremely high for the consumer by design; banks eat costs. Otherwise, faith in institutions would degrade.
 - As a result, a very low cost (and thus motivation) is felt by users today. However, an extremely high financial burden is taken on by the institutions to hide the consequences of user's poor security decisions.
 - Our goal for end-users should be to disappear. Good design is something you hardly notice.
 - In that, we face some challenges. Passkey authentication is going to be highly disruptive for users, some of which have gone their whole lives with username/password and view it as highly reliable and transferable.
- Judith dropped some knowledge bombs on us, inviting us to think about domain spaces beyond just what we're doing with identity today. Great quote “don't just focus on how these new systems are better. Focus on how they're *different*”
- Intended user vs actual user (both wrt the person sitting at the computer, but also the context in which these technologies are being applied)
 - Many users to one device is a common use case
 - Touched on activity in Bhutan, where devices may be shared across entire towns.

Transcript (heavily paraphrased):

These discussion notes are based on hastily scribbled shorthand, and transcribed hours later. Ideas and themes are appropriately attributed, but all words should be assumed to be paraphrase.

- Charles Mullenix
- Matthew Miller started us off. Prompted us with ‘people seem primarily bent on using VCs for authentication... do users really want to do this? Do I as a consumer really want to pull out my phone, install a wallet app, and sign off every time I want to log in?’
- Chloe: Who is the product for? I as a consumer don’t have a real problem with the status quo. Is there really a problem here, or is it a solution in search of one?
- Jacob: ‘like seven things to say just from all of that’
 - Never considered the difference between identity and authentication (a statement which garnered surprise from Matthew and David from FIDO)
 - “Magic Links” / deep links are a part of the status quo. People use them because they’re easy (though they aren’t secure)
 - We, as an industry, tend to tremendously over-simplify. “There are really like 5 things here, but you’ve drawn two bubbles on the whiteboard”
 - (may be misattributed) Walmart, banks, etc all have different needs and wants, but ultimately they come do identity because they want to reduce friction
 - I don’t trust LastPass anymore; it’s a new access point
 - (in a more direct response to Chloe’s point) The initial friction that a user experiences may well be worth, as the rest of their experience will operate with reduced friction (foreshadowing to Jacob’s later realisation about friction in general in the industry, and increased friction as a pattern)
- (Somebody, I didn’t write down who:) Most people of our generation just don’t care; they want something simple and easy.
- Charles, in direct response to Chloe:
 - The current state of AuthN is very rough for certain demographics of patients. Elderly folks end up having a 30% completion rate for 2FA (based on some internal research @Epic that I need to talk more about somewhere; maybe says more about MyChart than it does patients).
 - This problem will only get worse with time as more and more sites require MFA on entry.
 - Maybe it’s not VCs that save the day, but at the very least public/private crypto in WebAuthn will help reduce friction for users tremendously.
- Matt: Maybe the situation now isn’t straight up bad, but it could be better
- (somebody whose name I did not get): The friction isn’t actually all that bad today with many VC workflows, e.g. browser extension wallets and simple use cases are possible today with very low levels of friction.
- Peter: We have to design systems with both the *intended* user and the *actual* users in mind.
 - e.g. for a bank, the intended user is the holder of the bank account. In reality, the users of that bank account are both the holder of the account *and* the fraudster trying to get access. Our systems need to be designed so that they’re easy to use for the legitimate holder, and very difficult to use for the fraudster.

- Peter: Take a look at behaviour with mobile apps. How often do parents hand an unlocked phone to their children? Or how about device use and how it maps to real world use cases? Mobile devices are single-user operating systems. In practice, we see families all using the same device!
- Matt, agreeing: we have to be able to meet users where they are. In certain environments, we just don't have any control over that device's use.
- Peter: You all have talked about FIDO, but what good is FIDO if we've registered five biometrics to the device?
- Judith, captivating the room: This conversation has heavily focused on authentication. It has not touched on the concept and applications of *decentralised trust*. The power exists in what this technology enables beyond just human identification. Think about sensors!
 - I've been an ID person for a long time, but when it comes to talking about multi-factor authentication? I don't have MFA enabled on 90% of my accounts because of the friction involved.
 - We design for people who are similar to ourselves, or even an idealised version of ourselves; these idealised actors do not map to people in the real world unless we build that into our systems.
 - (bringing it back to her initial point): we need to talk about the technology's implications beyond just signup and authentication. It can streamline organisational processes!
 - (mentioned BC gov, but I wasn't able to faithfully capture since I don't know what BC gov is, but I think the general gist of it was:) These are use cases where we can, beyond just logging in, step out of that ecosystem and gain access to things without getting the original issuer involved!
 - **It's not 'why is this system better'; it's 'why is this system different'.**
- Michael, building on what Judith was saying: These systems are really just about transferring trust
- Judith: We often think about things on a 1:1 basis, but that's not it. These relationships transfer beyond the single transaction.
- Charles, building: This is actually a huge thing in healthcare.
 - Third party applications (e.g. AppleHealth) need to be authorised on behalf of a patient to request data from the underlying EHR (e.g. Kaiser's database). Today, this is accomplished via OAuth where the user is directed, in a web view, to the EHR's patient-facing application server in order to authenticate and then authorize the scopes requested. Not super surprising; this is the intended purpose of OAuth.
 - Unfortunately this places constraints on the architecture and requires duplicative action on behalf of the patients to authorize to different health systems (patients seeking care at many organisations *do* exist).
 - Imagine a world where a patient, deriving trust from a foundational credential, could instead authorize those scopes directly to the third party application without the involvement of the authorization server run by the EHR. A VC could do this, and then each data provider could verify the authorization in real time as the data was requested.
 - There are big unsolved problems with the above (how do we keep third parties accountable for patient communication? how do we ensure consistency? how do

we translate technical scopes into patient-facing consumable language?). However, it's a new dimension of capability that's unlocked by the tech.

- Judith apparently had a lightbulb moment here about how VCs can end up taking the place of certain existing protocols like OAuth; I'll ask her to comment on that later.
- Jacob: I have five kids. I have a kid with a college laptop, and that single Google account isn't capable of doing certain things. With multiple people on one device, how does the system know who is operating?
 - Also, how do we deal with merging duplicate accounts / identities in one domain?
 - Charles mentions that this is a pretty troublesome issue in the healthcare domain.
- Matthew: High assurance use cases like banking and healthcare must be particularly difficult, since you're working with all kinds of regulations in the space (mentions NIST SP-800-63 document set). If wallets want to play a role in these industries, they need to rise to meet these specifications! How can we build to satisfy these requirements?
 - Maybe a first step in the process is to build from other pieces of technology that already *do* meet those standards, or explore the patterns already established by tech that operates in these spaces.
- Peter: Don't worry too much about those regs. Focus on *usability*.
 - Regulations in other industries are real, but at the same time these regulations generally (albeit very slowly) follow the curve established by the technology.
 - Also NIST specs are not requirements in industries beyond government entities. They are guidelines.
- Peter, starting a new thread: We tend to think about these technologies as existing in the mobile world; we all sort of decided all at once that the solution was to use phones. In reality there are plenty of domains for which this model doesn't really work! Think about healthcare, or banking, where people are actually on desktops for the most part.
- Judith, building: If you haven't, you all should go watch the Trust Over IP presentation on the kingdom of Bhutan.
 - It's fascinating what they've done with digital identity. They're trying to prescribe a digital model onto all of the citizens in their country, but in many cases they don't even have *electricity*.
 - Forget family devices, in some cases the people are using *town devices*.
- Jesus: I work a lot with ethical farm labor recruiting, and we see many cases where people will have a first phone in their home country, purchase a new phone once they reach the US to work, and once they're finished they'll purchase yet a third phone once they return to their family in their home country. This person now has 3 numbers in so many months, and no email address.
- Jacob, gesturing to the photos of the mainframe computers on the walls: Look at these photos. How complicated was that? People at the time would surely assert that it was easier to do this using an abacus. Look at where we are now (gesturing with his phone).
 - Development led us here over time. Surely we will see more friction today with these tools, but as time goes on we'll see this decrease.
- Matt: We can sort of think about friction as a method of awareness for where our attention needs to be
- Jacob: Friction is also a motivating factor. It influences change.

- Peter: I remember something one of the senior engineers once told me. ‘Never solve a problem with a computer in four hours that you could solve in fifteen minutes with a slide rule’
- Matthew: Everyone is so hyped about this; we talk and care a great deal about identity in this space, but think about authentication. Authentication, for most users, is a brief stop along the user journey bringing them to a goal that they’re trying to accomplish.
 - Nobody cares about identity! We’re doing all of this work in the long run so that people won’t notice what it is that we’re doing.
 - Mentioned that if we do our job right, then the usability is so simple that patients *think* it’s less secure.
- Judith: We care a great deal about identity in this space, but how many bad behaviours do you personally practice when it comes to digital security?
- Charles mentioned the “good design is 99 percent invisible” quote.
- Peter: People make risk decisions for themselves based on the corpus of their life experience. People might use a sticky note underneath their keyboard, but this person has made this decision intentionally based on what they know about who accesses their home, etc.
 - With passkeys, this new information throws us off. Users don’t know how to integrate this new technology with their existing mental models.
 - Users have an extremely high degree of confidence in username/password.
- David, agreeing: There are generations of people now that have gone their whole lives exposed to usernames/passwords. Now we’re just going to remove it??
- Matt: Ceremonies in this new technological space are becoming less and less about a system asking a user who they are, and transitioning towards users telling the system who they are. That’s the direction we’re headed.
 - We’re actually in a state today where we don’t even need a username with WebAuthn.
 - Mentioned Discoverable Credentials as a means of approaching this state.
- Jacob: What about when you originally sign up? You need to identify yourself and enter/register a username.
- Matt: yes.
- Chloe: Does anyone actually know the statistics with identity fraud? I use the same username/password for everything, but this is generally because I only think about safety when it comes to my bank account.
- Mike: 20% of americans were victims to identity fraud in 2021. Companies typically just eat the cost because they care so deeply about patient perception. These things are typically handled without anybody knowing.
- Matt: Can we stop fraud with signatures, then? Recoverability is just so high
- Mike: 2020, banks posted \$56B in losses to identity fraud.
- Chloe: **Recoverability is so high, consumers just don’t care! We should be talking to the freaking banks!**
- Michael (different from Mike): Users want something that feels as private and secure as their house key, and I don’t see us moving in that direction.

- Judith: we need to get better at learning what end-users want and listening to them. We need to be holding focus groups and sitting down with people! We suck at this today. Much of it is that we're small, and don't have the funding to do that type of user study.
 - FIDO does, and they have been conducting these studies!!
 - It's very niche, but we can learn from them.
- Peter: We should also avoid waiting too long before actually doing this.

KERI + ACDC 201 Part II

Session Convener: Kent Bull

Session Notes Taker(s):

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

No Notes Submitted

Web 7.0 Trust Registry FrameWork - TrustReg Documents (DID Documents)

Session Convener: Michael Herman

Session Notes Taker(s):

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

No Notes Submitted

Aries Bifold - What is new?

Session Convener: Clécio Varjão

Session Notes Taker(s): [Steve Venema](#)

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

- <https://digital.gov.bc.ca/digital-trust>

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

Picture of the double-sided handout from the session



BC DIGITAL TRUST

BC Digital Trust represents the Government of British Columbia's commitment to delivering easy-to-access digital solutions that can be trusted to be safe and secure.

The B.C. government is building trust, meeting our duty to protect data privacy and security, and providing an easy way for British Columbians to participate in the digital economy.

WHAT IS BC DIGITAL TRUST?

BC Digital Trust describes all B.C. government digital credential and identity products, and shared services.



Continual Evolution

Meeting increased demand and cybersecurity threats.



Smooth Integration

Integrating with existing lines of business.



New Applications

Utilizing digital trust technology to improve digital services.

WHY DIGITAL CREDENTIALS?

Digital credentials enable confident online interactions and offer people and businesses more control over when and where they share data about themselves online.



Confidentiality

Connecting individuals and organizations directly and securely.



Authenticity

Determining that data is unchanged and comes from a trusted source.



Privacy

Individuals and organizations only share the information they choose.

DIGITAL IDENTITY SERVICES

The B.C. government has been offering digital identity solutions for over 20 years, starting with BCeID in 2002 and the BC Services Card Login in 2014. Both are now well-established digital identity services used to access hundreds of government services.

BC WALLET

In collaboration with other Canadian jurisdictions, the B.C. government has developed BC Wallet, a digital wallet that can be used to store and manage multiple credential formats. By developing its own digital solution, the B.C. government ensures that high security, privacy, and usability needs are met. BC Digital Trust utilizes and contributes to the open-source Hyperledger project from the Linux Foundation.

DIGITAL CREDENTIAL SERVICES

Digital credentials demonstrate B.C.'s commitment to modernizing and enabling a thriving digital economy that benefits both the public and private sectors. They empower individuals and organizations, giving them more control over how their information is shared through multiple credential formats.



Innovation & Collaboration

Contributing to digital trust and open source technologies, we're moving toward adoption of digital credentials across B.C. government services.



Enabling Confidence Online

Digital credentials are tamper-proof, increase people's online confidence, and reduce fraud.



Improving Service Delivery

Digital credentials streamline and simplify service delivery across an increasing number of B.C. government services.

BC DIGITAL CREDENTIALS

Individual Credentials

Person Credential:

A digital credential that can be stored in BC Wallet and presented as proof of who you are during online interactions. Currently part of the Law Society of BC pilot.

Law Society of BC - Member Card:

A digital credential combined with the BC Person Credential for Law Society of BC members to prove they are in good standing.

Organizational Credentials

OrgBook BC:

A searchable public directory of BC organizations enabled via digital credentials.

Energy & Mines Digital Trust:

EMDT is enabling and accelerating the B.C. government's entry into a digital trust ecosystem by creating a simple and secure way to share environmental, governance, and social (ESG) certifications and credentials.

BC DIGITAL CREDENTIAL TECHNOLOGIES



BC Wallet

A smartphone app that lets you receive, store and manage digital credentials such as permits, identities, and licenses.



Traction

An open-source technology that streamlines the process of sending and receiving digital credentials for governments and organizations.



LEARN MORE

Find out more about B.C.'s work toward building confidence online:

digital.gov.bc.ca/digital-trust



John Jordan

Executive Director
Digital Identity and Trust
B.C. Ministry of Citizens' Services



Aaron Unger

Director, Product Development
Digital Identity and Trust
B.C. Ministry of Citizens' Services



The Rubric Podcast

Session Convener: Erica Connell
Session Notes Taker(s): Erica Connell

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

rubric.cc

Recording of an episode of The Rubric podcast with guests Kaliya “[Identity Woman](#)” Young, [Phil Windley](#) and [Doc Searls](#) the founders of the Internet Identity Workshop. Hosted by Joe Andrieu. Produced and co-hosted by Erica Connell.

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

Discussion of dids and did methods. See rubric.cc to listen to the published episode. (Estimated publication date: May 6, 2023)

What the heck is a hash

Session Convener: Joshua Coffey
Session Notes Taker(s): Nicole Roy

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

Discussion of bits vs bytes
bit binary digit { 0, 1 }
byte, 8 bits, representing a decimal number between 0 and 255
when you combine lots of them together you can do lots of useful things

What's a hash?

Black box - blender - Takes as input, some bytes
Bytes go in, does ridiculous math, mangles the hell out of those bytes, returns new bytes

One-way box, transform the string of input bytes into output with no reversible relationship to the input, always returns the same output for a given input.

Characteristic of most hashing algorithms, gives you back a fixed-sized output regardless of number of bytes in input.

Slightest difference in the input completely changes the output.

Finding the input for a given output requires you to search the space of all possible inputs.

Classic example is password hashing.

Rainbow table attacks - pre-compute hashes for many given inputs, then just do database queries against them to try to find the input for a given hash value. So, people have developed stuff like salts - extra random bytes associated with your account that don't change, or if they change, cause your password has to be recomputed.

Different hashing algorithms:

MD5, SHA {2-256, 2-512, etc.}

Problem with "collisions" (multiple inputs share the same output) in MD5 and SHA1

Detecting tampering with a file

For inputs larger than the output, there cannot be sufficient numerical representations to prevent collisions. We kinda hand-wave over that sometimes. Numbers are large enough that for many use cases, "probably won't happen".

Cryptographic keys

Example, ROT cipher. Shifting characters down by x, wrapping around.

Shifting by 1:

Joshua
Kptivb

In this case, x=1 is the symmetric encryption key. Both parties (encrypter and decrypter / sender and recipient) both have to know the same key.

Symmetric encryption algorithm: AES

Block cipher, takes two inputs: Data and key (just bytes)

Key is 32 "random" bytes (discussion of pseudorandomness here)

Creates stream of output that is indistinguishable from random data

To decrypt, take in key, ciphertext, and out comes the original data (bytes)

Getting into initialization vectors - additional special sauce that can produce different output for the same input - 16 completely random bytes (the size of the block)

IV versus nonce. Same as nonce, unless you're implementing this stuff, then go look up the difference between the two

Diversion into elliptic curve cryptography - $y = ax^2 + bx + c$ (defines a curve)

Wacky shit - Points on the curve - points (p,q) $p+x$. Find that point on the curve, do that a million times. How does this even work? Mathematical operation that's hard to undo.

In EC cryptogrphy, the modulus is the important part (the remainder in division)

Asymmetric keys: Public key crypto. Share the public key, people can use it to encrypt data and send it to you, you can decrypt with your private key.

Digital signature

Sign data, if someone has your public key, they can verify the signature.

Signing - you hash the data, then you encrypt the hash with your secret key. That is the signature. Then, someone with your public key can decrypt the hash, and compare it to the hash they made of the same cleartext.

AnonCreds AMA

Session Convener: Stephen Curran

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

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

- [Hyperledger AnonCreds specification](#)

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

- What are AnonCreds?
 - Designed before Verifiable Credentials data model was created or standardised
 - Supports selective disclosure and zero-knowledge predicates for number/integer data.
 - In a standard JWT, changing anything in the body invalidates signature
 - Revocation is privacy-preserving in a different way than [StatusList2021](#) since it splits the elements need to reconstitute the revocation into two parts.

- Can predicates be used with no integer data?
 - No, but common examples are age since they can be represented as Unix time
 - Other examples are location, since they can be represented as lat-long
- Why does BCGov care?
 - Govt would need to effectively create a new unique, correlatable identifier like a Social Security Number (SSN) which is a heavy and complex task, and there's obvious privacy challenges
 - At the very least, would want to do selective disclosure
- Who uses it? Are there commercial products?
 - Is probably the most popular credential format, but this is changing in the past few years
 - Governments in particular are very interested in since it supports selective disclosure
- Do DIDs need to be stored on a blockchain?
 - No, people are implementing where they are stored on `did:web`, `did:cheqd`
 - What about performance? Not a lot on ledger, so it's fine
- Comment about Aries
 - This refers to the Hyperledger Aries RFCs as well as the codebase implementations in different languages. The two get conflated a lot.
 - If someone says "Aries has machine readable governance", sometimes it means there's an RFC but there's no code, and sometimes it means that there's code but no RFC.
- AnonCreds v2.0 and what's the roadmap?
 - Mike Lodder (ex?-Evernym) has been working retaining the privacy features, introduce BBS+, but do it in an opinionated way
 - When BBS+ was first announced, they decided to skip Link Secrets and predicates
 - Right now, 3 cryptographic types supported:
 - String: gets converted to a hash, then a number
 - Number: Just gets signed
 - Link secrets: Used for holder binding
 - "Blinded" means you know the link secret behind it
 - Add things like enumerated types ("enums") that can be stored in schemas, e.g., stored the states of the US
 - 4 different cryptographic schemes under it
 - CL
 - BBS+
 - BLS
 - PS
 - Presentations
 - Will be closer to Presentation Exchange

Rubber, Meet Road - The Common Actor Model (CAM)

Session Convener: Chirs Kula

Session Notes Taker(s):

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

No Notes Submitted

SSI Deployment Challenges / Phil Feairheller w/GLEIF

Session Convener: Phil Feairheller w/GLEIF

Session Notes Taker(s):

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

No Notes Submitted

Government-issued Digital Credentials and the Privacy Landscape (is there anything else you want to tell me?) - repeat of session on Day 1

Session Convener: Heather Flanagan

Session Notes Taker(s): Heather Flanagan

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

Link to paper for review (public comment closes 24 April) - <https://openid.net/2023/04/05/open-for-comment-privacy-landscape-whitepaper/>

Notes from Day 1 session: https://docs.google.com/document/d/1HpnV7Nc1nDnQvws5ABUv-8u6iAqbAkSnSvOf_LkH8-k/edit

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

Additional notes:

Have you considered how public notaries might offer a bridge to audit use of digital credentials? Public notaries are a formal management of identity and brings in the accountability mechanism.

Additional emerging concerns to think about:

- considerations for not digitizing identity documents?
- health care world - people are going back and saying digital health records have gone too far
- even broader implications of fraud
- metaverse - engaging and transacting online and the expectation of convenience

embedded digital provenance should be straightforward to include

SESSION #12

Making Credentials Beautiful with OCA (Overlays Capture Architecture)

Session Convener: Stephen Curran

Session Notes Taker(s): Stephen Curran

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

[Presentation Slides](#)

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

The challenges of making credentials beautiful (and recognizable) to end users was described. The technique of using the [Overlays Capture Architecture \(OCA\)](#) to augment information about a dataset was presented. A general overview of OCA was provided and then some specific information about using it with Aries credentials was provided. The big wins are:

- Multi Language display of credentials - e.g., English, French, Spanish, etc.
 - For labels and information about individual attributes, and about the overall credential.
- Branding information — elements of the display that the issuer can provide to make their credentials look the way the issuer wants them to look — without making the wallet look like a mess.
- Semantic information about the data — data type, encoding, format, standard, unit and so on.

We also talked about some ways to distribute OCA Bundles (as they are called), with BC Gov showing their GitHub repo of OCA Bundles, and [Cheqd.io](#) showing how OCA Bundles can be DID-Linked Resources on a ledger.

See the slides linked in the resources section above for lots of other links to relevant information.

AI (ML, etc) and SSI: Post-Scarcity Utopia vs Hellscape?

Session Conveners: Dmitri Z, Joyce, Davin
Session Notes Taker(s): Joe Andrieu

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

Slides: <https://docs.google.com/presentation/d/1YxEVKI4zHOG-6gAPOg90TvadYeN9h5zZ8uvsYBwHR8>

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

AI is moving faster than you realize. If you haven't been paying attention, please, do!

AI is driven by DATA. That's our jam. Personal DATA stores.

Not yet at AGI or ASI. It's this last one that is the trigger for the fear mongering going on right now.

Language model != just words. It's not just that they can use language well, it also means they can access all human knowledge.

Federate AI / Federated machine learning.

Not just privacy over the data. But also in terms of inferences, the models that result from the data.

Aggregation of surveillance is innate, so how do we navigate privacy in the face of that?

GPT4 is the first model that isn't published (in terms of papers describing how it works)

Supercomputer data centers running for months. Insane costs to build the model.
But now we can do this with reduced computation.

Code generated by AI was less secure than human written, but the people who used the AI thought it was more secure.

These models make up crap.

Some people think of this as hallucinations.

But its actually dreaming, because they don't have context.

The reason openai introduced Chat GPT to the world was to get more training data.

Once you've done the training, you don't need to keep training. You can do the inference with much less compute and storage. It can fit on your phone.

Dreaming means we have some bounds on what we do, relative to hallucination, where we can be convinced to do something real.

Two types of networks.

- Large language models
- Reinforcement learning

ChatGPT interface is reinforcement learning. That requires some human-assisted scoring of what is good and what's bad. That is a separate interface to ChatGPT. Typically, they've been hiring people to do that training, mechanical Turk style. But this training is quite narrow. It doesn't include our values and morals. They don't behave in a way that is safe for us and our communities unless we participate in that training.

Worldcoin wants to scan your eyes and give everyone \$13,500/year as hush money.

<https://worldcoin.org/>

Concern: when we talk about morals and values and such, AI creates a single answer. (Disputed)

One way to address this: we can all have a small transformer. Our personal AI. You can train it. It can talk like you. Participate in training the foundation model. Which matters because if you aren't a part of training that model, you aren't enfranchised.

The key thing: for better or worse these models CAN be personalized.

Microsoft 365 co-pilot video. It will learn on your businesses intranet. Now it is more likely to answer with details from your company's spreadsheets and marketing, etc.

From ethics: won't that incredibly reinforce the trust we have in these systems

What we need to fix is more important than having more freedom, we need to fix the low-trust society we are moving towards. Truth does matter.

Context matters. Pre-prompting in ChatGPT.

openassistant is an interesting open source project <https://open-assistant.io/>

Need some baseline regulation. Some sort of identity for AI, perhaps with different requirements for different levels of power. Bikes, cars, trains all have different regulatory frameworks.

We all have one of these deep neural networks on our phones: Gboard from google speaker independent voice recognition that is phenomenal, and it's only 50MB

Openness can help to understand what is going on and how these models are developed, but it also creates HUGE privacy problems. Can we survive privatization of secret AI?

We're born into this world and we all have to play a game. No one tells us the rules and only a few of us get to win. Soon we'll get to a point that value creation does not require human labor. At that point, unless you have equity in the means of production, then you aren't redundant, you are superfluous, which most people won't enjoy.

If there's general acceptance of SSI and such, we can change the game. We don't want the people who wrote the current rules to draft the next rules.

What we need is an underlying fabric of attribution for flows and interactions that allows people to make their own decisions about how we live our own lives.

We have the value. And we can add it to the general database. By retaining attribution, we can keep track of how we each contribute.

This moment is SHORT. We have to go.

People will build their own robots that work for us. That makes us owners.

This is a collective action problem. We now have the means, with AI for us, to make contributions for us.

Not everyone will want to participate.

ACDC reference / Principle of Least Disclosure / Contractually Protected Disclosure

<https://www.ietf.org/archive/id/draft-ssmith-acdc-00.txt>

"Chain-Link Confidentiality", n.d., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2045818

See also:

Ricardian contracts https://en.wikipedia.org/wiki/Ricardian_contract

(we can protect our data)

Need traceability on how data is used

We don't want your AI unless it incorporates our data.

Watson: 80% of the cost was data acquisition. Only 10% was the hardware.

What they are doing with those server rooms should become a commodity.

AI isn't just another tool. Our hammers have never talked to us, presenting themselves as cognitive entities.

John Searle -- Computers don't think because they are syntactic not semantic properties.
Transformers broke that.

This can be creepy. How do we fix that? Language and framing? Or more substantial changes?

Restrict Act just introduced is super scary. I just don't trust regulation.

We may not want to be part of this AI, but we are. It's sort of the soylent green of existing AI.

Clawing back some sense of rights to what we have made. It is us. It is ours. It is our legacy. That has to be liberated.

OpenID Foundation board is looking for a paper on the risks of this technology. That might be just landscape assessment, but then also, solutions to problems.

Coalition for Content Provenance and Authenticity (C2PA) - <https://c2pa.org/>
Dmitri's call to action. Bring your personal AI demos at the next IIW in Nov 2023.

Credential Trust Establishment

Session Convener: Mike Ebert

Session Notes Taker(s):

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

No Notes Submitted

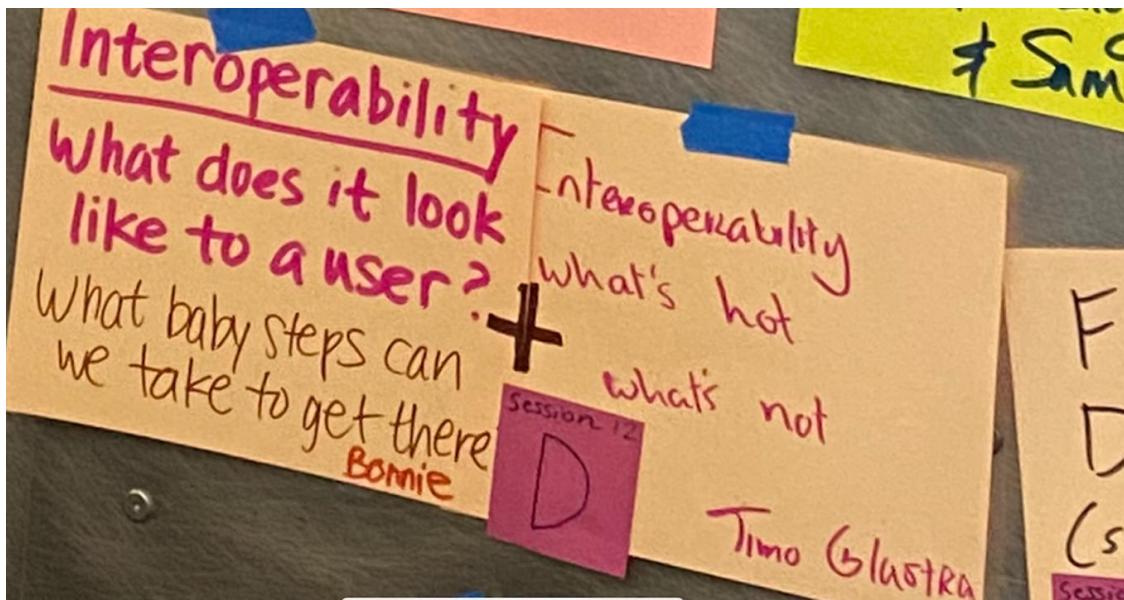
Interoperability: What does it look like to a user? What baby steps can we take to get there? & Interoperability - What's Hot? What's Not?

Session Convener: Bonnie & Timo G
Session Notes Taker(s):

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

Interoperability, end users, technology creators

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



Key takeaways:

1. A user doesn't care about protocols and all the nitty gritty. They care about the task they want to get done. They expect it to just work!
2. On the solution builder side, interoperability is always an important consideration. However, investing in interoperability too early can take away from other important goals like ensuring a seamless user experience for the problem at hand.
3. Context is important. Widespread interoperability will not happen overnight. But it can emerge in smaller contexts, perhaps within a technology circle, or a particular problem space/vertical. Take baby steps.

In summary, interoperability includes both user and technology considerations. The increasingly diverse talent showing up at IIW tells us we can accomplish this!

Interoperability

What does it look like from a USER'S perspective?

- ex. can choose any wallet multiple wallets can work to - familiarity for the user & convenience
- context : ex. credentials are created for one and often used in another context - data enables different contexts.
- when you don't have it - it stops you from doing what you want to do
- convenience for both user and dev - not collecting data over and over

- 3 layers
 - can I talk to you?
 - can I understand?
 - can I trust that

UX +
- credential design - what's in it?
verifies vs user's data needs.

{ what's hot?
what's not? }

- inter trust domain protocol - HOT!
- UX - HOT!
- actually testing between 2 user interface HOT!
- portability of credentials - HOT!
- pick and choose what I want to show - HOT!
- focusing on it too early → figure out the right time

Q: Trust establishment vs "interop"

Who is the user → the audience for which you are solving a problem

{ What are baby steps we can take to get there? }

- having a way to grab from more than one wallet - Web3 context UCAN (ucan xyz)
- how to incentivize market players, accessible
- TOIP tech - trust spanning layer - US health care portable Blue Button "Green Button" for energy sector
- governance - reusable pieces
- 4-corner interop model (Ken Holman)



Blockchain and Biometric Signatures

Session Convener: Tchaikawsky "Troy" Samuels
Session Notes Taker(s): Troy

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

Balancing the power granted in bills/laws without expectation dates, greater accountability and clauses that can void the bill/law.

Using transparency to build greater trust. If A 2-factor key generating repository is used then, query request should be logged on an immutable ledger and accessible via FOIA requests.

The overall draft structure would include:

- A open source matching software that hashes the biometric
- A govt issued key for generating a time-based 2-factor authentication code that is granted when a citizen submits only their biographic information.
- If someone is being investigated for a crime, one organization can make a judge approved request with a date ranges for a list of valid codes for the time range requested
- The requesting agency would hash the codes and combine it with a hashed biometric value to run a querying against the approved date range to identify any matching transactions.
- These request are logged on a blockchain in a way that allows for audits and to ensure corrupt abuse of the system is not at play. It would not be entirely visible to the public but would be subject to FOIA request.

This is an initial framework work that would help privacy/ policy and legal entities find a middle ground to bridge trust between government and pseudo anonymous Blockchain activity.

There still needs to be economic incentives to help this voluntary system flourish by offering business opportunity for businesses, convenience to the public and make it easier to comply with KYC and other financial regulations.

Dazzle Office Hours/Intro Get Your Personal Data Back!

Session Convener: Johannes Ernst
Session Notes Taker(s): Johannes Ernst

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

<https://dazzle.town/>

Creating A Decision Matrix Around Credential Exchange Protocols

Session Convener: Mathieu Glaude

Session Notes Taker(s): Mathieu Glaude

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

This is the document that we started working on during the session:

https://docs.google.com/spreadsheets/d/1_KKQZmmNRnEME96fZCPbMW-TC9j0tQ-dVuk5zzKa8U8/edit#gid=485340784

Inspiration was taken from the credential profile credential matrix:

<https://docs.google.com/spreadsheets/d/1Z4cYfibbE-rABcfC-xab8miocKLomivYMUFibOh9BVo/edit#gid=1590639334>

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

The purpose of this discussion was to see if there was value in creating a matrix where we could compare various credential exchange protocols against a common set of criteria. We concluded that there would be value in this, and have agreed to continue working on this document linked above. **If you have interest in participating in this effort, please include your name in the Overview sheet of the spreadsheet.**

Deep-dive on creds.xyz (a decentralized social reputation system for Web 3 Communities & DAOs)

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

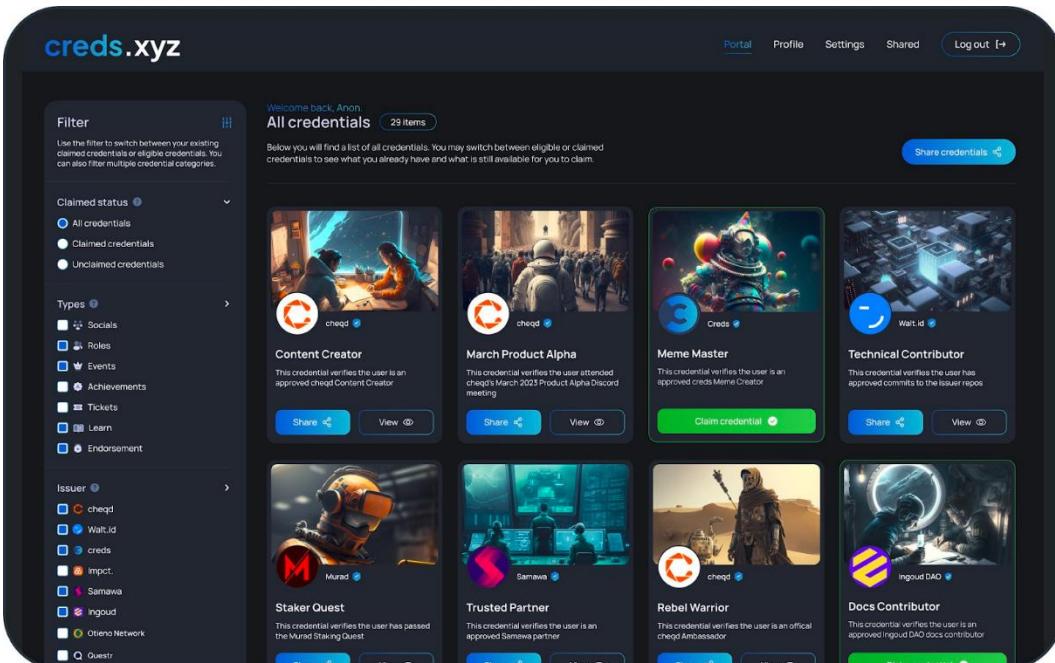
Tags / links to resources / technology discussed, related to this session:

Signup for waitlist on [creds.xyz](#), we'll be slowly expanding beta access

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

Building [creds.xyz](#) over the past six months is [cheqd.io](#)'s effort to make decentralised digital identity have **real** adoption. We're doing this by trying to make social reputation portable across Web3 online communities. We want to show that SSI can demonstrate product market fit by showing off a north-star use case that is **fun** and **engaging** and can have 100k's/1m's Monthly Active Users.

Check out [this Twitter thread for a full recap of how we're building this social reputation system.](#)



Dynamic Pitch Modulation and Satiric Prose

Session Convener: Jacob Siebach

Session Notes Taker(s): Jacob Siebach

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

Never Gonna' Give You Up: <https://youtu.be/3BFTio5296w>

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

To the tune of Rick Astley's "Never Gonna' Give You Up":

We're no strangers to Identity;
You've written tools, and so did I!
We're here to discuss what we're thinkin' of.
Talk to Phil or Doc, or even "IdGuy"!
Aaaaaaaaand if you're wondering what SPAC is,
It takes three sessions, just to see!

Yes, I just Rick-Rolled you,
Here at IIW!!

KERI IPR??? If it doesn't get cleaned up it's going to hurt

Session Convener: Kaliya Young

Session Notes Taker(s): Kent Bull

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

Kaliya: How do we get the KERI licensing into a good state?

Inbound = outbound policy of GitHub. Means licensing restriction of any inbound contributions has to match the outbound licence.

GitHub has a very well written description of how to manage an open source community on how to understand best practices for licence management.

Markus: The concern is that KERI used to be a work item in DIF, people who used to agree to the charter would contribute to KERI.

How do we protect against malicious contributors?

Sam Smith: inbound=outbound is agreed to when you use GitHub, when you sign up for a GitHub account. It is an implicit CLA.

I always do my homework. If other people didn't do their homework then that's ok.

We follow rigorously the Apache 2.0 licence policy and the inbound=outbound policy from Github.

Ray: Is there any potential for conflicts between the Apache 2 licensing and the IETF licensing?

Sam: No, the IETF licence is less comprehensive. it is essentially a lesser form of BSD. Apache is more restrictive and specifies in more detail what your contributions can be used for. They are compatible in the sense that you are only contributing spec text to the IETF. Apache 2.0 includes patents, source code, and everything else. You will find this on many open source projects that they will have multiple licences and you have to define what that means.

Lucy: Did I hear right when Sam said there is no Spec under Apache 2.0?

Sam: No, there is a spec under Apache 2.0. We will contribute it to IETF. When it is contributed to the IETF it will be contributed under the IETF licence. It is not any different in any fundamental process in many ways to the DIF contribution process. The difference is that in DIF you have to delineate between specification and code contributions. Under Apache 2.0 it is simpler and more straightforward. We also use the inbound=outbound rules to make it all easier.

Ander: It is still not resolved for me. If you go and try to work on an item you can be very lost on where to go. It isn't clear. It should be clear who is pursuing this effort and where to put contributions.

Sam: Yes, I would love if the DIF would put a notice on the website to point people to WebOfTrust.

Markus: I am just curious, why the Apache 2.0 licence and not the Creative Commons licence? Apache 2.0 is usually used for code, though is it used for documentation and specifications?

...No answer...

Kaliya: Multiple questions

1. Are there any KERI specifications in DIF?
2. Why was the decision made to leave DIF?
3. What is the governance over the existing specifications?

Phil: About leaving DIF, there was a disagreement about the membership policy of DIF. There was an independent consultant that was told he needed to join DIF in order to contribute. He needed to pay a high membership fee.

Sam: there were also people from large companies that wanted to contribute though they couldn't because DIF required their parent companies to join.

I also hired an independent consultant and paid his salary for a month to contribute yet because of DIF's policy none of his contributions were able to be accepted.

Kaliya: how does the WebOfTrust governance operate?

Phil: Benevolent Dictatorship for Life - BDLF

Book mentioned that covers various models of open source - [the Success of Open Source](#) by Steven Weber.

Catherine: What is the next step to do away with this confusion? How do we update everyone who needs to be updated?

Markus: two things can be done on the DIF side:

1. Existing repositories can point to the new repositories
2. The WebOfTrust repositories can explain the history of what happened and why it is all okay.

Andor:

1. Archive existing repositories, making them read only
2. Channels in DIF that are currently active right now that get updates all the time that should have it clear that nobody will respond to messages on those channels.

Sam: to Markus' comment I specifically refrain from talking about anything with DIF on the KERI README. If it would be helpful I would be happy to add a Readme stating the emails from DIF stating that they did the Intellectual Property Review (IPR) and agreed there

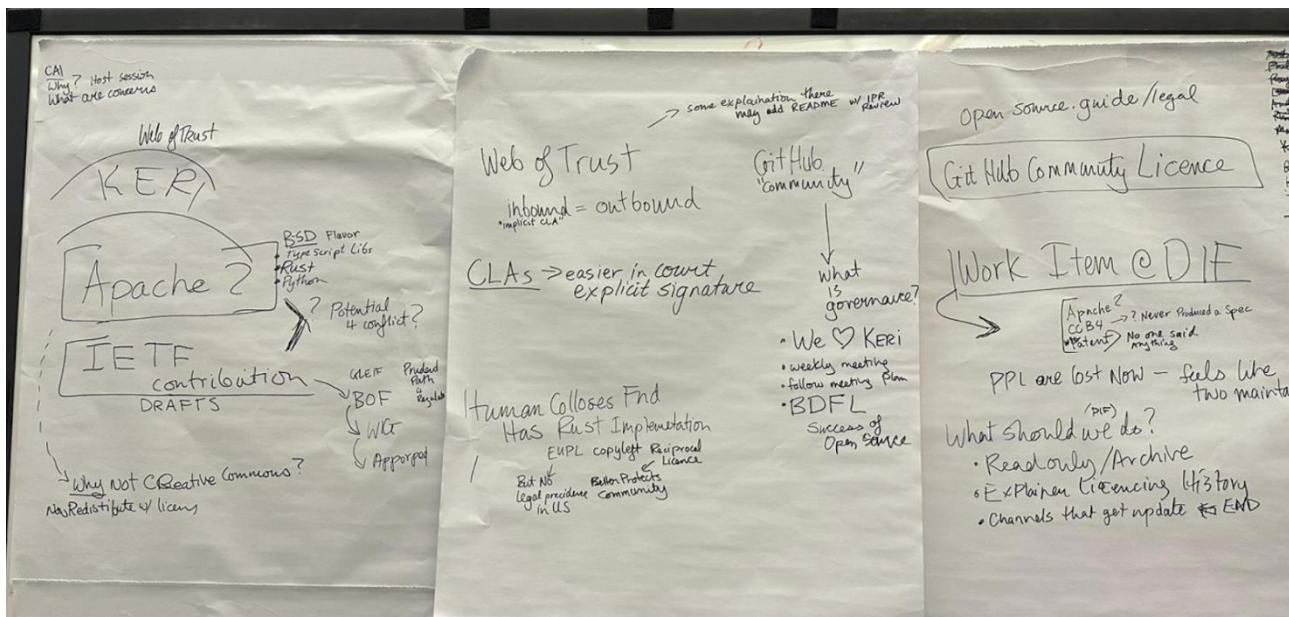
Kaliya: The Success of Open Source - a book on open source communities and why they work.

Lucy: I want to get clarification on the Human Colossus Foundation's KERI work (KERIox, CESRox). They have a Rust implementation of KERI.

Kent: They use EUPL 1.2. The argument came down to prioritising adaptability over reciprocal licensing. Since there is no legal precedent for the EUPL 1.2 in America it causes high legal uncertainty. Since Apache 2.0 has much legal precedent it has low to no legal uncertainty and American investors, specifically VCs, are more comfortable with the Apache 2.0 licence versus EUPL 1.2. So, maximum adaptability was seen as best arising from the Apache 2.0 licence due to lower uncertainty.

Sam: See <https://opensource.guide/>

Kaliya: ...took many good notes on paper throughout the session.



Fun with DIDComm (sub) Protocols

Session Convener: Nick Reynolds

Session Notes Taker(s): Nick Reynolds

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

<https://didcomm.org>

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

DIDComm is a transport agnostic E2EE communication protocol that can be extended via DIDComm Protocols that are not part of the core DIDComm Specification but are their own specifications registered on didcomm.org

Example (existing) DIDComm (sub) Protocols:

- Mediation
 - Message Types:
 - Request Mediation
 - Grant/Deny Mediation
 - Status/Pickup
- Basic Message
 - Simple message that contains a `content` string and a defined `lang` for localization

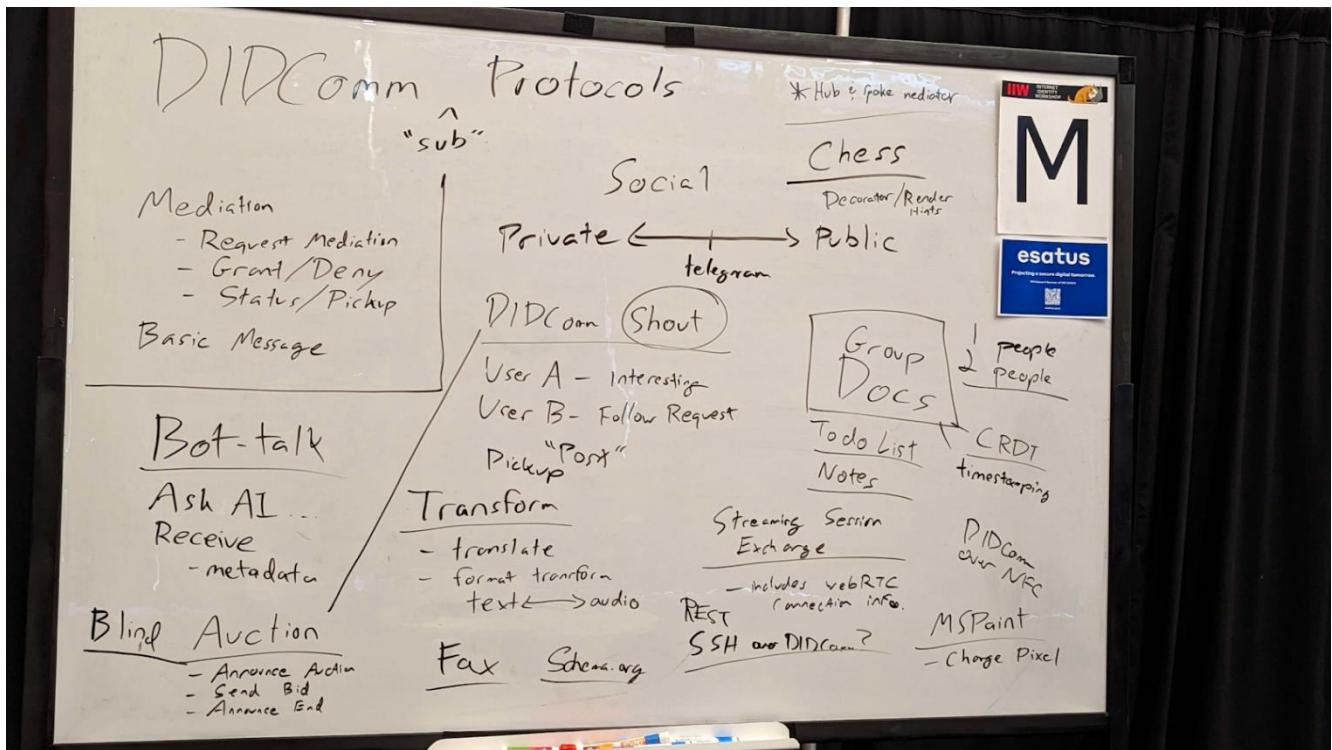
A few proposed ideas for future DIDComm Protocols:

- DIDComm Shout
 - A simple (not-super-scalable) social protocol, in the middle of the private-public spectrum.
 - User B sends a “shout follow request” to User A
 - If User A accepts, their agent maintains a list of followers and when they want to make a social post, they simply create a “shout” message and send it to all of their followers
 - User B’s Agent’s front-end aggregates all of the “shouts” they receive and displays them in a “social feed” format
 - Could possibly make use of the “pickup” message type, so that after User B starts following User A, they could request previous “shouts” to be delivered
- Bot-talk
 - A DIDComm protocol for interacting with LLMs/AI-Chatbots
 - User A could send a message to a DID associated with a specific LLM / Stable Diffusion model
 - LLM replies with a “Bot-Talk” message that includes not only the text or image generated, but additional metadata about the bot itself
 - What model is used (ideally referenced by permanent URI)
 - What data-set the model was trained on
- Transform
 - A protocol for transforming messages from one format or language to another
 - User A receives a message from User B and wants to share that content with User C, but User C doesn’t speak the same language as Users A&B
 - User A sends a “transform” message to a service provider to translate the content of the message from one language to another
 - Could also transform the format of the message (e.g. from text to audio)
- Group Docs
 - How could multiple users (or even just 1 user) maintain documents using DIDComm
 - Essentially sends diffs between different DIDComm agents that are interpreted in order to build documents
 - Constructing document could be difficult, especially when timestamps/order of diffs are unreliable
 - May be best to first focus on 1-person use case (e.g. personal notes / to-do list shared between multiple devices controlled by same person)
- Blind Auction
 - User A can announce an auction (either by sending a message to an “auction house” agent or via the “Shout” protocol)
 - Other users are able to submit bids directly to User A to create a blind auction
 - User A announces end of auction and then coordinates payment/delivery
- Chess
 - Simple protocol for 2-player game within DIDComm
- Streaming Session Exchange

- Use DIDComm to share WebRTC connection details to initiate a video chat/stream between users
- MSPaint
 - A service provider maintains a “canvas”, and pixels are updated on that canvas as “update pixel” messages come in from users
 - Users are able to fight for canvas territory like on Reddit “Place”

Other DIDComm Thoughts:

- REST/SSH over DIDComm
- DIDComm over NFC
- Fax over DIDComm
- Hub & Spoke model to handle scaling concerns
- Decorators / Render Hints included in DIDComm messages so that new protocol messages can be displayed without additional work



SESSION #13

WebAPI/Quy language to VC's (again)

Session Convener: Torsten Lodderstedt

Session Notes Taker(s):

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

No Notes Submitted

Your Identity is NOT Self-Sovereign

Session Convener: Justin R

Session 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:

- Presenter has an issue with the term “SSI”
- The fundamental issue is that there are different flavors of identity that are constantly getting conflated
- We have an “Intrinsic” and an “Extrinsic” notion of identity
 - Not to say that we ourselves “have an intrinsic/extrinsic identity”
- Intrinsic is “your selfness” – it is internal to you.
 - This can take a lot of different forms
 - The type of person you believe yourself to be
 - How you self-identify
 - Your immune system
 - Fundamentally decides “which parts of this bag of fluid walking around are and are not you?”
 - Autoimmune disease could decide that part of you should not actually be part of you anymore
 - SSI community talks about intrinsic identity *a lot*, but we’re building digital systems that are fundamentally dealing with *extrinsic* identity
- Extrinsic identity is not for you to decide
 - I do not decide my identity
 - I can choose which *parts* of my identity to disclose
 - I did not share which autoimmune disease I had, and I won’t share other things with you

- These, however, are not my identity; they are attributes. You use them to form *my* identity for *you*, which I do not control.
- I do not have a single intrinsic identity; I have many
 - There are many different aspects and things about myself that all coexist and intertwine
 - My identity in everyone else is a different identity for each person
 - Everyone's identity for me ties back to my intrinsic identity/attributes
- When I authenticate with a digital system, it doesn't care who I am; it just cares about *who it thinks I am* and what that means to it within its context
- Google used to brag that they didn't need you to log in to know everything about you
 - They didn't need to *know you* to know *everything about you*
- Self-sovereign identity is bullshit
 - It doesn't matter what I assert about myself in the world; it only matters what is perceived
 - When I send out a message, I can do everything in my power to control many aspects of how it's crafted/delivered/etc., but all that matters is *how it's received*, which is not fully within my control
- **Question:** Is one of the concepts here that I can say "I am John Doe to chase.com" but really in the context of that service I am user XYZ and they don't care about my "identity" (name)
 - Yes.
- Example given of DMV marking an alive person as deceased
 - This is an example of an external entity having a view of your identity that does not match with your own, and their view of your identity is very important
 - People believe what the DMV says about me; that's a problem for me if part of what they claim about my identity is that I am dead
- There are a lot of identities that get assigned to us that we have no control or even insight into it
 - This is obviously a massive driving motivation for all of the self-sovereign movement
 - You don't get to say that I'm dead; I get to say I'm dead.
 - But who cares what I say about me? People care what the *trusted/powerful entities* say about me.
- An example of well-meaning digital systems having expressions of identity in them that are harmful: binary gender encoding ("m/f") for individuals who may not fit said binary
- Bank algorithm, due to timezone differences, kept re-encoding a birthday as a different day, causing a large identity issue for one person
- If you ever want to convince an engineer (who says "I don't make political decisions, I just write code") that all engineering decisions are political, have them implement timezones.
 - Taiwan claims (self-sovereignly) that it is its own country and uses a certain timezone, yet China claims that that is part of China and therefore uses the China timezone
 - If you load up Windows in US, there is a timezone option for Taiwan; if you load it in China, there is not
- One health system encodes three values for gender/sex: sex assigned at birth, gender identity, and current legal sex.
 - These are all very important aspects of identity in different contexts
 - An example of designing digital systems to maintain the human element and how engineering decisions are inherently political decisions
- Will Smith famously said that, when filming The Fresh Prince of Bel-Air, he requested that his character be named Will Smith "so at least people would get my name right"
 - To all the world, the actor who plays Carlton is just known as "Carlton" – that's the identity ascribed to him. Nobody knows of him as Alfonso Ribeiro.

- Should we maybe define identity by three categories:
 - 1. Something you control
 - 2. Something you can influence
 - 3. Something you cannot control or influence
 - Fundamentally the thing that matters is the *acceptance* of one's claimed identity *by others*.
 - We should be focusing on the reception aspect.
 - Having “clean” data (ie well-known data formats and data that slots into it) is attractive to engineers / the technical world, but brings with it inherently political ramifications.
 - I got set on “default mode” when I was born in terms of the ways that the (US) identity systems
 - White / cis / male / male-presenting / etc.
 - These are the default things that are assumed about people, with “tweaks” necessary to be identified as “non-default”
 - The name “René”, when stored in the Massachusetts systems, is encoded as “Rene” – which is simply a different word.
 - A technical decision (with political/identity ramifications) was made: encode names as ASCII.
 - Identity has no value or meaning without a relationship to something else
 - Identity is directional
-

Notes by john

Intro by Justin: “I think we have a couple of flavours of identity as we go through the world, and these flavours are conflated as we go through the world” Talking about the models and how we approach this as we discuss the complexities in the physical world and the digital world

- Intrinsic
 - Who you think you are
 - How you self identify
 - How you project in the world
 - All the way down to your immune system

SSI Community talks about intrinsic identity but it is in the digital world which is more extrinsic

- Extrinsic
 - Things projected out and controlled by others

We do not have single intrinsic identity, we have many. May different aspects of self that interact. What the other perceives about the self, is the identity. All that matters to a digital system is what attributes it enters or uses in its' system

When we look at surveillance capitalism views of identity, companies know your identity before you interact with them

What the self projects or sends as a message doesn't matter as much as what information or attributes are stored or used.

- What happens when the institution has a person recorded as deceased when they are still walking around

Metaphor for data cleanliness - when is data cleaned - on import, or use etc - answer - everywhere you can

Question about unique self and normalized/cleansed data at the other - lost uniqueness?

Audience examples about institutions who can't record birthdates correctly when the birth is in a different time zones.

Audience comment about people being in a contract with their government - doesn't square completely with the intrinsic/extrinsic model. - The government model used the extrinsic physically existing person. This is external to the individual and is asserted by the government (the government hold the attributes)

Audience: As identity practitioners we have a responsibility to pay more attention to the humans in the machine.

Talked about different fields related to gender in medical records (sex at birth, gender identity, legal male/female)

How to bridge intrinsic/extrinsic. SSI is concerned about chosen presentations

Audience context for SSI is primary the first of the following:

- Something you can control
- Something you can influence
- Something you cannot controls

Our identity systems need to better at excepting what information is pushed out by the self.

Without the ability to receive what is being pushed out by the individual is necessary for the ability of the individual to express themselves.

Privilege in systems -

- system assume the 'normal' or the 'privileged'

To what degree does SSI help or hinder organizations understand that the subjects need to be able to influence

On the use of the word sovereign - can't force the service provider to accept sef assertions.

- Provider determines what are the necessary attributes required to provide a service (constrained by regulation)

Binding Identity to Publicly-Visible Content

Session Convener: Eric Scouten / Adobe / Content Authenticity Initiative
Session Notes Taker(s): Eric S

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

Slides available at: <https://acrobat.adobe.com/link/review?uri=urn:aid:scds:US:e5c06b52-27c9-4e72-8f25-c6c13057a64c>

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

I don't think anyone took notes beyond my slides.

AUTOREP - an autonomous decentralised reputation scheme

Session Convener: Johannes Ernst
Session Notes Taker(s): Johannes Ernst

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

Description of the Autorep scheme: <https://reb00ted.org/tech/20220810-autonomous-reputation-system/>

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

Reviewed the scheme. Lots of discussion on application areas, potential attack vectors and implementation choices. No new attack vectors found :-)

JSON Web Proofs - Status and Progress

Session Convener: Dan (?)
Session Notes Taker(s):

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

No Notes Submitted

Delegatable Verifiable Credentials

Session Convener: Phil Windley, Alan Karp, and Sam Smith
Session Notes Taker(s): Phil Windley, Jin Wen, others

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

Requirements must be strict, otherwise it will introduce vulnerability

capability: unforgeable, permission to

Delegation vs. Holder Binding

There's a difference between attributes and permissions. Credentials are usually filled with attributes that can't be delegated. Permissions can be.

Driver's licence gives permission to drive any car (in certain classes), a car key is a capability to drive a specific car.

Guardianship is a good example of a delegated authority. Long term (parent-child), short term (nanny-child)

[Authentic Chained Data Container \(ACDC\)](#) has two modes: targeted and untargeted. Issuer can issue credentials to specific entity or not. see spec page: <https://trustoverip.github.io/tswg-acdc-specification/draft-ssmith-acdc.html>

Credential is evidence of an entitlement

Claim is a statement of a fact (sky is blue)

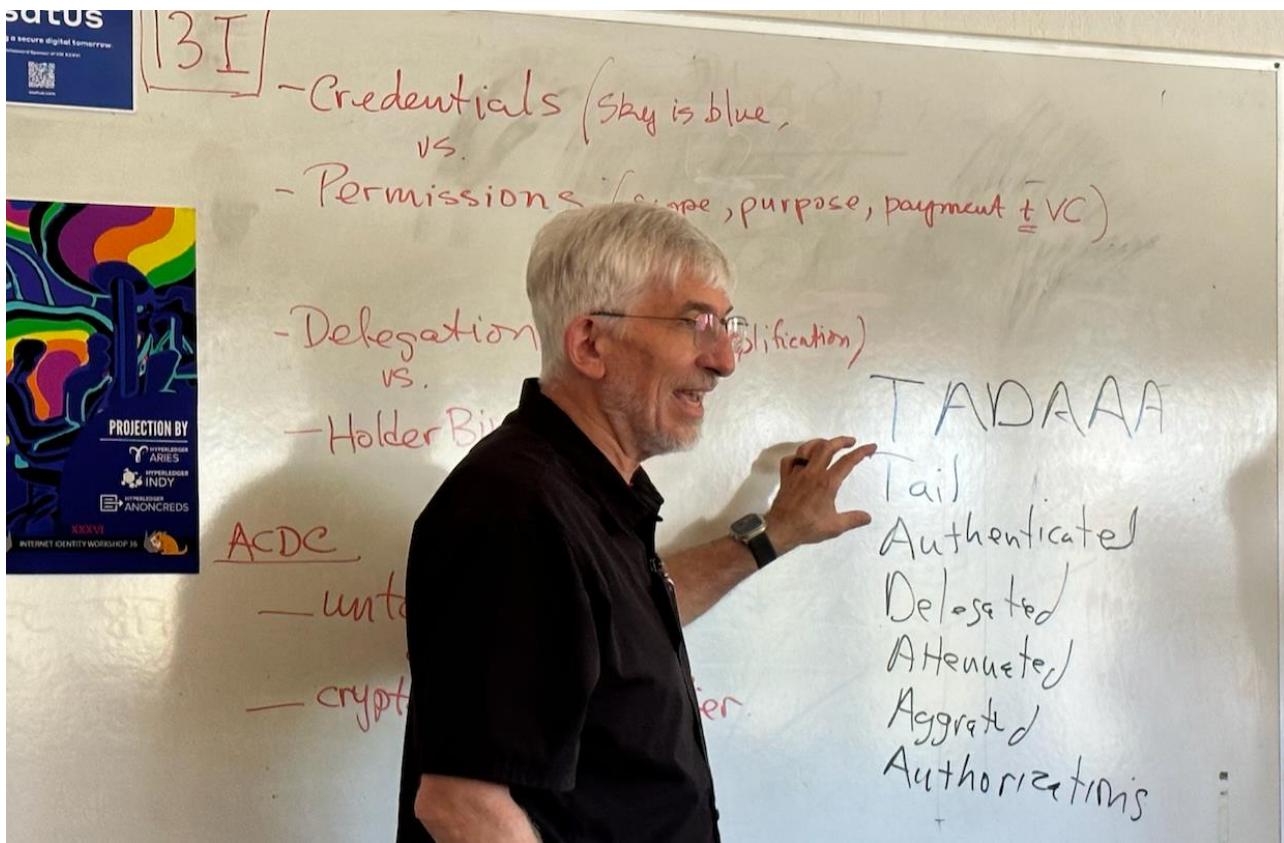
W3C credentials have a subject but don't say who it was issued to.

IXBL is a standard for issuing a business quarterly report. That's an example of untargeted issuance. Untargeted credentials aren't delegated.

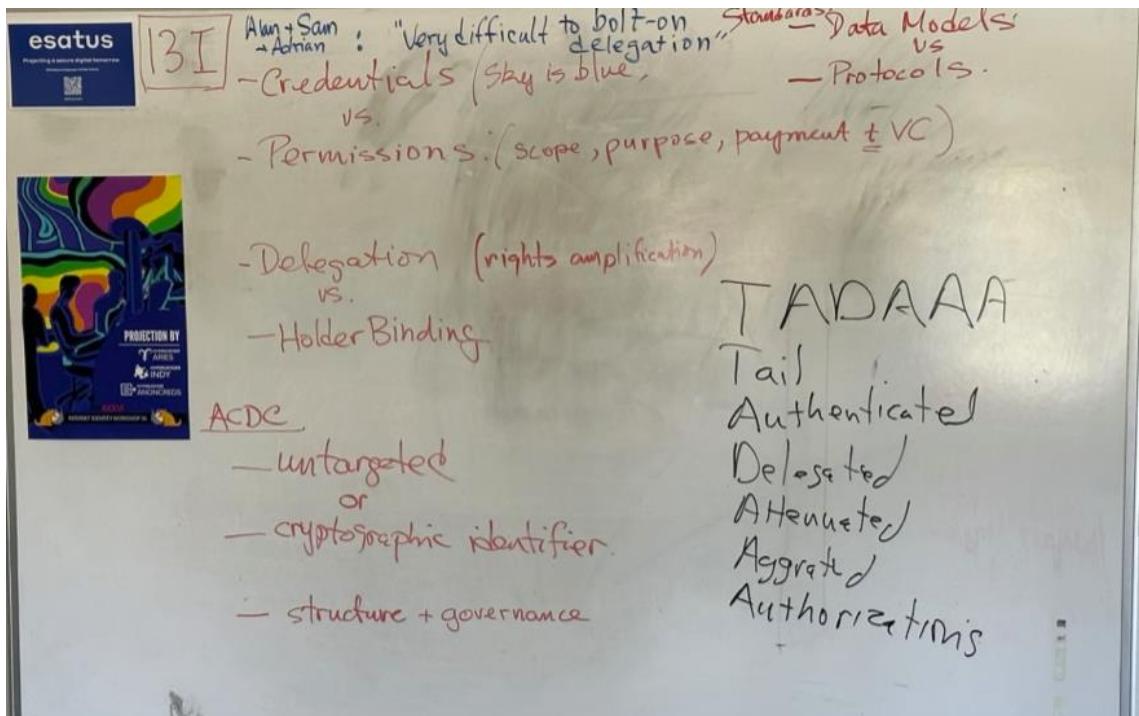
Rights amplification: you need prescription + proof that you are the person who the prescription was issued to OR their delegate + proof that you're over 21 (for some substances).

Attenuated delegation: Allows another entity to act on a subset of permissions that the person holds.

TADAAA: tail authenticated, delegated, aggregated, authorization. (verifier has to follow chain of delegations from tail to head)



Delegated permission could be a new credential/certificate just for that purpose.



Transcripts from Whisper Transcription:

[INAUDIBLE] Yeah.

And a question I want to ask you is, the way I've heard Phil introduce the issue is that the street is either that you need a delegation, or it was about hotpling, or you had places where you would not have delegated like the passport, for example.

And of course, that's true.

The question we knew here is, if you design a protocol around verifiable today, and I'm not talking about definitions, but on verifiable credentials, which are based on the passport that I've made.

You are concluding and not approving them, and maybe that's where they're sort of allowed to prevent the person.

The other one, the one where they said you needed that that we can like the procedure.

And so my question is, is it true that if you design for elevation, you can always do the non-derivatable password through space, but you can't do it the other way around.

All right, so the question was, if I design for one, then I get the other essentially for three, and not the other way around.

That was the question.

Well, I'll be honest, I'm kind of struggling, but then the same and you have to be separate.

In my mind, this is going back to my head based on my rehab.

It is a versus a has a relationship.

And yes, you can create tables that you really really specifically have in a family.

But if you also follow best practices that we might look at and properly meet the pros list, then the underlying technology still works in both cases.

- Right, but the problem is the networks.

And so-- - The board is not right there.

(audience laughing) - Yeah, so the problem is, if you say you should do something, they will do it.

And that means that if they're trying to issue a claim credential, I'll tell you, a permission credential, they may not include the specific thing that it's actually giving permission to.

And it's a problem.

So you want to have very strict rules that when you're verifying this thing for this use, these fields are mandatory, these other fields are forbidden, and vice versa.

And those sets overlap, but they're not identical in the two uses.

- Well, if you're looking at like, we're taking a particular view of the world, I'm gonna view how programmers might like to do this, and then imposing that onto them and saying, "This is what you're doing.

" - I'm saying if you don't make the requirements strict, they will work around the margins, and in this case, you're gonna end up with vulnerabilities.

Not just gonna be confused, but you're gonna end up with vulnerabilities.

That's the risk, that's why I have to restrict it.

- Sure, and we can have this discussion but I don't want to be over there.

- I wonder if you can give an example of a property that would be required in one, forbidden in the other, or vice versa to try to kind of clarify this.

- Yeah, so the permission, I have to name the specific object I'm giving the permission to.

And in a driver's license, what does that even mean.

But somebody might say, you know, it's your car, and all of a sudden I have a driver's license that's just for driving my own car.

I could imagine that there was a-- That's the very thing.

That's right.

And in our classes, but it's not a specific part of the process.

So this is something-- these permissions are something called capability-based access control.

And a capability is an unforgivable, transferable permission to use the painted desk.

And unfortunately, transferable permission to drive my car.

That's a capability.

But it only works on my car.

It doesn't work on your car.

Whereas my driver's license I can use to drive my car.

So these things are essentially different.

But as I said when I started, I think that our times when we want to be able to delegate are claims to maybe just assault where these are acting on a account rather than another person.

Not a prescription problem.

We actually had that.

My wife was taking pain meds and she sent out a 17-year-old son to go pick up the prescription and he couldn't.

But she was only 17 and it was a controlled substance.

if my wife could have delegated to him the complaint that he was acting on her behalf as someone over the age of eight and a tenacular solid spell, and it was actually a delegation of a forever complaint not a permission.

So I'm the author of "The Description of Space" five, seven years ago.

In the "Barthel Credential" context.

And one of the issues that we need to address, because I was going on the premise, which Gerald and Alex were verified, that we want there is a community to have the construction be at the sea.

Now you just earlier said exactly the opposite.

I know.

And so since it's a good use case that we probably have thought about, can you, the point that was difficult for the community to manage, and I still have the gift and the solve, is the reputation point that you're there.

because I point without, I mean, the police said it was strictly, it was strictly, you had revocation, but so you had revocation, the president was filled by some point, so you had revocation by the position that you issued it, and you had, the police posted it, then you went and had to open the evidence.

So, and they also come to that, how the surveillance components, which is people's substances, which was doing surveillance on most of the physician were sure as well as the doctors, and that's because they're going to be subject to the other medicines.

So, the prescription use is actually for their treatment.

- It actually has a delegation in it, in that the physician has got permission to write the prescription.

The prescription must be a delegation from the doctor to the partners of the-- so let me sit down and ask you a given that you all have this nice and brilliant thing, where what was I going to go and say that my team fell prior to the angels.

Do you know what it is.

To me, the prescription is the permission to receive the medication.

But it's not a capability in the sense I manage, because it doesn't designate a percent of pharmacy for active debt.

I would say prescription is a bad use to verify with credentials, because it's a double spend problem.

And you actually want it to be essentially a cryptocurrency type of thing, rather than a credential.

So because in a verify with a credential, it's the issue, or generally, that does the revocation, not be a verifier.

- I agree with you.

- It wasn't terrified me.

- I understand that.

- So I want to make the point that in computer science, Western Ranchert came up with the speaks at, speaks for relationship.

And in our claims credentials, we don't have that ability right now.

And the more I think about it, the more people know.

And so the validation of the claim, that it speaks to me on the basis of this credential.

I think it's actually a useful concept.

And yesterday I released some writing.

So it is easy to do that.

Good.

[INAUDIBLE] Well, writing.

Yeah.

So-- [INAUDIBLE] [INAUDIBLE] Yeah.

Right.

So that writing is a good example.

I'm just wondering if you can think about it afterwards.

[Inaudible] Right.

And so this is where I came up with the problem, which is up to six of those restores on the consent of some.

So I can delegate the permission.

So we can do this as a permission.

And in fact, from a lot of the guardianship, you can think of your child as having a set of permissions as representative of individual families.

And I'm delegating to you.

that in that sense is you gain responsibility if you can see the delegation chain.

You could delegate it to a man.

You can also delegate the leadership and make the essential permissions rather than clients.

But I think it's important to just break the line and which one you choose will determine how you build the system.

[INAUDIBLE] [INAUDIBLE] I asked my question because I need your answer.

Yeah, I got it.

Which is, is the difference in the [INAUDIBLE] that if you design the delegation, you can get what you call hold the monument for three.

But if you design the hold the monument, you cannot get the delegation for most of it.

Certainly, if you start with the boulder, you're not going to get the initials, because boulder mining is not making a specific object if you have permission to offer it.

Which is what I feel like that's so pretty similar.

But if you start with the claim that the building is capable of it, it's not boulder mining defined by nature delicately.

- It must be, don't you.

- Is that fixed with your model of what's going on.

- Yes, I'm always confused by a phrase.

(mumbles) An AC/DC model, we have two models of AC/DCs.

Targeted, untargeted.

Untargeted means there's no target of the issues.

issues something, they can make claims, they can issue reports, they can make a statement of fact, they can do work, they can say whatever they want.

And all that you're getting is the ability to secure and contribute whatever that issuance is to the issue.

The sky is blue.

The sky is blue.

Right.

in a targeted one, you're saying an issuer that has an identifier.

And we only use cryptographic identifiers because we don't want to fall down the trap of some object with properties that you can physically consolidate to some entity with cryptographic things and then target the other identifiers of the cryptographic identifier and say I issue this, so you have an issue by an issue two.

We call the issue by the issuer, the issue two the issue week.

So you have two identifiers.

What the issue two gets by that issuance is completely dependent on the ecosystem governance framework for the type of issuance that you make.

So to give an example, I want issue two here and issue two here.

That's right.

[Inaudible] >> No, I don't say that.

One target is the sky is blue.

It's a class public key point of start.

So there's a confusion in the term credential, which I know there's lots of language lawyers out there, but the word credential is defined to the evidence of entitlement.

That's the number one definition.

evidence of an entitlement, a claim could be a claim about an entitlement, or it could be a claim about that, like this guy is blue.

So to say credential, you have to be fine, you have to be fine for precisely that.

As a community, say, well, credential means claims, or credentials mean entitlements, or did you go.

But when you start to say it's a credential or permission, Well, you have the third one, I am talking.

So the third one is that I've been using credential lists saying something about a particular target.

But you've added one.

This is a claim about the state of the world in the end of the making part.

No.

But the number of people in the very far front of the union will say no.

That's right.

So no.

You can't all be a bad one.

Why bad in that.

values cases to make claims about things.

So our different, and I can't, I can't, government, government is next.

(audience member speaking off microphone) - The government.

- The secret issue is a untargetable, if you read this back, there's nothing about who it is issued to.

So all it's saying is a issuer says something about a subject that can be verified.

doesn't say it was issued to the subject or anything like that.

And in fact, they can be transferred around.

And it's in respect that they can-- it is outside of respect to determine who it was issued.

Or in fact, who it was presented, which is where the term "whole" is providing up from.

The whole group is presenting it to a verifier.

And they are providing some sort of proof that perhaps they are the subject.

But that's outside of the-- [Inaudible] [INAUDIBLE] [Inaudible] Yeah, that's the target.

That's the target.

I'm not saying this.

But this would be a good term.

Yes.

So in ACDC, one of our use cases is IXVRL.

So IXVRL scan, and IXS9.

com, right.

Also the company is supposed to scan.

[Inaudible] [Inaudible] [Inaudible] [Inaudible] So, you can issue an annual report in some of the science that is an untargeted issue.

And so, ACDC is going to be used for any part of the equation that is to be any type of issue.

And you can say, hey, we investigated the behavior of loss and how, and their gestation permits, and we want to publish a report on that.

I want to securely attribute the problem that we published on the board back to the issue of order, so that we can use an easy decision to do.

Because it basically says, I issued some information.

I made some claims.

I made some statements.

You can specifically tell.

[INAUDIBLE] Yeah.

[INAUDIBLE] Here's my information.

[INAUDIBLE] Then it would be different.

[Inaudible] Yes, in the sense that the authority is an asset of the mission.

So if I move a professor in university and I have standing in the community that says not only authority, it's sort of information.

and I have a graduate student that his document is authoritative, but I do it to write a letter of reference that said, on this subject, this graduate student actually does part of it, that the student gets part of it, but then they would release it.

That's giving them permission to not speak for the student.

So, you have both questions.

Does it make sense to know.

[Inaudible] So I have no trouble arguing the car, giving my way to it, so I'm ATM card.

I have to go right out of the house.

The ATM card was the capability of permission to withdraw money from the specific bank account.

So that was a permission market.

That was a commitment to my training to the car.

The prescription is close to that.

is permission to get a specific number of kills in the specific country.

How many.

Sorry, let me say eight.

It's a big one.

It's a big one.

But that's the way we did it in 1770.

But it could be a credential from the network to the doctor as from the medical reports to the medical group as granted permission to write the speech.

The doctor delegates that to my wife, and now she now has permission to put that in her (audience member speaking off microphone) But now, now it comes down to the fact, when I get a prescription, my doctor says, "What pharmacy do I come to.

" Now that's just advisory, but if you go to another pharmacy, that will transfer.

But in this case, they are designated a specific pharmacy, almost an exact set of pills that I use to go to.

So in that case, there's no need to be-- that once I fill the prescription, the pharmacy itself is a barber.

And you don't get that prescription because it's not there now.

[INAUDIBLE] Okay, what's confusing is that there's issuance and presentation.

So the right way to deal with description is the doctor issues an authorization to a pharmacy, and then it names the person who's going to receive it, and then the person presents who they are, the person to the pharmacy, and that presentation of their faith and wow, and now enables the rules the diplomacy is given.

But that's missing the step.

My son can't pick up on it.

That's right.

That's right.

And so this is where the claims credential, her identity, which she delegates that to myself.

Yes.

For this purpose, that would work.

But I was moving totally around from the doctor to the patient's agent of the practicing.

[INAUDIBLE] Because I'm not understanding.

I thought they would have to do the presentation.

the user has to present their identity.

(audience member speaking off microphone) Yeah, so what you're showing, in my approach, with those who are doctors, the patient, the major, what you're presenting to the pharmacy is a change of progesterone that shows that the doctor is certified by other medical (inaudible) The doctor agreed with the specific promotion to me and agreed.

I, that will be to you, but the mission to pick up on restrictions on my opinion.

I can help.

I think, what I'm showing the fantasy is the prescription and your driver's license.

And if your driver's license says that you're less than 21, and they may not like to pick it up.

But that is physically what is needed.

- That's the way it comes today, but not in prevention.

In prevention, it's a huge event.

- I didn't say it was a huge event.

You know, you corrected my initial thing.

- You know, it's a huge event.

(audience member speaking off mic) - Yes.

- But not in this event.

- But not in such an event.

- In the form of the internet.

- No, no, no.

The interesting thing is, we trust the curtain.

I've issued to her, just doing public heat, that's not attached to these things.

It might have been just for the purpose of all she has to do to the corresponding private suit.

So if you put ideal heat into it, you're wrong.

When you go, you're given to them that you are the person I gave it to.

Your father is the one that I date with.

No, that doesn't work.

Because you might really prefer as a 70-year-old-- You're adding a second condition.

[INTERPOSING VOICES] [INTERPOSING VOICES] [INTERPOSING VOICES] [INTERPOSING VOICES]
[INTERPOSING VOICES] [INTERPOSING VOICES] [INTERPOSING VOICES] That's right.

That's right.

So in that case, in that case, to pick up the controlled substance in a pharmacy will require an additional prevention.

This is called, for example, patient care.

Now to show that you are the agent of the person who is in the prescription list of issues and you need some additional criteria to handle this particular prescription.

[Inaudible] [Inaudible] [Inaudible] And it's very important, without attenuating delegation, every climate is-- the president has to enable him to fight with the permission to do that.

So attenuated delegation is I have a collection of permissions and I want a great impact on the subset.

And I can create a new delegation.

of the validating and the reprendential, that has a subset of permissions.

And the way that we prove that we have that permission is to simply prove myself that we're good.

There's a risk on that.

There's a position that I prescribe their own medicine.

I prescribe you what I come to try to help you make it.

And that would be a property of the verifile that has to guarantee that the delegations are legitimate.

So for example, if my delegate is subset of my position to Adrian, and Adrian delegates to speech members, more than I need him, the verifile would not be legitimate.

That's the way that it could be.

[Inaudible] We're seeing it live.

Sam Smith, I'm an academic.

I came up with this academic.

Oh, okay.

I was so hoping.

[Inaudible] This is not just too monic.

[Inaudible] [Inaudible] Whoever's its potato has to then fall back into the source.

And all that.

I want to think of the source of confusion, which seems to me to be the right thing to do.

Which is the difference between PCs being a data model and capabilities in the data model, purely.

And then the protocols, such as DIPM or DQM-PI, that are separately standardized.

So, we put this in the context of what we were talking about in the last two days, what we see and what we believe in the violence that you can face this is the fact that you can use a answer that a scientific citizen standardizes the data model with the protocols that are to apply to that data model in order to meet their intent.

Whereas in our community, the SSI, we've chosen to standardize of our state-building markets, and maybe others, but you keep taking the road.

- We have.

- But as a teacher, people reference some people go to the standards.

We've thought about this, and then we've completed an opinion of our goals, and our market interests have grown up into these paintings of standardizing protocols and that alone, a lot of things are forward binding, and resulting in periods of no progress on that front.

So is that a fair thing to say, that's eventually very viable, and the capabilities are exclusively made in models, and the public knowledge made a problem in the building.

- So the 1988 by which I understand, and I learned by myself, So I will leave all these details to understand this.

I will, I can specify what the requirements of the standards must be able to do.

I'm not worried about how they actually do it.

But for example, in the delegation of the handshake, I'm a full of brain research.

So, did it come to me and ask for a thesis.

I will make the decision based on evidence made in claims that he was at the end of the web.

I say it might be right at me, but it might also make the game different.

And I'm going to decide whether to go.

But I'm not going to delegate to you when you make the request, I want you to give me a help of heed that you created just for this case.

I just created for this whole case, and I will create the potential for what was in that key.

That's something that none of the world knows.

There's no sign of anybody.

I'm sorry.

So, when you're asking for a petition, we're going to present some reason why I was attending.

It's the idea of a bit of a union, some reason, but yet, the first one to do is to connect with us.

It's a complicated, just created for this purpose.

[Inaudible] [Inaudible] Now, whether you get an interaction or not is totally dependent on the ecosystem governance framework for the type of your initial year grantee at the moment.

So, ECE is just to provide a structure that says, here's a verified data structure that has a syntax and current data structure.

So, what you do with the data structure is it's almost everything done.

So, if you don't have an ecosystem governance framework, that should be useful.

[Inaudible] [Inaudible] Yes.

So you don't really know what's changing under the age of four years.

You're actually years of working for whatever they want to look for.

They can put whatever their education is in them, marks be so inspired, they have different rules to go.

[Inaudible] [Inaudible] [Inaudible] I say I don't recognize RSA systems.

I think about it.

And I'm going to find it different.

Well, that's part of the spectrum.

And you have to understand that.

I mean, you're only RSA systems.

You're lying back.

So we need to already say that.

Let me just add to the point that I look for the map.

I believe it's hard to do what you guys are just talking about.

You can do that.

Fucking that is using coke ins and kippets.

In other words, the only one that goes with the contents of your severe disease is the resource valve.

And if you want to do a delegation, you have to do it via coke exchange.

If you have a coke and you send it to the resource, there might be a new one that lets self-sail the conditions and enough that.

[Inaudible] So, Adrian wrote out data models and protocols.

And, you know, W3C, Verifiable Prevention, is a data model, which anyone can construct in any way.

But what that doesn't allow is everyone sort of figures out different ways of exchanging and doing things.

Does your idea of governance, ecosystem, include how one goes about issuing to a wallet, or a wallet, does they take you a whole very fast.

Those are protocols.

Yes.

So just a small subset of protocols that are [Inaudible] Whatever it is that the ecosystem of governance decides they'd like to cover, they get to governance.

Right.

So, I know.

I know.

Because, because, because, I can point to a specific example.

I can point to the life system of this framework.

And it is multiple documents, multiple pages long, I don't specify quite a bit of stuff, but I don't specify things like what type of wallet you have.

So if you gave an example of a full-time wallet, they don't constrain it.

But they do constrain the issuance process, the NIL level two plus for IDP authentication, And there's also, I get the assurance, and they specify quite a bit of things.

But they say, is that the people to decide how they manage their wallets and get something to have the wallets and how they do it in the database.

Because it means that there's enough flexibility in terms of the application, but they don't want to.

Which means that some people can do that.

- Well, many people do it differently.

- Yes.

- Doesn't really-- Right, right, right.

[INAUDIBLE] Yes, so there would be an opportunity for people to say we want to add to our [INAUDIBLE]
[INAUDIBLE] [INAUDIBLE] Sorry.

I have a neurotic here in the world, and one of the ways I'm a neurotic here, I believe I'm standardizing the absolute minimum set of things that I get here.

And that means it's OK if two people can't talk directly to each other, because then there's a business of somebody who can do the translation of the word.

So I'm trying to minimize the number of oral creams we have for the pre-eminent.

And it's a very small set.

So especially for admissions, or I don't think it works like this.

That can be a really small set for the creams where I'm going.

That's where I have to stabilize the hospital.

Basically, this is all that happens.

Basically, this is that.

It's a very, very mental system.

It goes away with the muscle.

But it does something in a way that makes it difficult to attack the muscle.

So, for example, speed up must be legal.

So, you can't have dynamically speed up and change out of the muscle.

[INAUDIBLE] So yeah, so I walked the board here, there's a huge global agreement, I don't want to stall it.

And I think that's a recipe for more animals.

[INAUDIBLE] Can you answer the question.

What did I DO? I pointed an NFT to a Verifiable Credential!!!

Session Convener: Mahesh Balan

Session Notes Taker(s):

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

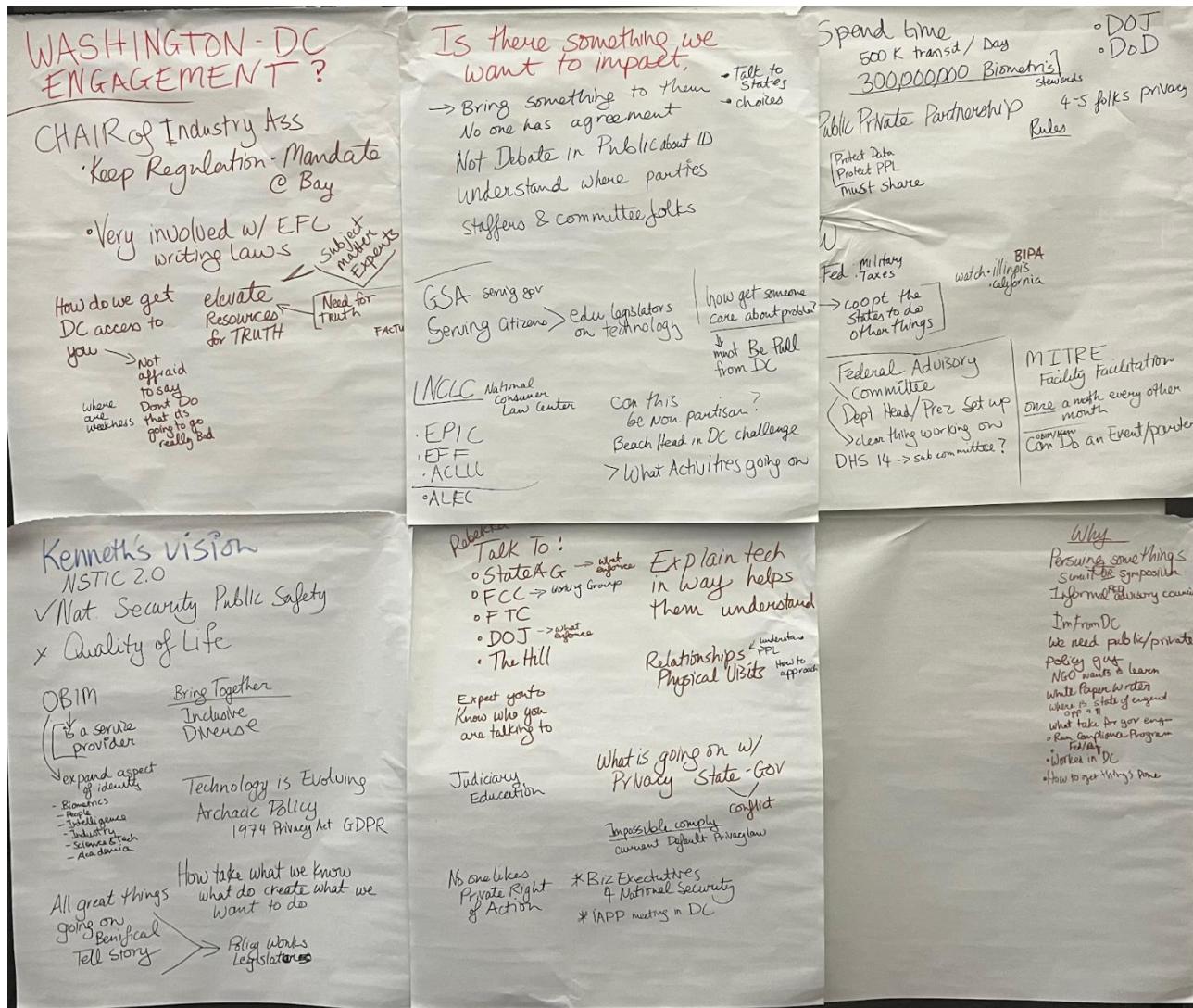
No Notes Submitted

Exploring how to engage more w/ Washington DC - What are hurdles to adoption?

Session Convener: Kaliya & Rebekah

Session Notes Taker(s): Kaliya sharing notes based on white board

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



Kaliya asked folks around the room why they came to the session.

- pursuing some things - summit or symposium
- Informal Federal Advisory Council
- I'm from DC
- We need public/private engagement
- Policy Guy
- NGO wants to learn
- White paper writer
- Where is state of engagement are their opportunities.

- *What take for government engagement*
- *Run Compliance Program Fed/Requirements*
- *Worked in DC*
- *How to get things done*

Washington DC Engagement?

Rebekah shared about one of her many roles - Chair of an Industry Association

- Keep Regulation Mandates at Bay
- Very involved with EFC writing laws
 - Subject matter experts are needed
 - Elevated Resources for truth

There is a deep need for Truth

Question put forward -

How do we get DC access? To you need to not be afraid to say don't to that it is going to be really bad

Sharing where weaknesses are in proposals

Rebekah outlined key people to talk to regarding identity

State Attorney Generals - considering what to enforce

FCC -> working group forming

FTC - regulates

DOJ -> what to enforce

The Hill - makes legislation

Another person highlighted another key group that could use attention/education the Judiciary.

Expect you to know what you are talking about

Explain the tech in a way that helps them understand

Relationships are key

Physical visits are also important

What is going on with Privacy and State Government.

There is a lot of potential for conflict between different laws in different states.

It is impossible to comply with the current default privacyLaw

California - CCPA

Illinois -BIPA

No one (amongst large companies) likes the private right of action.

Other key groups in DC

- Business Executives for National Security
- IAPP meetings in DC

Kenneth shared some of his vision

Looking towards doing an NSTIC 2.0

The national security mission of DHS/OBIM is going really well.

- 500k people transit boarders every day
- we store 300 million biometrics - stewards for this data.

- we have 4-5 folks just focused on privacy to deal with all the rules.

Mandate to protect the data, protect the people and when required we also share data.

How can the resources leveraged for Quality of Life

Bring Together - Inclusive and Diverse perspectives

Technology is Evolving

Archaic Policy 1974 Privacy act and GDPR

How take what we know, how do we create what we want to do?

All great things going on - we must tell beneficial stories -> Policy Wonks & Legislators

OBIM is a service provider

expand aspect of identity

- biometrics
- people
- intelligence
- industry
- science & technology
- Academia

There was a discussion in the session about the 10th amendment and how the federal government does the military and taxation but the states do everything else and anything else they want to do the federal government has to coopt the states into doing.

There are bills at the state level on privacy in California and another bill BIPA in Illinois focused on written consent for collecting/using biometrics.

Federal Advisory Committees are something that only the head of a department or the president can set up.

They must have a clear thing they are working on.

DHS has 14 committees right now - working on trying to get a subcommittee of one of these.

EVENT possibilities....

MITRE has Facility and Facilitation

Perhaps meeting once a month or every other month have some kind of event?

OBIM/Ken can do an event part...

There is also space/corner at Identity week America that Kenneth has reserved.

Kaliya offered to be part of helping with an event(s)

Big Question

Is there something we want to impact

- bring something to them
- no one has agreement
- Not debate in public about ID to understand where the parties are and where staffer and committee folks

GSA - severing government
[who is] Serving Citizens -> educate legislators on technology

How to get someone to care about the problem?

- must be a pull from DC

Can this be non-partisan?

Beachhead in DC challenge

> What activities are going on

Key to have engagement with the civil society sector.

NCLC - National Consumer Law Center

Key Civil Society Groups to engage

EPIC

EFF

ACLU

We took down e-mails of folks who wanted to be more engaged with how the identity community gathered around IIW engages more in DC. If you want to be a part of this conversation please contact Kaliya directly
Kaliya@identitywoman.net

Session #14

The Great Migration: DiDs and VCs are perfected! The face a world full of Active Directory. How Do We Make it Easy to Switch?

Session Convener: Josh Green - Cisco/Duo Security
Session Notes Taker(s): Josh Green

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

The core reason for the session was to have an open discussion to what appears to be a legitimate potential barrier to enterprise adoption of SSI: The need for a coherent migration path.

Many enterprise organisations have 10s, even 100s of Active Directory deployments, often acquired over years of acquisitions. In many cases, the complexity of the nested groupings of access rights reaches a level where even the IT administrators do not know the purpose and necessity of some of the groups, and are afraid to tamper with them for fear of interrupting critical processes or infrastructure.

As such, in the enterprise space, no DiD/SSI solution is likely to gain traction if it cannot address the challenges of migrating from these types of environments.

Thus, the question was posed: What should this middleware be responsible for doing? How might it do it?

We discussed a scenario where an employee is promoted from manager to director. What needs to happen?

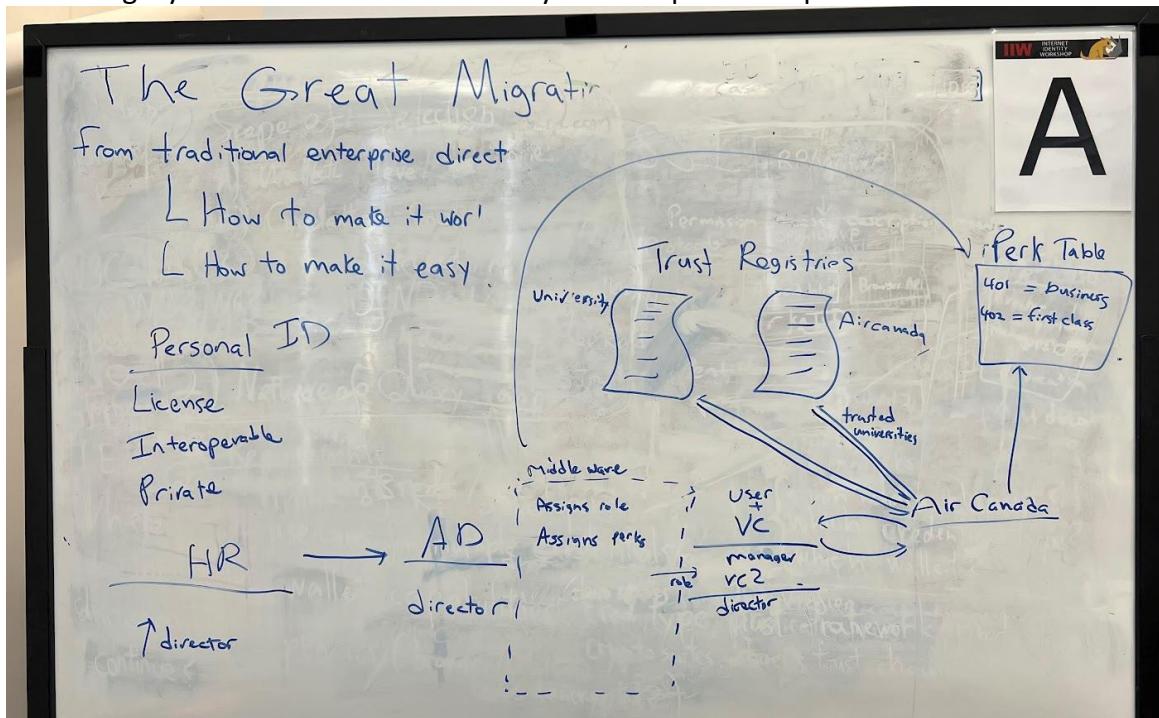
The group agreed that a number of things would be necessary:

1. The middleware would have to consume AD job titles and add those to issued verifiable credentials.
2. Depending on where entitlements get stored, we may need to take a variety of actions:
 1. We could simply have applications make LDAP requests to retrieve group memberships and use those for authZ.
 2. Instead, the middleware could scan AD and create a mapping table for groups to claims that need to be included in VCs or trust registries. (Depending on where entitlement mappings are going to be stored)
 3. Depending on where claims live, the middleware will then either need to have the ability to add to the organisation's trust registry in accordance to what group memberships the user would be granted in AD. OR, it will need to either revoke or issue a new VC to the user that reflects their new access. (Issue an additional

credential if the new role results only in additional access. Revoke, if any access needs to be removed.)

3. We also discussed a scenario such as a job role granting an employee external entitlements/perks like the ability to fly in business class as a director. The hypothesized that there might need to be an external table mapping such perks from the value that an airline might understand to entitlements that exist within the organization. The translated value might also need to be added as a claim to the employees VC. (Or perhaps this could be handled as part of an SD-JWT or a verifiable presentation, etc)

As can be seen, a lot of possibilities were discussed, and we didn't necessarily decide on how it SHOULD be done, but the group did unanimously agree that the ability to interact with AD and other "legacy" user data stores will be key to widespread adoption.



Verifiable Credential rendering method or VC 'render Method' vc rendering a display

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

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

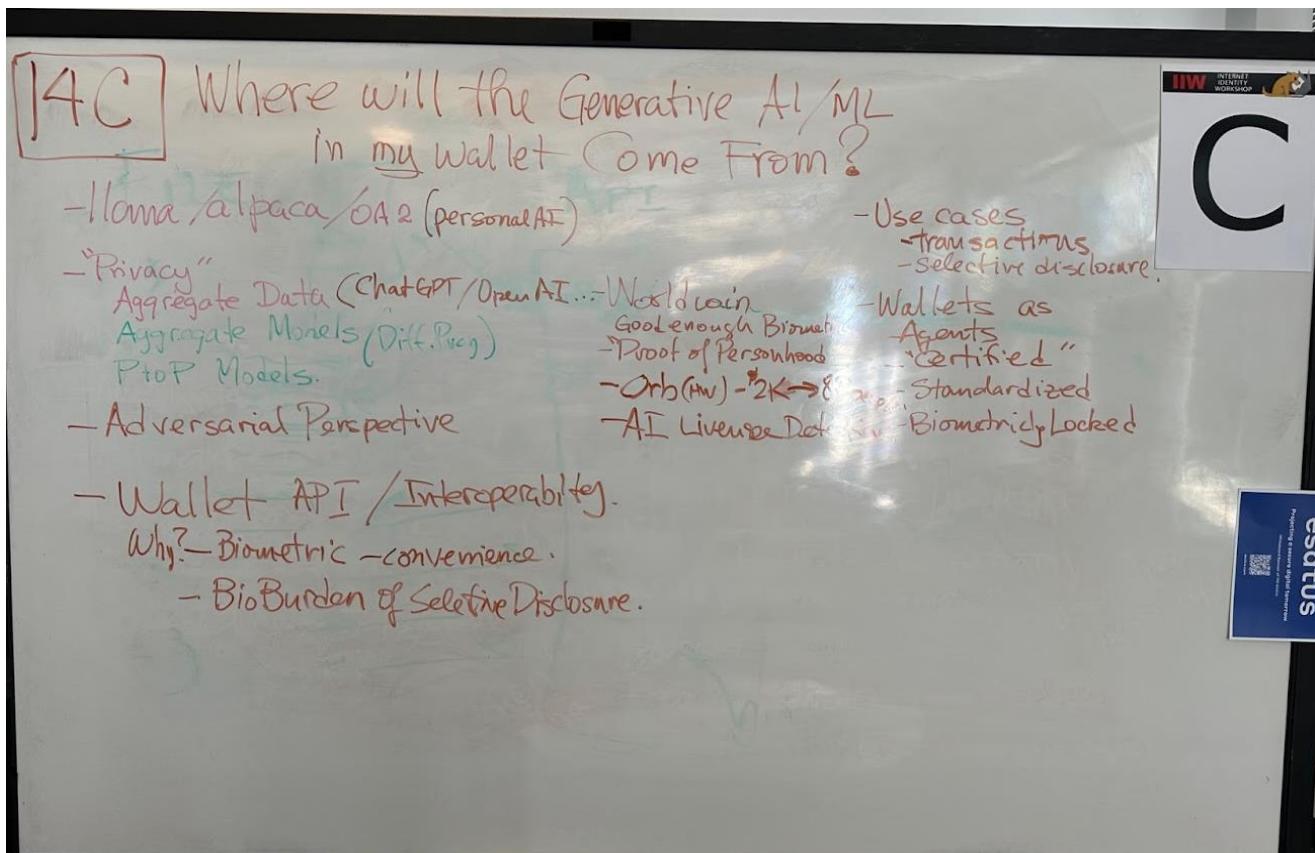
No Notes Submitted

Where will the Generative AI/ML in my Wallet Come From?

Session Convener: Adrian Gropper

Session Notes Taker(s): Adrian Gropper

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



OWF Project Ideas

Session Convener: Torsten L

Session Notes Taker(s): Jin Wen / transcription of recording

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

Medix: Jorge F

no code/low code wallet development, react native for android, iOS

- offline first
- security first

Sam Curran:

Transcript Only - no notes:

[Inaudible] Sorry, sorry.

Okay.

And what kind of, what is that.

Is that a wet toilet or is that still a curiosity.

It's a reality, it's a native act.

Oh, it's a native act.

You were basically combining the rich form index and what.

That's correct.

Yes, that's correct.

So, what is the back end.

There is a back end.

Because the way it works in index is it needs to, that the map needs to come to the server to provision the metadata.

So it's not standalone, but Mendex provides a framework for securing first and conflating first, which is very important for our user base, because farm workers live in remote areas and there's poor connectivity.

[Inaudible] Because we have made it.

Because we have made it.

We can put any Android device in the iPhone device.

[Inaudible] We find that a lot of our users have smartphones that are Android 9, iPhone 6's or older devices that if you build modern have to do web apps on the browser.

It may not work in my problems.

But we have native works a lot more reliable.

Can you address some of our own websites, some stuff that's been fed into the space of your world that's about football and it's going to get your local system.

DICOM and connection implications.

All areas, please.

Okay.

I guess the need to use areas.

To date, currently.

But I know that there's other financial formats like OpenIT, OpenConnect, or VCs.

So we can build the back end of Java.

And it also has support for JavaScript so we can build support for other platforms.

That's why I like the concept of the wallet engine because it's not one thing.

It can support absolutely everything.

So it's kind of aggressive right now.

Yeah, I'm not positive.

the RSRM on JavaScript, perhaps you know that better, but that has some VCI client as far as I know.

It has implementations for parts of my E4VC, RSRM on JavaScript, the one that you are using.

- Yes.

- So it's not only the classical different world and it also supports, or at least it's on the robot to support other friendship apps.

It would be more than, it would only be spoken.

- And I heard the MD update from the lady that did the MD update.

they're looking at extending indeed to support overlays capture architecture yep did you go to my presentation.

no I missed it.

overlays capture architecture I missed it.

aww man that's like a presentation yes it's like a presentation yes the visual display no, the visual display yeah yeah don't use the word presentation (audience member speaking off microphone) Okay, thanks a lot guys.

Anyone else.

Do you want to bring something to the table.

I don't know.

I don't know what it would mean.

So obviously, we do everything-- the BCGov wallet is just the same as yours.

It's bi-fold, 80% bi-fold.

But it's a whole wallet.

Your definition of wallet is different from our definition.

So our definition of a wallet is the thing, this thing.

It's not the storage necessarily includes storage.

But anyway, how do you say that.

Your definition.

And you said-- The back end-- the back end, the storage component.

Engine.

No display.

No display.

I will not think about it.

OK.

That's not what I interpreted Daniel's-- No, I-- Isn't that OK.

I think the term "water" is the same.

But the idea is that the OWF doesn't-- That's right.

That's what I mean.

--have this one wallet.

So let me get that straight.

I'm going to invent that term.

OK.

And I'm not happy with it.

OK.

So what I'm looking for is, in the end, we need to-- I'm very pragmatic.

Although I'm a German, I'm very pragmatic.

[LAUGHTER] In the end, the OWF must solve a problem.

Right.

It's expensive to build a wallet.

So we are looking for components that reduce the pain I'm not looking for something that fits in the certain architecture.

I'm pragmatic and that experience is not to know when you need to start creating cells.

Again components are useful for developers.

And I always use the example of a certain patch of code implementation.

To me that sounds to me simple design because it doesn't know end state and G.

But that's fine because over time we will learn what it takes to control all those components.

right, this is an evolution.

The starting point is let's get solid for something in that sense, right.

And over time as a community hopefully we will learn, hopefully we can build more complex things.

Right, so let's call it for a moment, look at it.

- Yeah, okay.

I don't know, I mean, I don't know enough about what it would mean to switch.

So the obvious thing we've got, It all started in the work we do in the end.

We've separated Aries five years ago, separated non-cred last year.

So the components are there.

Aries is not a enterprise blockchain component.

So whether it fits in Hyperledger or not is open to question, but it's been there and Hyperledger is an outstanding organization.

So I don't know what it would mean to move it around, move it over to the US.

I don't even know if that makes sense.

Neither do I.

Exactly.

What's the current umbrella of the architecture.

Yeah.

But the developers can combine packages from the.

Yeah.

>> Perhaps an idea, like let's say you're planning to implement OCA in a generic fashion that could be integrated by different kinds of bullets for the U.

N.

rig, so on.

That might be good fit for it as a library component for O.

N.

F.

>> So that's now just a library component within, right now it's a React Native component inside ARIES Mobile React Native.

Probably will make it more generic so that others can use it in so far ways.

Yeah, that's a component.

[Inaudible] Yeah, I missed the presentation but I missed it too.

It's a web page.

I don't know if it's enough.

If you want to go there, I mean, we are implementing every day and everything is in the open and we're doing all open source, every line of code we write is open source except maybe are deployment scripts.

Oh sorry those are open source they're just not that useful to others although at times you do not publish your secrets.

You do not publish our secrets.

That is absolutely correct I was just thinking of this.

I mentioned I think there's the FPM.

Yes.

(audience member speaking off microphone) - Very big privilege.

- When we started using GitHub for projects, if you see that the very first project that used it, published, they encrypted a copy of the database of a bunch of public information from citizens and put it in GitHub.

- Oh my God.

[LAUGHTER] This is bad.

Anyway.

[INAUDIBLE] [Inaudible] [Inaudible] But I don't think you need to start from the top or bottom.

You're probably in a corner.

And then when they go to the open source components, they happen to be a remote foundation and are useful to build in the logical components [Inaudible] I want to get started.

I think honestly, I don't think I'm going to stop designing this.

Because there's only a problem doing this in general.

I'm just, I'm just, I just want to get started.

I want to get the first package into the warehouse and it's going to be any component.

And we don't care.

All that component is compatible with any other component.

Right.

So what I'm going to say is, to move on, I don't know what I'd like to say.

I've got to put a consultant there.

That's important.

I've got one more time.

So here's the question.

My problem with that approach is-- [INAUDIBLE] From a technical standpoint, I don't think there is something I don't think so.

[Inaudible] (muffled speaking) I mean, as a reference, as a framework as a reference, that's very helpful to say, hey, we're going to talk about potential fires, we're going to talk about the protocols and the ICU.

I agree.

And it could be in human policy relations, but then you need to be a designated president, right.

I'm not sure if we have the ability to do that in a immediate process.

It depends on whether or not the ICU is going to be part of the treaty on that.

[INAUDIBLE] [INAUDIBLE] I think the thing that makes most sense from my point of view or from my understanding would be to start with new components that are getting developed right now, basically, that are of interest to more than one implementation.

Like, OCA, I think, is a very good example.

We were thinking about an S and JWT implementation that also supports sign interfaces, like, can use HSM or whatever, right.

And I think these kind of library steps are the first steps that we have to think about.

[INAUDIBLE] Yeah, the TypeScript library, and then if you support for HSM.

So we are a bit on the-- [INAUDIBLE] Yes, that is something we could be discussing.

I can't guarantee yet, but that is one of the ideas we have.

OK.

One time.

[INAUDIBLE] I'm not a fan, but-- [LAUGH] [INAUDIBLE] Yeah, exactly.

[Inaudible] So most implementations right now are more like a prototype level and they require you to have a CFP software.

So for example the biggest documentation in JavaScript.

iscript requires a different keyline and that is basically a software key.

And like for us internally it was like this won't work especially for like business use cases, we need hardware as a product.

[INAUDIBLE] So for example, no, I'm not thinking right now.

I wrote one phone, I'm thinking, for example, a third one.

And then we could use, let's say, oh, we use a keyboard or whatever.

Or we use Hashi-Kop or whatever.

And you could do the same.

Like, if you have an interface for it, >> Okay.

>> So, I think that's a good question.

>> Okay.

>> So, I think that's a good question.

>> Okay.

>> So, I think that's a good question.

>> Okay.

>> So, I think that's a good question.

>> Okay.

>> So, I think that's a good question.

>> Okay.

>> So, I think that's a good question.

>> Okay.

>> So, I think that's a good question.

>> Okay.

>> So, I think that's a good question.

>> Okay.

>> So, I think that's a good question.

>> Okay.

>> So, I think that's a good question.

>> Okay.

>> So, I think that's a good question.

>> Okay.

>> So, I think that's a good question.

But the emotions.

Okay.

In the light.

As a word, as a man, I think they are already in contact.

Why is it coming.

Or is it going to the proposal of the project.

They go through the process and they are filling out the proposal right now.

Or they want to come to their existing board.

And.

[Inaudible] [Inaudible] I'm not ready to run a project there, but what I'm interested in is that kind of to say science in some cases.

I would love to build a cloud-based wallet.

I guess it would be at least a cloud-based wallet.

And from what I hear, it's connected use to web art to devise metrics in social extension to web art and art VRF to go random functions of time.

Do you think it would be web art that would be designed for the participants.

That way, it could possibly, I don't know if you'll stand the test of a peer review, but it could possibly, for an audit, possibly develop all the functionality in what types of web options and use on-device encryption mechanisms in the browser.

We'd love to sponsor them, at least, I think we were eventually interested in [Inaudible] [INAUDIBLE] figure that out.

But that way you can find it really weird at least HSM sitting in data centers.

[Inaudible] It's a way, you don't have a web log, and you put it in the same text, and the design is the best how you authenticate using web log.

Now, with PRS, you can get solved and do different things that will have its own internal.

So it comes back with a derived symmetric field that you can use in the browser.

So that way, you can encrypt stuff and put it back to the server, and it will be sitting on the server, but nobody can, only, so whenever you need it again, [Inaudible] that you could derive symmetric keys in the ground on the device that originate from your fiber key in this realm.

Would that give you multi-device capability.

So the task key, that's the thing.

You have to think about that.

Whether it's viable, whether the tasks live Ohio.

So we have many unknowns here.

But it's true since it is a huge web option, you get past key.

You can't avoid passing.

So essentially what you're doing is you're doing the last pass model, right.

You've got a blob in the cloud that nobody knows the key to.

You bring it down, you use it.

Every once in a while you sync back.

In theory, other devices that you have can use the same blob.

So it's all an iOS device, you know, you would actually get to retrieve that same dog and decrypt on another device.

That could be, you know, accessing your iPad and that would be bad, whatever.

So there are a lot of things, you know, but potentially you could build sort of a broader storage.

- You can build the storage that then becomes portable where you use it.

- And then what's really, it's an adoption That would be much easier if people had to install in specific orders.

Interesting.

Yeah.

Cool.

Sounds like it was an extension to the [INAUDIBLE] Yeah.

But PRF is a new thing.

It's not-- it's in this draft spec or something.

[INTERPOSING VOICES] It is available in-- not as far, I think.

[Inaudible] >> Thank you.

>> That's interesting.

[Inaudible] >> Is it the name or the module, this PRF.

>> It's an extensive webinar.

>> Okay.

>> It's on PRF.

>> So it doesn't even function.

>> Yeah, because a PRF is just like a standard.

>> Yeah, exactly.

>> Yeah.

but they can stay safe from here.

- Okay, got it.

(man speaking in foreign language) I think I haven't seen it.

Are people here interested in MPC.

Are people here interested in MPC style wallets.

Multi-party competition.

(mumbling) So is that for like organizational.

(mumbling) [Inaudible] >> Yeah.

So you're sharding the keys and then-- >> Yeah.

And like one thing that you could do with SMBZ, for example, for the space is to-- you have like a very fine, that never like export information.

Basically, you can say you have something that verifies the credential, but the credential is never fully in place somewhere because it's a multi-party competition.

And from the system you get this, yes it's true.

I don't know what the main is, but I think from an identity perspective, one of the immediate use cases would be privacy preserving the refers.

for us.

We can guarantee that the extent of information is not expectable as long as one party of the amount of computation is not corrupted.

Is that what you're going to do.

I mean, you're going to do something awesome.

(laughs) I would like to reply to all this at the very point.

I think I'd better speculate.

I had so long time to go there.

I'm lost in action.

- Yeah, I'm actually interested in that type of OpenID type of wallet that could hold a generic identity information.

For example, a user trying to open an account in a bank, they need to verify their identity.

So you could do the driver license, or you could do their maybe passport.

And we try to find a way, is there a way to hold that information in the user's wallet.

So that later on, it doesn't depend on Apple wallet, it doesn't depend on Google, Android wallet, whatever.

but that's kind of standalone that could be in store either way.

And that the person, so they're using the open ID, open ID, uh, all the, uh, claim, matchable and potentially if that could be done on the identity assurance being done, that could capture the information inside for

the, for example, the ID, ID, identity assurance spec, we have, you have a layout of all this result of identity assurance during the KYC.

Can you-- (audience member speaking off microphone) Yeah, can you capture that one in the water so you can be showing, hey, I did that KYC on such bank or such organization, then if you trust that type of KYC, you can take this.

(audience member speaking off microphone) (audience member speaking off microphone) I don't know yet, so I'm just presenting an idea.

(audience member speaking off microphone) Okay.

Yes.

(audience member speaking off microphone) (audience laughing) (audience member speaking off microphone) - Absolutely, I mean if you want to do the bullet, you can make sure you're doing it.

- And they're asking, they're not there, nobody's done, that project hasn't been done.

- There are projects out there.

And some of them are open source, but some of them are on the open documents.

Microsoft is operating on the top of something.

And they're all, I mean we have an interesting thing.

Some of the libraries, and the tricky board is which platform to create.

And there is need, and I would like to gather people.

That's the reason why Android left the room.

It's almost already committed to the need of a more confident that they provide development resources for the project.

Okay.

Because they seem to need to build that, but they do not want to build the mobile again themselves.

They don't want to download it in the process.

So they would be providing development, the best people in that project, the development of the project.

And that would be.

Is it an interaction.

[INAUDIBLE] Is that an interaction.

Is that a protocol.

Oh, that one's a bad one.

[INAUDIBLE] Would you like to check it.

I don't know.

I'll know that that's more than I can assume.

[INAUDIBLE] Yeah, we'd like to check it.

We'd like to check it.

But we're not going to share the data that we're driving.

That's not about the discourse.

We're not driving.

It's about willingness interest.

You need a willingness to come here.

Yeah.

That's what I told them.

I appreciate it.

A general idea, but we won't be able to do that.

But that is something I do believe would be insanely valuable for the open-ended, for the people.

It's a key part.

I know that very fast, but.

One thing I do believe that would be very valuable, but I couldn't convince people internally yet, yet would be key clock extension for relying party.

Because like so many companies or enterprises are using key clock for like the lock-in processes.

Like that is one of the big multipliers in my opinion.

These kind of integrations.

OID for VP.

And like one of the-- - As a Veri-SAR.

- Yes, relying party.

I'm not sure what the reference implementation is going to be.

I guess no one knows from the European Union.

But I do believe that would be something that allows a lot of adoption, like fast testing.

No one knows what the implementation will look like.

According to what I have in mind, it's interesting, where it's not reference to or what it's for.

It's a fun thing to do.

It was me then.

I see fast and so nobody really know what the first implementation of the reference for the application will look like.

Most likely it will be ISO.

And I think it will be great if we as a community could also help.

So is that similar to what we've the VCR fan.

You know about that, right.

We've been using that for years.

Yes, but in this case you could do it basically without an intermediate.

can do a quick kick off extension.

That would actually-- So straight to the relying party.

From the wallet to the relying party.

So the kick off would be the verifier.

But that's what we're doing today.

It's just we have an extra component in there.

Yes, I can find it in between, right.

Yeah.

Yeah, exactly.

This would be without.

Yeah, exactly.

OK.

OK.

Can we have the same proof, opening for the peak.

Yes.

Yes.

[INAUDIBLE] Yeah, I was just saying, we've had key club integration in using back-up.

And I do believe that was one of the best demos we could have done because most people I talked with that looked into DITCOM and Occupy, they started with the key club then.

Yeah.

Okay.

What are these interests.

Should we start talking about the special interest group.

Do you want to ask a question.

I think this is a project that we go into the process.

Yeah.

And you guys have prepared that.

I think those ideas have been intended for.

And nobody can do that in much detail.

Is there still a really long poll.

Around the world.

Though we have those goals from your very good foundation.

But there is no longer such a goal.

- There's still an architecture call.

So people are welcome to talk about these things in that call.

But if you want to have a call or a series of calls focused on, well particularly a series of calls, both on something more specific.

And Mike and Kim said, I got a working group of task crews.

So if people are interested in that, that's a very likely thing you can say, let's have a task or a force to build one of these.

To look at building one of these, right.

You have meetings for a few months, and then you can say, well, we figured out where these resources and those codes come from.

Or this was an interesting idea with people.

Something like that, right.

If there's enough interest, it's probably I'm a little good to keep your conversation going.

As I said, I would like to start off with this.

Yeah.

Okay.

Well, the ideas, commitments.

Yes, thank you.

I think therapy.

I just wanted to get that one.

I'll just say, I know this is all the technologies for open wallet.

If in your organization, and they know a lot of problems with the wallet, a lot of the wallet expertise, is in very small organizations or in standards groups, etc.

, so they don't have it, If you are connected to groups that have actual user experience teams that can work on the actual interaction patterns, not that user interface, we know people are going to brand into their own interface, etc.

, but so that we can start to develop common interaction patterns across wallets, because that's where it's gonna hit the end user.

I've been trying to preach this for six months now.

We need to have that.

So we have spun up a task force in Trust Over IP for looking at wallet interfaces or the interaction patterns task force, but I said focus on wallets for now.

And it's like three practitioners that are in that area And we really need the people with that type of expertise that are used to doing your awards and how to discuss that so that they can be helpful to the people coding the wallet.

Okay, this is how we want it to be.

So if you have those expertise, send them to us and it's usually a different department than the coding department.

But if you can talk to them across the organization and say, hey, we get some resources on this business is coming.

- We should chat because we've had a group doing that across five organizations for a year.

- And when you say we, 'cause I know you have a lot of-- - UCgov, Ontario, Quebec, and some other companies around you.

- I'm talking to you.

- So yeah, it's about 10 people.

- But you guys just, what I always get back is they're too busy working on their stuff, so yeah.

- Yeah, it's in the context of it, but they've done service design, they've done surveys, they've done all sorts of things like that.

I have to tell you, as a newbie, downloading your wallet, what I downloaded it for last August, just to start experiencing them, yours was the most user friendly, and the tutorials you have with it were the best of it.

- That's the UX group in the interaction pattern.

- Let's get them working with that.

- Maybe that is a way to get involved, I don't know.

That's the type of group you want to have, maybe.

or just over at the UNB

[INAUDIBLE] Yeah.

Yeah, I've been interested in getting even broader engagement from more communities.

[INAUDIBLE] Let's see.

[INAUDIBLE] [Inaudible] You'll see.

Web 15.2: Shiny Toy or Pit of Despair

Session Convener: Justin Richer | John Wunderlich
Session Notes Taker(s):

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

- Do your due diligence
- Ask questions
- Listen more than talk
- Offer to help

Rule 1: We will mention no names - only stereotypes/archetypes

Red Flags

- This is the nth attempt at a project that has previously failed
- This project is special without being able to express specifically how this is special
- Silver Bullet Syndrome
- Unearned deference to leadership
- If you can't imagine three real people faced with the problem
- The high paid visionary that dictates their ideas
- Problem can't be expressed in lay language
- If there isn't a clear reason for your expertise
- Always having an answer
- Inflexibility at ideation
- The need to be right
- The need to be agree with
- Team structure doesn't match power structure

Caution Flags

- Not having done the research in the space
- Not willing to learn from what already exists (dismissed existing solutions)
- Lack of initial scoping or failure to recognize scope creep
- If the problem is not recognizable
- Not willing to explore multiple paths
- "Walking in the room and recognize that you are the smartest person in the room"
- Why is someone bringing up the same issue over and over again? (Why is the wheel still squeaking)
- When the project leader doesn't agree with the project charter
- Inappropriate metrics
- hush money (NDA proliferation)

Green Flags

- Being in love with the problem not the solution
- A fascination with the customer's journey

- An understanding of how the problem is solved
- Is there a clear vision (visionary)
- Clear statement of constraints
- Independently multiple people have come up with the same idea
- Opportunities for growth/learning
- Opportunity to contribute expertise
- Do the various personalities conflict productively?
- Empowering talented marginalized individuals

Yo-ID A reusable IDV network, as simple as possible

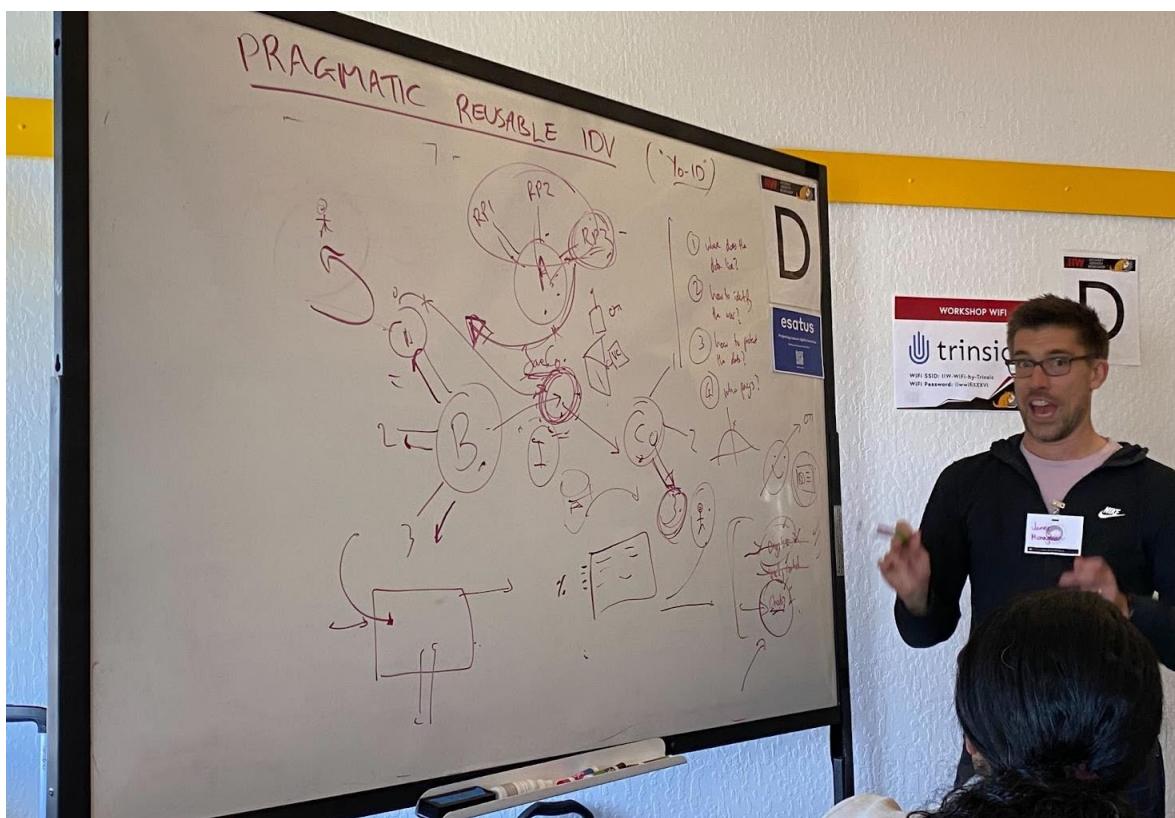
Session Convener: James Monaghan

Session Notes Taker(s):

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

IDv, identity verification, business model

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



Type You Notes Here – No notes

Principled Peacemakers ~ A Real Identity Demo

Session Convener: Johnny Bry
Session Notes Taker(s):

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

No Notes Submitted

PERCEPTIONS - Let's talk about those related to identity...But more importantly, what is the Gov't doing with my biometric data? (Inquiring minds want to know)

Session Convener: Kenneth Gantt the ID Guy
Session Notes Taker(s):

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

No Notes Submitted

Did:eth + did:ens Update and Call To Action

Session Convener: Nick Reynolds
Session Notes Taker(s):

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

No Notes Submitted

SESSION #15

SPAC #3 = Secure Privacy Authenticity Confidentiality - Tradespace Strongest A+C+P

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

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

Sam Smith's SPAC whitepaper

https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/SPAC_Message.md

Slides from Presentations:

https://github.com/SmithSamuelM/Papers/blob/master/presentations/SPAC_Overview.web.pdf

What AI will never do or be

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

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

Doc's presentation:

<https://docs.google.com/presentation/d/1QUE4qiZ6lbqw-yCprJWKqxth1vBDawxW/edit?usp=sharing&ouid=118022380936577102587&rtpof=true&sd=true>

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

- Understanding Media: The Extensions of Man (by Marshall McLuhan)

"We shape our tools, and then our tools shape us" - that's the spot we're in right now with AI - that quote, AI thinks it's from McLuhan, but it actually comes from Father John Culkin, SJ. Attributed to McLuhan bc it was in his book. "Supposition all the way down"

AI trained on crap will regurgitate crap

- "Every new medium works us over completely" (From "The Medium is The Message")
- Every media is technology, so how does tech work us over?

- "Laws of Media: The New Science" Tetrad of Media Effects

On the subway - everyone is plugged into a rectangle. Everyone was worked over by that.

Enhances conversation, reverses isolation (not present), retrieves agency, obsolesces mass media

Every new medium creates an environment

Digital tech + the internet

Enhances you name it, retrieves everything that can be digitized, obsolesces print/tv/radio/telephony, reverses cyber crime, surveillance, you name it

"Digital tech is the biggest thing since oxygenation" - Joi Ito

AI enhances everything you can do it can do better, retrieves every human and machine experience, obsolesces all that shit that you and your tools used to do, reverses "oh well, just ask the damn machine"

Michael Polanyi - Almost completely quote-proof. But: "We know more than we can tell."

Know > Tell

Tacit > != Explicit

And then we talked

Bridging Protocols

Session Convener: charles lehner

Session Notes Taker(s): golda velez

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

(asked what interests are in this area, people answered:)

blockchain protocols

metamask, uniswap

social protocols; noster/twitter/fediverse0

matrix, signal

ssb, farcaster, activitypub

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

attendees;

- nonbrand names

- not having to care which protocol it is - just who i want to talk to

blockchain - tends to be a security failure

speaker:

2 different categories: financial protocols, chat messages

attendee: in keri for dummies, protocols vs platforms - platforms grown independently, needs to be a protocol that connects them together - bridge should be just invisible

incentive for building bridges is different from financial to social

defi: has incentive to pull bitcoin in

social: want to keep people in

some platforms tried to have 1-way bridges

but paypal succeeded more by not having them trapped

compatibility can be a competitive advantage

knowing not locked in

gmail could do that because SMTP is an open protocol

most of things people actually use socially are not open protocols

challenges;

standards of display

threading

security (ban on one side of the bridge - no on other side)

awareness

could there be a network map of all the bridges

bridges rot

natural bridges?

are there natural mapping

IIW kikochat coins - most people weren't aware of them!

with verifiable credentials why can't our social graph be vcs we own?

maybe could bridge each one into vc ecosystem hub and spoke

for the

johannes: its not a technical problem, its an incentive problem

someone wants to monetize the network

fediverse is like email in that no one owns it

free uncontrolled network can enable other kinds of businesses like paid fediverse clients
that cannot happen in a closed network

if people build a new thing, they generally want to monetize it

if people want to build on an existing thing, usually they want to grow it

bridging out from twitter - trustless bridge is hard, but trusted bridge is possible
can rely on

g: fundamental problem between algorithmic discovery vs centralized anti spam
j: decentralized reputation if it can work we can keep out the spam

would you want your bridge to also be algorithm/spamfilter
or maybe the bridge needs to carry reputation but not filter

the larger the network the more information we're likely to have

the smaller the network the more likely someone comes with no reputation
independent reputation service

human level - informal mechanisms with small scale

what is current state of bridging?

there are apps you can connect all your social accounts

indieweb - posse - syndicate from your personal website

post out and pull responses in

used to work better 10 years ago - but now the apis are closing down -

old app used to be imo - xmpp - was difficult for them to keep up with incentives

but creates opportunity - clearly people want the ability to talk to all

fediverse is rich data

bridgy - it makes it easy to publish to all social networks bidirectionally

bridgyfed

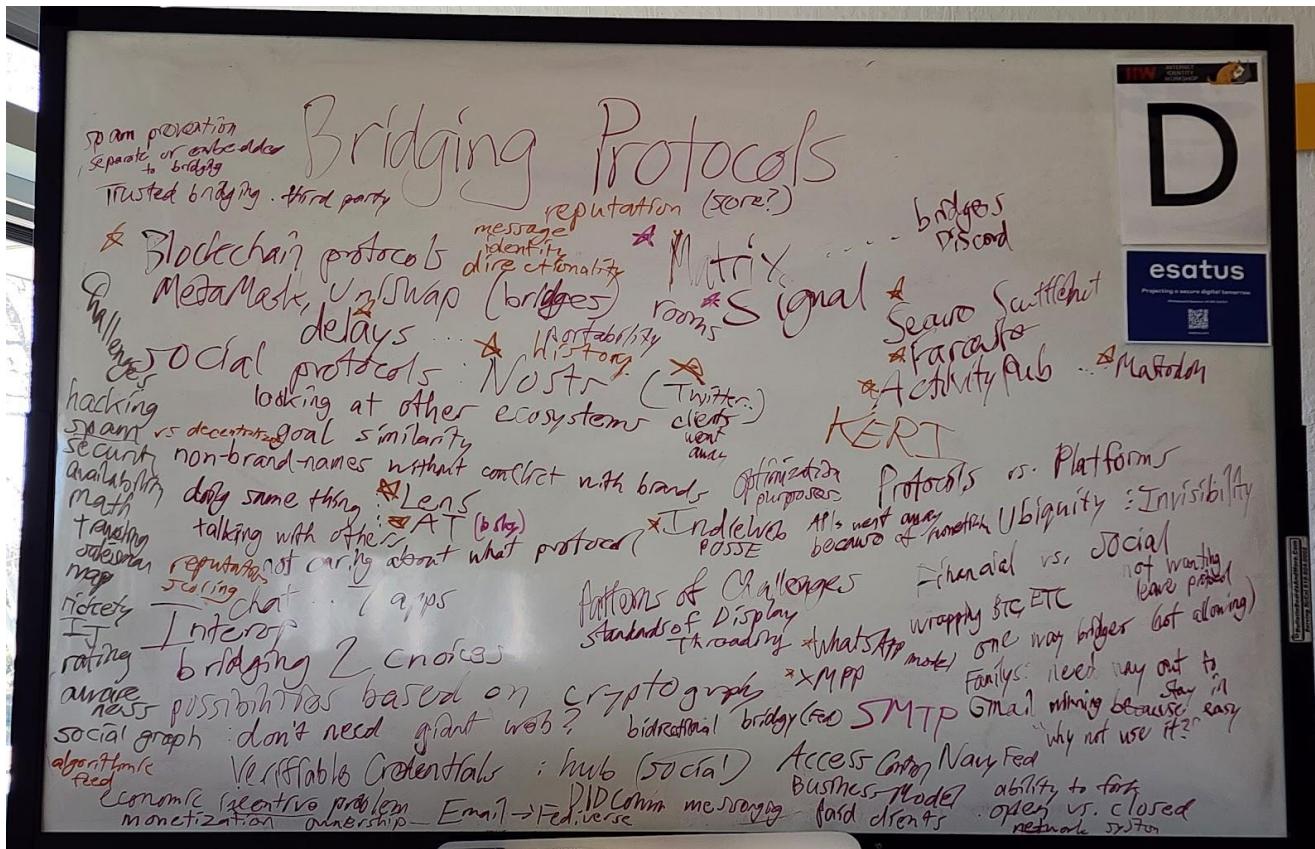
matrix bridging is pretty good

bridges to irc, slack

no signatures

matrix <--> activitypub

Hi i'm Charley from Long Island and organizing meetups
and writing a test suite for vc2



Browser APIs and Intent Handlers (for wallets)

Session Convener: with Adam (Adain?)

Session Notes Taker(s):

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

No Notes Submitted

Digital ID/SSI Researchers/Scholars masters/PHD Student Network? What do we do to start/support this? How do we create annotated Bibliography?

Session Convener: Kaliya Young

Session Notes Taker(s): Kaliya

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

A few people came to the session.

We had a good sharing of resources.

How can all the identity scholars globally be seen and connected?

They are in radically different disciplines, political economy, political science, sociology, anthropology, international development, women's studies, computer science, history etc.

Could identifying and connecting these people be funded by funders keen on identity?

There are academic fields for cybersecurity and privacy - not so for identity / digital identity.

One of the people who came to the sessions did so because they, as an implementer, have key questions they don't have the resources/capacities to answer. They want to know what academics they could approach to help with research.

Kaliya has been working on a bibliography about digital identity that she can share with the PhD and masters students that she advises.

Trev Harman from ID2020 shared a bibliography of white papers and reports he has been collecting - links to those have been shared with Kaliya and will be integrated into the bibliography.

If you are reading this and want to see/access the bibliography please be in direct touch with Kaliya@identitywoman.net. The reason for not directly publishing it is that it is not ready for wide circulation - getting the bibliography into professional shape good for sharing will be quite a bit of work.

One of the questions that was raised is where to find the resources to document the scholars and get the bibliography into good shape - if you have inspiration/capacity to fund the furtherance of the bibliography also be in touch.

What would it take to build a scholarly field? This is a big question but worth asking.

Calling All EDs - What Can We Do Together? / Jean Q and John

Session Convener: Jean F. Queralt

Session Notes Taker(s): Jean F. Queralt

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 session brought together a number of Executive Directors from the organizations participating in IIW36 in order to further synergies among them.

A collaborations would cover topics such as

- Identifying common challenges
- Identifying areas of support across organizations
- Finding funding opportunities
- Establishing methods of participation in relevant policy making fora

The main outcome of the session was the commitment to organize a regular call among EDs to keep exploring all of the agreed items.

Hyperledger Identity SIG Launch

Session Convener: Char Howland (Indicio) & Hart Montgomery (Hyperledger)

Session Notes Taker(s): Char Howland

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

Meeting page: <https://wiki.hyperledger.org/display/IWG/Identity+Implementers+WG+Call>

Recent meetings: <https://wiki.hyperledger.org/display/IWG/2023+Meetings>

Meetings are bi-weekly on Thursdays at 8am PT / 11am ET / 3pm UTC

- Check the [Hyperledger Calendar of Public Meetings](#) to find next meeting

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

- The Hyperledger Identity Implementers Working Group and Hyperledger Identity Working Group are joining to become the Hyperledger Identity Special Interest Group (SIG)
 - Vipin Bharathan has chaired the Hyperledger Identity Working Group
 - Char Howland and Tim Spring have co-chaired the Hyperledger Identity Implementers Working Group

- Vipin, Tim, and Char will co-chair the Hyperledger Identity SIG

In this group we track progress updates from working groups in Hyperledger, ToIP, DIF, W3C, etc. and invite speakers to give presentations and demos on relevant topics. This group provides a roundup of community news, a high level overview of work happening in working groups, and an entrypoint for newcomers.

Goals of the SIG

- Consolidate and expand the existing Identity Implementers / Identity WG communities to drive more coordination, communication and collaboration across Identity projects at Hyperledger
- Collaborate across Hyperledger Identity projects as well as collaborate with other SIGs where Identity is important (e.g. Financial Markets SIG, Healthcare SIG)
- Lead outreach to LF Identity communities (TOIP, DIF, OWF, etc.)
- Bring in outside voices (startups, orgs, govts, corps, individuals) to discuss important topics and demo new work in the decentralized identity space
- This SIG will act as ambassadors to the identity community outside of the Linux Foundation, building bridges with outside organizations, efforts, projects, companies, individuals, etc.
- Create a forum for Members to engage the “Identity Conversation” within Hyperledger, sharing stories of successes, failures, opportunities, and challenges

GLOBAL Assured Identity Network (GAIN) Update - VCs interop profile - Interoperability /Network or Network

Session Convener: Gail H, Elizabeth G, Dima P, Mark H, Torsten, Dima
Session Notes Taker(s): Jin Wen

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

<https://openid.net/gainpoc/>

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

Connection to: Mobile Ecosystem Forum

Demo: KDDI produce a GAIN a SIM demo on the airport to show how an international traveller could open a mobile subscriber account using the banking credentials acceptable

Next steps:

GAIN provide informative decision for participants to decide if they want to trust the



Transcript:

[Inaudible] [INAUDIBLE] regularly to drive this effort and to sort of focus moving quickly into the future.

And yeah, so now I'm going to start something other than I can do that.

That's done.

And I know that this is where we don't want to start the show.

I'm going to show you how to draw a picture of it.

It's connected.

Free, um, you know, it's just a map.

And it's going to make it a little bit neat.

And I feel that we all want to play the game today and we'll be testing some more.

So, actually, actually, Dimash, should we also just add in the first part as well.

(indistinct chatter) (indistinct chatter) (speaking in foreign language) [Inaudible] (inaudible) There have been quite a bit of work, more than it is, on connecting people to their own violence and trust, meaning that their relationship with your bank, your bank can launch a new one.

Usually they are on the banks because the banks have KVC requirements I have been experimenting with a German therapist for a long time.

I have been experimenting with the way I changed my technique to use global care.

I know it's not how do you get access to, how do you get someone to buy or to buy or ask to use.

You ask, "What am I going to do with this.

" And I need to inform myself that I have a question.

[Inaudible] [Inaudible] [Inaudible] (inaudible) [Inaudible] Wasn't there also a kind of principle that we wanted to make it as simple for the relying party as possible.

It was another important aspect.

[Inaudible] (muffled speaking) (muffled speaking) and then we start to do a test project.

The program that we use to define tools to make a connection or any kind of insurance.

So that's a day to change.

That was easy.

When you test it, it will work.

The next phase for us was how do we use that trust technology for difference.

And this road probably spent nine months trying to work out how to use the trust between the nine and one of the things is a kind of a, some principle that they're trying to pull.

It's who are trying to minimize the quality of the essential infrastructure.

We want to reward our own peace and focus, and we need peace for those that are not certain.

And they always have their focus system, how they are known, and what they're surprised about their goal.

And peace, how they've met their own, and so we wanted to rely on that.

Do you want to implement additional maintenance information.

Can we try to treat it as viable.

Can I just add one comment, Dima.

And the reason for that was because if we try and change the protocols, or define one single protocol that everybody has to use, then we're effectively enforcing change on every IDP and RP on the planet.

That's probably not going to happen.

Yeah.

I don't mind if I just open that IDP or how do we set it up, and if I do, we don't describe that at all.

So, we try and forget it.

We have those types of things existing without any protocol or any ability to do the right thing.

We will be able to put our IDP, [INAUDIBLE] (inaudible) [inaudible] This is where we will talk about how to wind bike and find out what I can use to get there.

And how that makes you wind bike, and how to get that bike.

Each of those things, they come in there.

[Inaudible] [Inaudible] [Inaudible] I've been experimenting with community work with the participants in the working group of the existing and the powerful companies because they are generally widespread.

38 different participation groups are in it.

Yes, that's organizations.

That means 30 organizations and growth.

And we've done a cool concept which really binds the test systems from patient-notes [Inaudible] And that federation, so they use the federation code, that they are all in the same protocol, and the speed is different than the support system.

Inside the circle.

So that's what I do.

We've got just a phone term.

[INAUDIBLE] [Inaudible] We had a day to change and we looked at the polls and made it by the police.

We had really good jobs and we would have been actually in the same position.

So all three of those networks are exchanging information at a close time.

And I'm finishing with a highlight.

Those are brought up organizations.

[Inaudible] And we have a demo which we will talk about in part.

Yeah.

[INAUDIBLE] The demo was, it actually did properly, but KDI, I think that they all did arrive at the Japanese airport, how the religion is seen on the spot, using the, with the old sister language.

So it's pretty simple, pretty impressive.

I'm just calling, I'll just, I just want to say, I think you said, "I land, but I'm not that one.

" Oh, yeah, I did.

I think they did victorallababy around there.

I would love to hear what is IronSA.

Bringing that up, á cameroon is around.

What does the Middle East do.

So I think foreign India [Inaudible] We share income infrastructure, we share identity, but we're not talking about the things about the individual.

- So now we're looking at programs where we're going to have to inject with the technical field.

- Yeah.

We sort of feel like that's going to be, now we're moving into how we can get our IPs, which might be a little bit more, but how can we get them to reach a very powerful potential.

(muffled speaking) - I'm quiet.

- One minute, 53 seconds.

I'd like to show some of this case that we.

It's not that you are just arrived at the point that you did the next operation with your smartphone, but your working plan might be expensive for a soul to remove the other component.

People might think that the same process is normal, but you have to stop trying to buy a city plan if you are not safe.

(inaudible) (muffled speaking) [Inaudible] So thank you, how about it.

[INAUDIBLE] [Inaudible] [Inaudible] [Inaudible] Did that answer your question, George.

[Inaudible] [inaudible] (inaudible) We're using it to identify the problem.

[INAUDIBLE] (muffled speaking) [Inaudible] [INAUDIBLE] [Inaudible] That's what we are saying.

And then what we wanted to talk about now is any question you might have about what we've done so far, including anything about the OAXA or speaking through your own policy framework now.

So then we could rather focus on how we think that's a greater viable dimension than just the pieces.

We've done a lot of work at the conference going on that can help us progress that.

And then it's also other approaches [Inaudible] Yeah, well, but just framework stuff.

Okay.

[Inaudible question] And that's under Charlotte Crespo, right.

[Inaudible question] Right.

I think you know more about it than I do.

[Inaudible question] So one of the other non-profits is the Open Identity Exchange and they are quite well connected into influencing some aspects of UK government.

I think that's probably our strongest relationship there.

Yeah, I'm a board member of OEX as well actually.

[Inaudible] [Inaudible] [Inaudible] Yeah.

We've made an assumption that the policy level trust is already established.

[Inaudible] So it's a bit of policy level stuff in OIX, but also how to map the different policy components from different jurisdictions to each other, or at least analysis of the gaps.

Yeah.

[inaudible] Yeah, so, yeah, so, you know, across one of these boundaries you might find, in this state, 63 on one side and GPG 45 on the other side.

So an RP in the UK wouldn't really recognise a NIST level of assurance and vice versa, right.

So that's one of the aspects of the thing we've got a working group in OIX called the Global Interoperability Working Group.

You're on that one, yeah.

- Yeah, it's doing.

- Yeah, cool.

- I want to work for when to see that.

(mumbles) [Inaudible] So at an island level, that needs to be done before the individual member organizations can interact with each other.

So it means that if the trust is not as tailored, then pretty much the screen you just showed earlier won't be able to.

It wouldn't work, yeah.

You wouldn't be able to pick your bank if you were in an island that hadn't been connected at both a policy level and a technical level.

[Inaudible] So the one problem that is the best in the end knows that, will know the result of the technical process, for example, this kind of effort, the Japanese effort.

People have a discovery mechanism to listen to the AI or get a list of the one-five that's available here or this type of piece of paper there.

So the protocol, existing protocol, is extended where you pull the existing file.

And then when the file talks to you, I have a way of authenticating.

So you know that indeed this is actually the one that I have with my AI-type system because of the use of prior applications in AI infrastructure.

So this is what we established here.

Marcus probably touched on it in a sense that you need that policy, but again, nothing stops in your video-like system, connecting to nothing in your video-like system, but the work is on the use of the method for AI-type.

Let's say if I want to connect (inaudible) And I can do the leg work and say that your level of assurance means you understand that, my level of assurance means what.

This is how I'm acting.

What we're trying to do is we're trying to simplify for a part of the network that you get to pursue.

You can connect now, but if there's a network policy, you don't use until that purpose comes in.

[Inaudible] Entities.

Entities.

Yeah.

Right.

Yeah.

(audience member speaking off microphone) (mumbling) the next question from them is, if we want to go to the last slide, we will do it.

So, the only way we could do it right now is probably with the server key and key F in connection.

In order to, and we haven't, like I said before, we try to minimize the possibility of a central entity.

We haven't actually decided if it will be a central or some sort of distributed trust list that distributed with the stereo system might have said, "I want to trust this one, These one might not hold the peace."

There's multiple layers to it, right.

So before we had ecosystems, everybody that came up here between each other.

And then we had these bubbles up here, or these islands of trust appear, where RPs and IDPs would trust that each other had signed up to a set of common policies, essentially.

And now what we're trying to look at is joining those islands of identity trust together and allowing for consistent communication between them in a much more dynamic fashion.

So we're getting away from even peer to peer at an island level, maybe.

And there's nothing to say anybody can't do all those peer to peer things in the future if they want to, but the benefit is I think a greater scalability for all of the existing entities and islands of trust.

(audience member speaking off microphone) So, if we took the Italian Federation, for example, that enables communication between IDPs and RPs within, between members of that Federation.

So they've established policies and contracts and all of the important documentary stuff that then underpins them being able to communicate with each other.

- Like a rule book.

- Yeah, a rule book, exactly.

And so what we're trying to do is to take that up to another level, effectively federate the federations.

- Can you explain this better on how (mumbles) - I hadn't.

So in the data plane protocol that we used as our first step, there's an attribute in there that defines which trust framework the identity of the individual was established within.

So effectively, that's a tag that's saying Mark was established through the ID Connect trust framework or you know a UK trust framework or whatever it is and then that allows the recipient of the data to understand which local rulebook my identity was established and presented under.

[inaudible] So I reflect on that, if you remember back to X509 certificate authorities, the certificate itself contains a link to the policy documentation.

This is kind of similar to that saying this blob of identity data was done in compliance with the policies described by that network.

[INAUDIBLE] And another important point of view about the issues is that in the alpha JSON, we have all participating as a randomizer in the PC world.

We have to do all the way there and as an IDG, they just use the same interface.

But we don't prescribe in this cycle.

I think it's a huge release in general for a whole bunch of things.

And that's why we're looking at a very powerful potential to be pulled right now.

[Inaudible] >> Yeah, it's important to point out that those are complementary efforts, right.

So the networks themselves can be directly connected like what we've been here for.

You can take the interface and be approached and then connect it in a wallet layer, a wallet to be worked with.

You can really get a control over how to solve the problems of how, and trust framework map and fill is a two-trust interest.

And we're not even trying to say that a wallet needs to necessarily exist within the rulebooks of a trust framework, although it's entirely possible they could.

So it allows for those kind of pre-floating wallets, or ones more like what is presented in the EUDI are a governed kind of controlled wallet implementation.

- Yeah, so you mentioned that obviously one design was not to add additional structure or protocols to any one island.

So in the mapping question, the mapping protocol, does that exist at the island level.

- And so I think one of the things that is likely to come out of the global inter-ability working group at OIX is a list of gaps that need to be filled in that space.

There is already clearly good evidence that the trust frameworks cannot readily be mapped.

So there's going to need to be some more work.

And what we're doing in OIX is not just identifying the gaps but trying to work out where we think the appropriate owner of that problem space.

So dice it up into several problems and suggest to certain organisations that it looks like it's within their normal business to attend to that problem space, whatever it is.

So I can't say too much more because we haven't finished yet.

One question, so in your POC and your three islands scenario, did, was there another, what was the agreement between the islands to use their existing protocols.

Was there an additional and explicit policy.

- Yeah, so I think when I said that, you know, if you're trying to move up to the point that you were using the pandemic, that actually is not there, but what you do today, (inaudible) [Inaudible] >> And then there was a green policy agreement to do that for you.

(inaudible) (inaudible) For which there is a new commercial, anything, it's free at all for the United States, but anyone else who wants to decide a participation period, and that's ensuring essential to the things.

A safe space, you know, to make sure that the eye care, you know, the eye care foundation is the new one to teach, and to make sure there's a safe space, and then a discussion, or whatever it comes about is shared politically, and to reduce our hours, and to ensure that there is an appropriate heat process within that community, right.

There's rules in how that group There was one other really important real deal which is no real PII because we didn't want to fall into any problems there.

[Inaudible] [INAUDIBLE] [INAUDIBLE] [Inaudible] There was something that sprang to mind there as well.

Another really interesting debate was around those perimeter components that are famous kindly highlighted in blue for us there.

We really didn't want to put proxies of any sort in there, certainly in the data protocol.

So from an architectural perspective there needs to be something there at a logical level but it doesn't have to be a separate proxy.

It could be an SDK bolted onto an existing, every existing entity in the network.

So that would be enabling them to participate by adding a small additional component that they manage themselves, resulting in no additional data processing and data processor.

- And an entity on a pilot could participate or not.

- Exactly.

[INAUDIBLE] [Inaudible] (muffled speaking) with each other, I think it is, so we're kind of providing kind of a facilitation.

So what we're deciding on as we're scaling this, that our team is gonna keep the PR, where are you gonna have something at higher level that's (mumbles) at higher level and a way to have that facility that's the interaction.

So there are some kind of common values we can have at the different levels and their own knowledge is the kind of a decentralized federated platform.

There's pros and cons.

And actually, you could also do both.

So and we thought about architectures where there is a component of kind of central reference.

And that could be implemented in a decentralized manner.

But it's also possible for the Islands of Trust to build their own peer-to-peer if they prefer not to use the shared resources, whatever that is.

(audience member speaking off microphone) We have to achieve this, so I get a lot of their trust in these companies.

That's one thing we'll let for later.

So what Mike is saying is that we're okay.

Option number one is you do create a central trust for them.

The central trust that everyone refers to.

Option number two is everyone has a coping event trusting them.

Eventually they can modify it.

Maintain themselves.

And the option is you build your own customers.

[INAUDIBLE] [Inaudible] [Inaudible] [Inaudible] Whatever is sitting at the top, yeah, whatever sits at the top becomes informative rather than authoritative.

[Inaudible] (muffled talking) (muffled talking) (inaudible) (inaudible) (inaudible) (inaudible) That' alot of work because Abedia said that.

It snowmed.

(inaudible) [Inaudible] [Inaudible] [Inaudible] [Inaudible] And vice versa.

[Inaudible] [INAUDIBLE] [Inaudible] (inaudible) [Inaudible] and on the policy decision part, as we went through the work on other parts, given that some of the people went to a technical standard to try to open the department of use at the end of the day, how we can have a fair application map for that kind of idea.

Fair technical development, and that's how people go for a new opinion.

I want to add another thing, and I'll mention that there are also a lot of people that are working for each ecosystem.

For these ecosystems they're not just like people stable, they're not just standing still, they're doing that by who are already joining our community, how do we get people to help me, if you're partner we have that kind of network, right, so what under each ecosystem is not wanting new networks, but how does the policy jacana is doing work, in the world, how would they automatically just update information into a department.

So that's absolutely an area we've been talking about and one of the features and areas we've been looking at and ID Federation is around more dynamic registration or kind of on demand.

And we came to the conclusion that mechanism worked quite well because we could definitely do regular periodic updates of the entities.

But actually, we also wanted to allow, for example, an IDP in Italy, to not have to maintain in its operational system all of the metadata of all of the possible relying parties across the network of networks.

So there was quite good conversation and some, I think, really good technical work on how you would do that in a just in time way.

And Federation does allow for some of that to happen through the hierarchy that exists.

defusing Federation.

So from a technical level there were some ways to do that.

Is that fair presentation.

[Inaudible] [Inaudible] - I'm going to jump in with a quick call to action.

I know in this group we are looking for keen implementers to come and do some real project concept work and in particular channeling Torsten.

We would like implementers who want to do some perfect concept work, particularly with verifiable credentials in this space.

So anybody out there who's interested in doing that, please let us know.

And the OIX pitch as well, we're working on global interoperability.

No, but I'm pretty sure, well I don't know if we've ever actually voiced that directly, but this one would be a good start I think.

Yes, that one is.

I need your attention, verifiable credential stuff.

So that'll be VC1.

(audience member speaking off microphone) - And as the opening gambit for BlockTBD as well.

(audience member speaking off microphone) I don't know if we've really written that down here.

(audience member speaking off microphone) [Inaudible] for Australia, they slept in the matter.

It's a gentleman named Tobias who's moving around here.

It's a part of the community for their public attention group.

So you can make it together.

The cool authors.

One of the cool authors in spec.

And also a member of the United States in the profession of working there.

It all comes together.

The Italian group that implemented her.

They are also doing her music.

They're doing her stuff.

They're trying to get other.

Notes in this book can also be found online at
https://iiw.idcommons.net/IIW_36_Session_Notes



Heidi Nobantu Saul 🐝蝶 @nobantu · Apr 19

...

A lively game of Cards Against Identit being played at the end of @idworkshop Day 2 ~ hilarious to sit on the sidelines listening!

#iiw #iiw36 #cardsagainstidentity



2

1

11

354



Speed Demo Hour / Wednesday April 19

Thank You to Our Sponsor

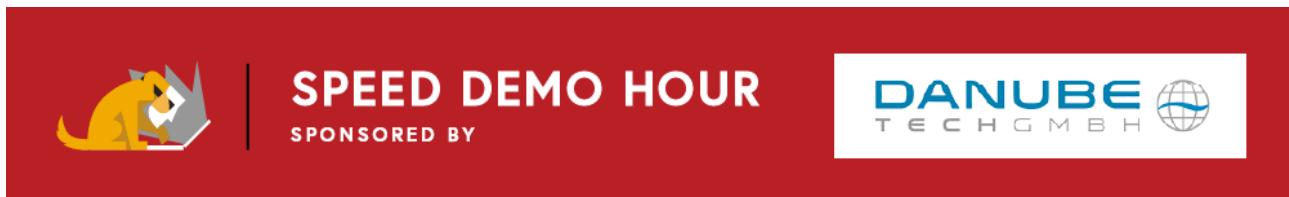


TABLE	Demo Description
#1	SitePassword: Alan Karp URL: https://github.com/alanhkarp/SitePassword/blob/main/README.md SitePassword is a self-sovereign, full-function password manager that calculates your passwords instead of storing them. It puts you in control of the metadata used to sync across machines while allowing you to get your passwords from any browser. And the best part is it's free.
#2	Clutch, demoing web3 Platform: Sheela Vats URL: app.clutchwallet.xyz Clutch is a web3 platform which provided account abstraction wallet (browser extension, Dapp and mobile) and Decentralized social network with privacy.
#3	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!
#4	Animo Solutions: Paradym: Timo Glastra URL: https://youtu.be/HYRevw1Dds Paradym is a low-code builder for SSI solutions. Users can create YAML-based workflows with triggers and actions to seamlessly integrate verifiable credentials into their specific use cases. Paradym makes SSI development accessible by handling all infrastructure and complexity.
#5	Infisign / The use of verifiable credentials for Passwordless login across applications using OpenID connect: Aditya Santhanam URL: https://www.infisign.io/ Infisign is an Identity and Access management ecosystem supporting Self Sovereign Identity, a Zero-knowledge proof-based passwordless ecosystem. It utilizes the best cryptographic techniques such as BBS+, and Ed25519 signatures coupled with OpenID connect to provide a quick, secure and the most efficient replacement to passwords. The organizations now have the ability to use Zero trust based authentications for SSO and also OS based authentications for the first time.
#6	2060.io DIDComm Chat: Ariel Gentile and Fabrice Rochette URL: https://2060.io 2060 is a set of open source tools that enable building rich decentralized chat services, combining text, pictures, video and voice notes with the power of Verifiable Credentials.
#7	Dock: Nick Lambert, Elina Cadouri, Mike Parkhill URL: https://dock.io/ Issue Verifiable Credentials in a few clicks or with one API call. Dock Certs is a no-code, easy-to-use platform for issuing and verifying VCs and creating Decentralized Identifiers, and an API to enable organizations to add SSI functionality into their applications
#8	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?

#9	Nextcloud Login with OpenID for Verifiable Credentials: Christian Bormann, Torsten Lodderstedt URL: https://openid.net/openid4vc/ & https://idunion.org/?lang=en We will show a complete flow from credential issuance into a native wallet to credential presentation for login into a Nextcloud instance. This demo was built in the IDUnion project (a project founded by the German ministry of Economic Affairs and Climate Action). Over time, we implemented the flow with different credential formats (AnonCreds, LDP/BBS, SD-JWTs). The latest revision uses Selective Disclosure JWTs with hardware based cryptographic holder binding.
#10	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.
#11	RootsID DIDComm v2 connect-a-thon: along with Atala Prism , Blocktrust , Veramo , Nessus , and more URL: https://rootsid.com Participants will demonstrate (https://hackmd.io/j6U6JpQ2SRexSUKL7i2XRg?view) several DIDComm v2 agents/services/mediators discovering, connecting, messaging, exchanging verifiable credentials and other trust tasks using open source software/standards including DIDComm v2 https://didcomm.org/
#12	esatus AG, SOWL including use case “access to Windows and other applications”: Dr. André Kudra, Azita Hosseini Nejad URL: https://esatus.com/index.html%3Fp=8009&lang=en.html Azita and André will demo how our SOWL solution suite enables users to log on to Windows and other software applications by means of verifiable SSI credentials. The demo includes an overview on onboarding users and issuing credentials
#13	Microsoft, SpruceID, Ping Identity, IBM, Avast: Oliver Terbu, Kristina Yasuda, Andrew Hughes URL: https://identity.foundation/jwt-vc-presentation-profile/ Interoperable presentation of Verifiable Credentials between Wallets and Verifier built by different providers.
#14	Authentic Identity: Jason Colburne - Qui Identity URL: https://qui.xyz Qui is enabling individuals to capture, own and share authentic data about their career and professional lives. We will take our users on a journey from custodial to on-device signing to balance user experience, education and control.
#15	Indicio and Abacus: Dynamic Authorization with SSI Credentials: Mike Ebert and Jacob Siebach URL: no link yet Too often the subject of dynamic authorization utilizing SSI credentials is theoretical in nature, but no longer! We are pleased to present a working demonstration of a system that calls the Abacus authorization system to find out if a user is authorized for various actions, which integrates with Indicio Proven to check if the user has the verifiable credentials required to be authorized for the given actions. You can now set the policies to protect your endpoints, and use verifiable credentials as part of those policies, without hard-coding policies into your software!
#16	Velocity Network Foundation: the internet of careers: Andres Olave URL: https://velocitynetwork.foundation Demo of the UX of Andrew Hall claiming his education and work credentials into his Career Wallet and sharing them to take his next step in the future job marketplace all by leveraging the utility layer known as the Velocity Network.
#17	Trinsic / OkeyDoke: Michael Boyd URL: https://demo.okeydoke.io & docs.trinsic.id OkeyDoke is an ecosystem of farm auditors, farmers and suppliers. This demo showcases how a farmer gets audited, receives a credential, shares that credential with a trusted party. The demo showcases privacy-centric features like selective disclosure, adoption-centric features like wallet access without downloading another app and provider-centric features like no code trust registry creation.
#18	Global Legal Entity Identifier Foundation (GLEIF) - vLEI: Phil Feirheller URL: https://www.gleif.org/en/vlei/introducing-the-verifiable-lei-vlei Enabling SSH access to any virtual machine using a vLEI, an ACDC credential and KERI.
#19	Cheqd: Ankur Banerjee and Alex Tweeddale URL: https://creds.xyz , How cheqd is making online reputation and digital identity portable across Web3

#20

Low Code Identity Orchestration with Agama Lab : Mike Schwartz / Gluu
URL: <https://agama-lab.gluu.org>

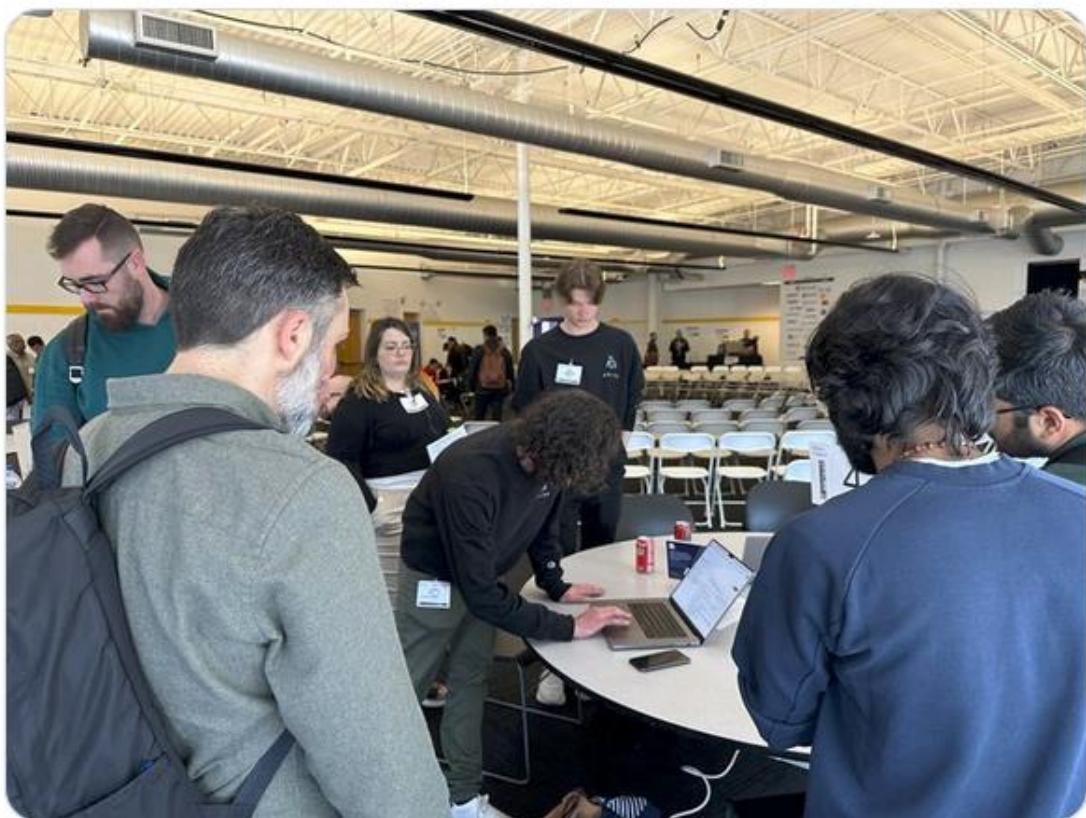
A great user experience starts with a great "identity journey," whether that's registration, authentication, social login or account recovery. See how to use low code and OpenID to whiteboard the identity journeys of your dreams. Code is saved in your Github account, including binary releases, which are ready for deployment.



Timo Glastra @TimoGlastra · Apr 19

...

We had a great demo hour at #IIW to show off [paradym.id](#) ?. If you missed the demo, I'll be doing a series of quick 15-min demos next week. calendly.com/timo-glastra/p... ✓



5



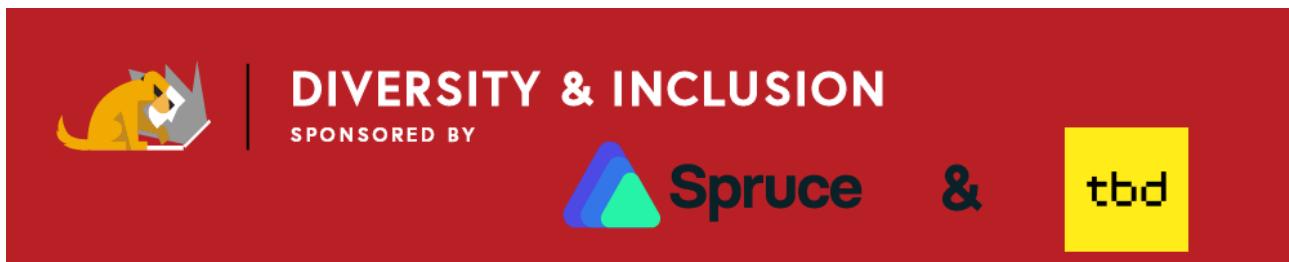
10



500



Diversity and Inclusion Scholarships - Spruce ID & tbd



Thank You to Our Diversity & Inclusion Scholarship Sponsors SpruceID and tbd

Through these sponsorships we gave reduced price & complimentary tickets and/or travel and lodging reimbursement to 7 new attendees to IIW.

We care about increasing support for women, black, and other starkly underrepresented technologists in our ecosystem. We can't build identity for everyone when demographics are homogeneous.

We are also interested in increasing participation from people that represent developing economies, as a counterpoint to the sweeping claims some SSI companies make about the technology's potential while their actual connections to those communities are limited.



Some IIW Experience Tweets



Travis Edwards @TravisADAPTECH · Apr 18

Excited to start another adventure at #IIW with a great community.

...



22



OxJane @janeyang0515 · Apr 21

6/n Overall, I left the #iiw36 feeling energized and optimistic about the future of digital identity. While there are certainly challenges to overcome, the passion and creativity of the community give me hope that we can build a more user-centric and decentralized internet.

...



37



Karim Stekelenburg @ssi_karim · Apr 22

Jet lag slowly setting in after another amazing @idworkshop. All the sessions, discussions, and new people I've met have once again left me full of inspiration, motivation, and awe. This community is simply amazing. Thank you all! #IIW

...



578



David Luna @identityluna · Apr 20

First ever #iiw done and dusted. Two key takeaways:

...

- I work in an industry with some amazing, welcoming, and kind individuals, and while rooms full of experts can be intimidating, they're forgiving of newbie mistakes.

- OID4VC is looking to be pretty darn significant.



33





Timo Glastra @TimoGlastra · Apr 22

...

I've learned a lot about decentralized identity and ssi over the last few years, but at #IIW I learned that I know just a tiny bit

1

1

14

350



Jean F. Queralt @JFQueralt · Apr 21

...

#IIW36 is over.

It's been an absolute pleasure to be a part of it and get to know all the cool people from the community.

Shout out to [@SpruceID](#) and [@TBD54566975](#) whom made my participation possible.

Also thx to [@IdentityWoman](#) and [@nobantu](#).

There will be a next one.

1

1

2

97



trustoverip @trustoverip · Apr 28

...

Recap Internet Identity Workshop #IIW36 by #ToIP member Mathieu Glaude. Many ToIP members called sessions. A great time collaborating in the Identity community to create the future of Digital Trust.

<https://trustoverip.org/blog/2023/04/28/internet-identity-workshop-36-in-review>



1

1

6

170





Danny Suárez (A builder)

@dannysuarez

...

Thrilled to have attended #IIW in person for the second time! The discussions on new identity challenges like machine impersonation, standards, and authentication using offline/online apps were truly enlightening. It was amazing to connect with other experts in the field.

← Tweet



1:26 PM · Apr 19, 2023 · 187 Views

1 Quote 2 Likes



Blog Posts About IIWXXXVI

Here's a summary from the event that [@mathieu_glaude](#) wrote as a guest blog post for [@trustoverip / https://trustoverip.org/blog/2023/04/28/internet-identity-workshop-36-in-review/](#)

Internet Identity Workshop Report by Phil Windley @windley
[https://www.technometria.com/p/internet-identity-workshop-report](#)



Indicio @IndicioID · Apr 20

Our team had a great time at #IIW 36!

...

Thank you to everyone who worked hard to put on an amazing event.
[@idworkshop](#)

To hear about some highlights from the final day, and the conference as a whole, tune in to the latest episode of Identity Insights 



[youtube.com](#)

Identity Insights - IIW Recap Day 3 April 2023

In this final episode of our special series of Identity Insights on IIW XXXVI we catch up with Mike Eber...



2



3



110



Stay Connected with the Community Over Time - Blog Posts from Community Members

New Community Resource

Each week Kaliya, Identity Woman and Informiner publish a round of the week's news from the industry. It is called **Identosphere - Sovereign Identity Updates** (**weekly newsletter**)

You can find it here: <https://newsletter.identosphere.net/>

As a follow up to the session 'Let's Bring Blogging Back' an IIW Blog aggregator has been created here: <https://identsphere.net>

If you want your blog to be included please email Kaliya: kaliya@identitywoman.net

A BlogPod was created at IIW - Link to IIW Slack -

<https://iiw.slack.com/archives/C013KKU7ZA4>

If you have trouble getting in, email [Kaliya@identitywoman.net](mailto:kaliya@identitywoman.net) with BlogPod in the Subject.

Planet Identity Revived ~ @identitywoman & @#InfoMiner cleared out & updated Planet Identity (see links below) you can support the work here:

<https://www.patreon.com/user?u=35769676>

IIW Community Personal Blog's shared via: <https://identsphere.net/blogcatcher/>

IIW Community dot.org's in the IIW Space: <https://identsphere.net/blogcatcher/orgsfeed/>

Doc Searls - Candid Photo Gallery from IIWXXXVI



Day 1: <https://www.flickr.com/photos/docsearls/albums/72177720308162829>



Day 2: <https://www.flickr.com/photos/docsearls/albums/72177720308164549>



Day 3: <https://www.flickr.com/photos/docsearls/albums/72177720308154085>

Hope to See you October 10, 11 and 12, 2023

IIWXXXVII / The 37th Internet Identity Workshop

REGISTRATION OPEN in June 2023

IIWXXXVII #37
OCTOBER 10-12 2023

HERE @ the Computer History Museum-

* IIW GLOBAL Open Space
WORKSHOPS *

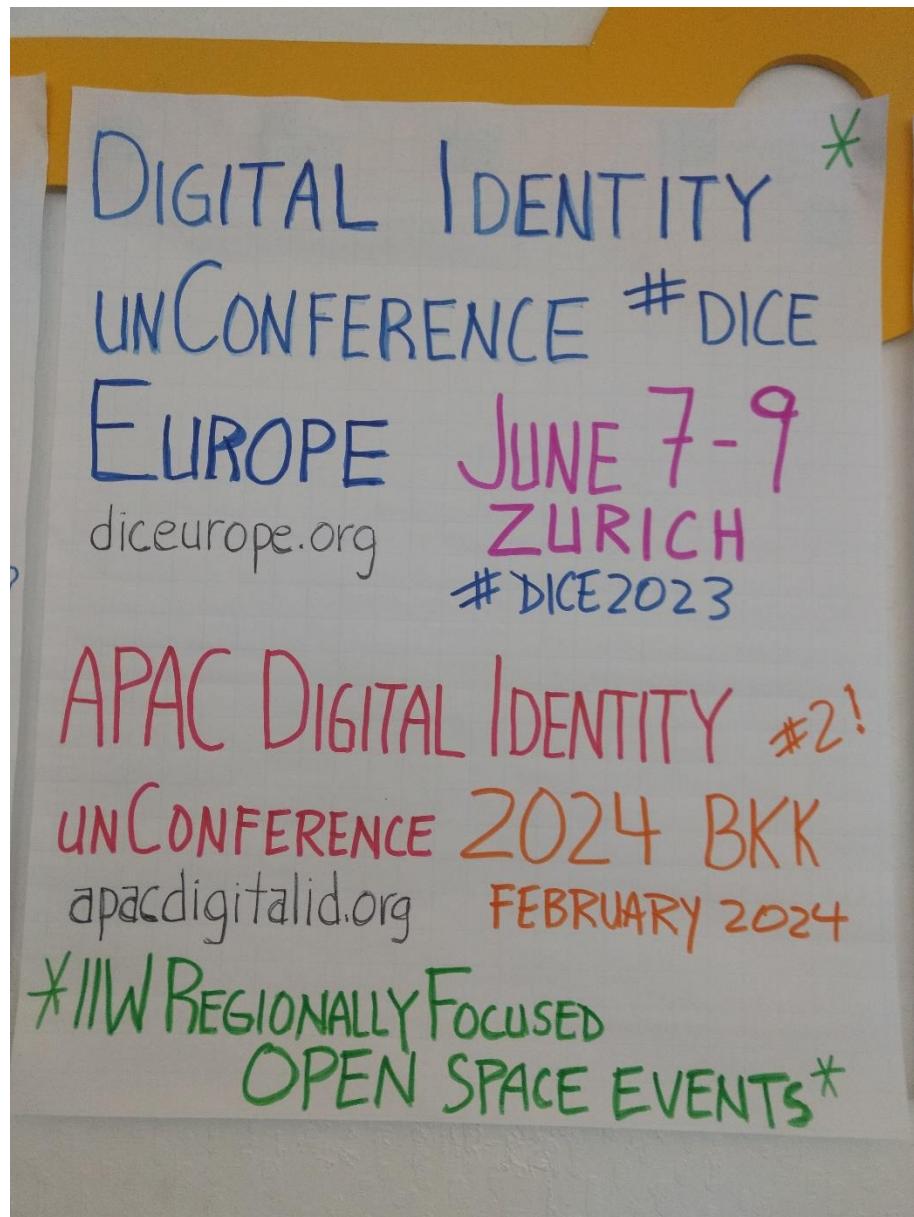
IIWXXXVIII #38

TBD SPRING 2024

IIWXXXIX #39

TBD AUTUMN 2024

Inspired by IIW™ Regionally Focused Open Space
unConference's



Digital Identity unConference Europe #DICE2023
www.diceurope.org

APAC Digital Identity unConference #APACDigitalID
www.apacdigitalid.org