



# *Book of Proceedings*

[www.internetidentityworkshop.com](http://www.internetidentityworkshop.com)

Collected & Compiled by  
HEIDI N. SAUL & SAMANTHA WINDLEY

April 26 - 28, 2022

In Person at the Computer History Museum / Mountain View CA



Opening Circle - Back IN PERSON / photo credit @timcapelii  
[#IIW](#) opening circle! So great to see everyone again!  
[@idworkshop](#)

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

[IIWXXXV In Person in Mountain View, CA](#)  
[November 15,16 and 17, 2022](#)

# Thank You! Documentation Center & Book of Proceedings

## Sponsors: JOLOCOM - Anonymome LABS - AyanWorks



@GETJolocom

@AnonymomeLabs

@ayanworkstech

## Contents

Thank You! Documentation Center & Book of Proceedings Sponsors: JOLOCOM - Anonymome LABS - AyanWorks .....	1
About IIW .....	6
Thank You to our Sponsors! .....	7
IIWXXXIIIV Daily Schedule .....	8
IIW34 Agenda Creation = Schedule & Workshop Sessions .....	10
Tuesday April 26, 2022 ~ Day 1 .....	10
Wednesday April 27, 2022 ~ Day 2 .....	11
Wednesday October 14, 2021 - Day 3 .....	13
Notes Day 1 / Tuesday April 20 / Sessions 1 - 5 .....	16
SESSION #1 .....	16
Verifiable LEI (vLEI) Update and Progress Session .....	16
IIW 101 Session-All About OAuth2 .....	16
FIDO 2 101 .....	19
Intro to Hellō .....	21
CIDPRO: Nonprofit Identity Industry Certification .....	22
OpenID for SSI .....	23
Welcome to Kantara - Active Groups .....	24
Self Sovereign Identity (SSI) is highly 'centralized': How can we fix the rotten core of issuer reputation? .....	25
Platform Decentralization .....	28
Mee.foundation .....	28
SESSION #2 .....	30
Use cases for vLEIs .....	30
IIW 101 Session - Introduction to OpenID Connect .....	31
Verifiable Credentials V2 .....	31
The Dew .....	34
Create a DID in 5 minutes .....	34
DWP The Decentralized Web Platform .....	36
vLEI Ecosystem Governance Framework .....	36
Me2B Spec Intro .....	36

Libp2p.....	36
User Experience - Making the Metaverse Fun .....	37
SESSION #3 .....	40
High-security Use Cases in “passkeys” Era .....	40
IIW 101 Session UMA (User Managed Access) .....	41
Control Channel for Identity on the Internet - DIDComm .....	57
How to think about DIDs.....	57
Global Assured Identity Network PoC 101 .....	58
25 Billion Password Compromised - Preventing Account Takeover Using Open ID .....	58
What if You Had All Your Personal Data in a Single Place You Control? Demo & Discussion..	59
Reinventing Digital Identity - Consumer Merchants & Regulators.....	62
Where are the Complete EcoSystems? .....	63
Consensus - Do We Agree on What it Means to Agree?.....	69
SESSION #4 .....	71
ACDC for Muggles - Authentic Chained Data Containers NO WIZARDS!!! .....	71
IIW 101 Session / All About SSI .....	71
Introducing the Spritely Networked Communities Institute: Re-Decentralizing Online Communities .....	71
Web Browsers + Identity Flows .....	72
What Credential Format is the Best? .....	72
The ByWay Local - First ECommerce Without BigTech Giants .....	73
On-Chain Application of DIDs (did:sol & Cryptid).....	74
DIDs + Directories of Trust / Machine-Readable Governance File Basics.....	76
Data Monetization.....	77
SHOW ME the MONEY!!! A Conversation on PD&I Commercial Models / .....	78
SESSION #5 .....	78
ACDC (Wizards) Authentic Chained Data Containers .....	78
JSON Web Proofs (JWP) .....	79
Introduction to the Trust Over IP Foundation (ToIP).....	80
euCONSENT - Interoperable, Anonymised online Age Verification Across Europe .....	88
Build an SSI Proof of Concept in 30min or Less .....	89
godiddy.com .....	89
What Did You Wish You Knew When You Started Identity?.....	91
the chicken, the egg or the verifier? A verifier first approach to adoption .....	92
Self Sovereign IoT Helium, Picos, DIDComm .....	98
Twitter (What could twitter be?) .....	101
When Do We Need a Ledger? (KERI, ORB, DID:WEB, IPFS).....	102
Notes Day 2 / Wednesday April 27 / Sessions 6 - 10 .....	106
SESSION #6 .....	106
Use cases for vLEIs .....	106
DIDCOMM Super Stack.....	106
Advanced Syntax for Claims .....	106
Common Features & Requirements of SSI-based Storage.....	107
IDPro AMA and What is the Future of the IDENTITY Profession? .....	107
Bridging the Gap (Between Traditional IAM and SSI) .....	108
Human Rights by (Protocol) Design .....	110
Indy DID Method & Network of NetWorks.....	113
Open ID & SSI Credential Issuance .....	114
Access Control Use Cases.....	115
Building privacy-preserving payment rails: without commercial models, SSI will fail .....	115

SESSION #7 .....	116
verifiable LEI (vLEI) Update and Progress Session .....	116
Introduction to GNAP .....	116
Keep - UX design for the vLEI Ecosystem .....	118
Identities for the Martian smart home: An urbit discussion self-sovereign IoT.....	120
Sign in with Ethereum 101 .....	121
Wallet Security - the overloaded trust relationship.....	121
LEAKED CREDs 101 - How Leaked Creds are Used to Compromise IAM Systems?.....	121
Backchannel Logout and SSE.....	122
Reference Architecture or Trust over IP - Universal Interoperability .....	124
BBS+ Signatures.....	125
Bottom-up trust structures w/ KILT VCOs .....	126
SESSION #8 .....	127
ISO Mobile Driving License - Convergence for Adoption? - Fireside Chat Format .....	127
TPM Tutorial - Using it for User ID and Device ID.....	130
SSI Solutions: Risks, weaknesses and trade-offs .....	131
KERI and/or Ledger (Part 2) .....	132
DiD Science an analysis of global DiD Data .....	134
Webauthn, WebOTP, FedCM, Password managers - what is their relationship(s)?.....	135
Identity in the Supply Chain: GS1 Verification Library PDC and Future Use Cases .....	137
We ran a survey for SSI vendors: Find out what we found! .....	138
Machine Readable Governance Code .....	138
Credential Manifest + Wallet Rendering: Getting to V1 .....	140
SESSION #9 .....	140
How to store all your personal data in one place - technology.....	140
Dealing with a 1000 SSI Wallets and many more credentials .....	141
CESR - Composable Event Streaming Representation / CESR Proof Signatures.....	142
Hyperledger 101 .....	142
Web3 Credentialing for TODAY's Webb Wallets .....	143
Blockchain vs. "The Right to be Forgotten".....	144
VC in edu .....	145
Presentation Exchange W3C VC's .....	147
Interoperability is dead! Long live interoperability! An open discussion.....	147
Supply Chain Traceability .....	149
Verified Connections.....	149
How To NFT ME! - Secure My Personhood.....	149
SESSION #10 .....	150
Vaccination Certificate Chained Credentials Privacy Aware Presentation & Presentation	
Exchange -over- http(s)/ Ronald Koenig .....	150
Securing API Access with ZKS .....	155
DID URLs .....	157
Open Trust Claims - Atomic Trust in a Dangerous World - Interactive Hack.....	158
VP Holder Binding with Session DID through Capability Delegation.....	158
DWN Deep Dive - Discussion .....	159
Interchain Identifiers .....	159
Credential Formats - What is the Best .....	160
Domains of Identity - Presentation of Kaliya's Book .....	160
Verifiable Web Forms.....	161
Best Way to Work with and Engage Orgs - My Data, MEF, Me2B, Mee... ..	162
JWT - VC Interop Profile .....	163



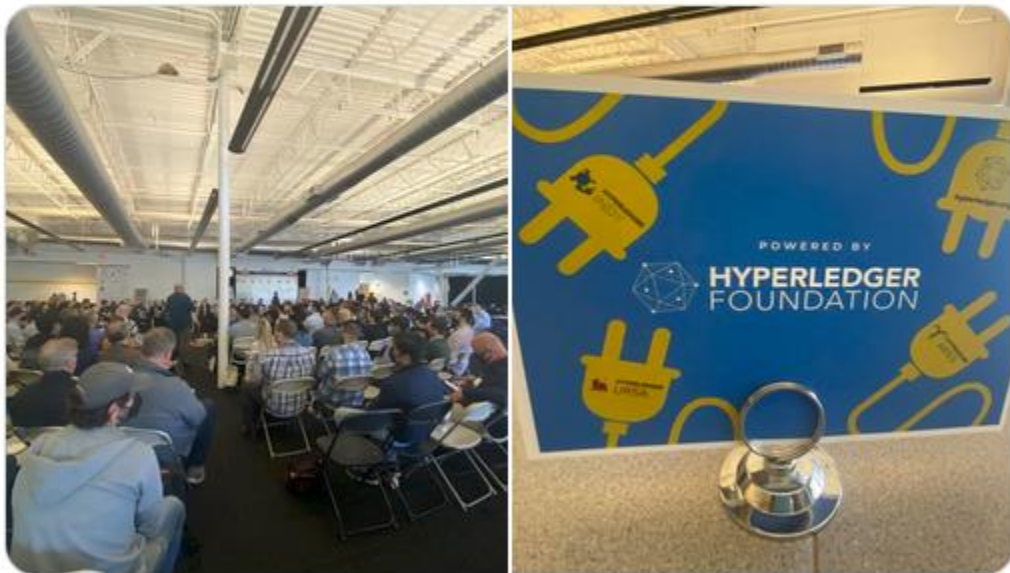
Interoperability Part 2.....	163
Notes Day 3 / Thursday April 28 / Sessions 11 - 15 .....	165
SESSION #11 .....	165
CESR Proof Signatures .....	165
How to Govern All Your Personal Data in One Place? .....	165
What to Expect with DIDcomm V2 (Sam Curren) and Auto-Generating Language Wrappers for SSI Rust Libraries (Steve McCown) .....	166
Identity Conspiracy Theories .....	166
MARKET ADOPTION STRATEGY for Global Standardization (How to get Budget!!) .....	179
Teaching SSI with Caucus Credentialing .....	179
SESSION #12 .....	180
How SSI Will be Adopted (my P.O.V.) .....	180
User-Centric Request Model .....	181
NEVER say WebAuthN is hardware-protected - unless you check attestations .....	183
KEPLER Design Overview: Shallow or Deep Dive .....	184
Kim Cameron & The Seven Laws of Identity.....	184
Can we solve the Bring Your Own Wallet Problem? .....	185
IdentiTEA for you & Me - The Trust Triangle, Triple Entry Accounting + the New New World .....	187
Identity Crisis? - Identity in the Age of AI.....	189
SESSION #13 .....	191
Poly: The Game of Community Governance.....	191
Tunnel to KERI Island - How can we interoperate with KERI?.....	193
FIDO / WebAuth for Verifiable Credentials.....	194
VALUE CHAIN How is value spread across.....	194
How do we make JSON-LD W3C Credentials Suck Less? .....	196
GLOBAL Covid Certificate Network POC Demo.....	197
They Might Be Squints? (or Distributed Addressable Processes) .....	197
Self Sovereign IoT Decentralizing Sensors w/ Helium, PICOS & DIDComm.....	198
Thoughtful Biometrics - A conversation & Workshop in July .....	201
mDL + FedCM + VC-data-model = ? .....	202
SESSION #14 .....	203
Presentation Exchange Over http(s).....	203
Let's KERI on Together. ....	208
@ Address - Fingerprints #Tags a discussion of identifier classes .....	208
So I think an Open Space unConference would be good to do for my: Organization, Association, Community.....	211
Life is Global - Living is Local LIL & LOL - Building for Humans without Bull-Dozing their Humanism .....	211
Are you telling the story you think? Communication Workshop .....	215
The Everything Graph: Building Anything from Identity Primitives .....	216
SSI & IoT (identity powered renewable energy) .....	217
GDPR: Does the G stand for Glitter Nails? A shared Vocabulary.....	218
Cards Against Identity .....	220
SESSION #15 .....	221
AR - ACDC Reputation - How to build a distributed auto resourcing Algo using ACDC .....	221
Going to DWeb Camp Aug 24 - 28 Community Planning .....	221
Discussion: Best Practice & Architecture for Cloud Enterprise Wallet .....	222
Moonshot ideas to GET DONE by NEXT IIW.....	223

DIDLANG Language for DID identifiers, documents, clustered DID agents, and DID Objects	224
DID Method Rubric .....	224
MOBILE CREDENTIALS - wish lists, changes to standards org, how to help each other.....	226
Popper's Paradox of Tolerance.....	227
Digital Identity as a Response to Climate Change .....	228
"The Scout Mindset" Why some people see things clearly, and others do not. ....	229
Demo Hour / Wednesday April 27.....	231
Diversity and Inclusion Scholarships .....	234
Kim Cameron - The 7 Laws of Identity .....	235
Stay Connected with the Community Over Time - Blog Posts from Community Members.....	236
Hope to See you November 15, 16 and 17, 2022 .....	237



**Hyperledger Foundation** @Hyperledger · Apr 26

So great to be back in person with this community at [#IIW](#) Internet Identity Workshop #34 ! Thank you 🙌 [@IdentityWoman](#) and [@windley](#) and [@nobantu](#) for all your work in getting us all back together and creating an inclusive space for all. We are honored to be a sponsor.



1

7

11



## About IIW

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

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

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

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

The event is now in its 17th year and is Co-produced by Phil Windley, Heidi Nobantu Saul and Kaliya Young. IIWXXXV (#35) will be November 15,16,17, 2022.



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

### May 16

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

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



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

Thank You to our Sponsors!



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

Upcoming IIW Events  
[IIWXXXV #35](#)  
[November 15 - 17, 2022](#)  
In Person in Mountainview, CA  
<https://internetidentityworkshop.com/>



## IIWXXXIIIV Daily Schedule

<b>TUESDAY, April 26 / Doors Open at 7:30</b> Doors Open at 7:45 AM for Registration * <b>Have your Covid document (Vax or PCR) ready &amp; a Mask!</b> 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
<b>Welcome Reception &amp; Dinner</b> 6:00 at Fuego Grille & Sports Bar 140 S Murphy Ave. Sunnyvale, CA 94086			

<b>WEDNESDAY, April 27 / Doors Open at 8:00</b> Barista! - Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme Donuts - Fruit - String Cheese etc.			
IIW Women's Breakfast Roundtable	8:00 - 9:00	Lunch	12:30 - 1:30
Opening Circle / Agenda Creation (SHARP)	9:00 -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
<b>Conference Reception &amp; Dinner</b> Back A Yard Caribbean BBQ (w/V&V options) - Here at CHM!			

THURSDAY, April 28 / Doors Open at 8:00				
Barista! - Bagels (PB&J, Cream Cheese) - Yogurt - KrispyKreme Donuts - Fruit - String Cheese etc.				
Opening Circle / Agenda Creation (SHARP)	9:00 -9:30		Session 4/Working Lunch	12:30 - 2:30
Session 1	9:30 -10:30		Session 5	2:00 - 3:00
Session 2	10:30 - 11:30		Closing Circle	3:00 - 4:00
Session 3	11:30 - 12:30		IIWXXXV Nov 15, 16 & 17, 2022	
Drinks/Dinner 5ish No Host @ Steins Beer Garden 895 Villa St. Mountain View <a href="https://www.steinsbeergarden.com/">https://www.steinsbeergarden.com/</a>				



**Joachim Lohkamp** @JoachimLohkamp · Apr 28

A fantastic long awaited **#IIW** in person meeting it was <3  
 THANK YOU @nobantu @IdentityWoman @windleyn @docsearls for  
 bringing us all together in person again!!  
[@idworkshop](#)



3

4

22



## IIW34 Agenda Creation = Schedule & Workshop Sessions



Sarah Cecchetti, CIDPRO @Sarah\_Cecc · Apr 26

Let's do this! #iiw



1



27



152 distinct sessions were called and held over 3 Days.

We received notes, slide decks, links to presentations and photos of whiteboard work for 139 of these sessions.

### *Tuesday April 26, 2022 - Day 1*

#### **Session 1**

1A/ vLEI Update

1B/ IIW 101 Session OAuth

1C/ Fido 2 101

1D/ Intro to Hellō

1E/ CIDPRO - Non profit, Identity Industry, Certification

1F/ Open ID for SSI 101 (aka SJOP w/Demo)

1G/ Welcome to Kantara - Active Groups

1H/ NO SESSION

1I/ Self Sovereign Identity is Highly 'CENTRALIZED': How can we fix the Rotten Core of Issuer Reputation?

1J/ Platform Decentralization

1K/ Mee - Consumer focused, tech agnostic, identity metasystem, nonprofit, open source motherhood, apple pie

#### **Session 2**

2A/ Uses of the vLEI - ID for organizations and representatives

2B/ IIW 101 Session - Intro to OpenID Connect

2C/ Verifiable Credential V2 - Charter Scope etc.

2D/ The Dew / Wizard -

2E/ Make DID in 5 min.(with free, open tools only) How? Bring your approach - Tell the World

2F/ DWP The Decentralized Web Platform

2G/ vLEI Ecosystem Governance Framework

2H/ NO SESSION

2I/ Me2B Spec Intro  
2J/ LibPZP  
2K/ User Experience - Making the Metaverse Fun

### **Session 3**

3A/ High Security Use Cases in “Passkeys” era  
3B/ IIW 101 Session UMA (User Managed Access)  
3C/ NO SESSION  
3D/ Control Channel for Identity DIDComm?  
3E/ How to THINK and DID's  
3F/ Global Assured Identity Network PoC 101  
3G/ 25 Billion Password Compromised - Preventing Account Takeover Using Open ID - SSE  
3H/ What if You Had All Your Personal Data in a Single Place You Control? Demo & Discussion  
3I/ Reinventing Digital Identity - Consumer Merchants & Regulators  
3J/ Where are the Complete EcoSystems?  
3K/ Consensus - Do We Agree on What it Means to Agree?

### **Session 4**

4A/ ACDC for Muggles - Authentic Chained Data Containers NO WIZARDS!!!  
4B/ IIW 101 Session - SSI 101  
4C/ Introducing the Spritely Networked Communities Institute  
4D/ NO SESSION  
4E/ WEB Browsers + Identity Flows  
4F/ What Credential Format is the Best?  
4G/ The ByWay Local - First ECommerce Without BigTech Giants  
4H/ On-Chain Application of DIDs (did:sol & Cryptid)  
4I/ Machine-Readable Governance Files 1 and DIDs + Directories of Trust  
4J/ Data Monetization  
4K/ SHOW ME the MONEY!!! A Conversation on PD&I Commercial Models

### **Session 5**

5A/ ACDC (Wizards) Authentic Chained Data Containers  
5B/ JSON Eb Proofs (JWP's) What, Why and How  
5C/ Trust Over IP Introduction & What's Next (ToIP)  
5D/ EUconsent - Interoperable Anon Age Verification Across Europe +  
5E/ Build an SSI Proof of Concept in 30min or Less  
5F/ Godiddy.com by Danube Tech  
5G/ What Did You Wish You Knew When You Started Identity?  
5H/ The Chicken, The Egg, or The Verifier - A Verifier First Approach to Adoption  
5I/ Self Sovereign IoT Helium, Picos, DIDComm  
5J/ What Should “Twitter” Really Be?  
5K/ When Do We Need a Ledger? (KERI, ORB, DID:WEB, IPFS)

## ***Wednesday April 27, 2022 ~ Day 2***

### **Session 6**

6A/vLEI Uses  
6B/ DIDCOMM Super Stack  
6C/ OpenID Advanced Syntax for Claims  
6D/ Common Features & Requirements of SSI-based Storage  
6E/ IDPro AMA and What is the Future of the IDENTITY Profession?  
6F/ Bridging The Gap! (Between Traditional IAM & SSI)



6G/ Human Rights by (Protocol) Design - Make surveillance and profiling as expensive as possible...

6H/ Indy DID Method & Network of NetWorks

6I/ Open ID & SSI Credential Issuance

6J/ Access Control Use Cases

6K/ Building Privacy - Preserving Payment Rails for Identity Exchange

### **Session 7**

7A/ vLEI Update

7B/ Introduction to GNAP

7C/ Keep UX Design for the vLEI Ecosystem

7D/ Identities or the MARTIAN Smart Home: an orbital discussion of self-sovereign IoT

7E/ Sign-In-with ETHEREUM 101

7F/ Wallet Security - the overloaded trust relationship

7G/ LEAKED CREDENTIALS 101 - How Leaked Credentials are Used to Compromise IAM Systems?

7H/ BACK CHANNEL LOGOUT & Shared Signals & Event (SSE) as a Token/Session Revocation Mechanism in the 3PC Deprec

7I/ Reference Architecture or Trust over IP - Universal Interoperability

7J/ BBS +

7K/ Bottom-up Trust Structures w/ KILT VCOs

### **Session 8**

8A/NO SESSION

8B/ ISO Mobile Driving License - Convergence for Adoption? - Fireside Chat Format

8C/ TPM Tutorial - Using it for User ID and Device ID

8D/ What are Still the Risks & Weaknesses in SSI Solutions?

8E/ KERI and/or Ledger?

8F/ DiD Science an analysis of global DiD Data

8G/ Webauthn, WebOTP, FedCM, Password Managers - Relationships?

8H/ Identity in the Supply Chain: GS1 Verification Library - POC and Future Use Cases

8I/ We ran a survey for SSI vendors: Find out what we found!

8J/ Governance Code

8K/ Cred. Manifest/Wallet Rendering: Getting to V1

### **Session 9**

9A/ How to Store All Your Personal Data in One Place - Technology

9B/ Dealing with a 1000 SSI Wallets and many more credentials

9C/ CESR - Composable Event Streaming Representation / CESR Proof Signatures

9D/ HYPERLEDGER 101

9E/ WEB 3 Credentialing for TODAY's Webb Wallets

9F/ BLOCKCHAIN vs. Right To Be Forgotten: 3 Solutions

9G/ Edu - VC's

9H/ Presentation Exchange - W3C VC's

9I/ INTEROPERABILITY is DEAD! LONG LIVE INTEROPERABILITY! An open discussion

9J/ Supply Chain Traceability - VC, DID, Linked Data

9K/ Verified Connections

9L/ How To NFT ME! - Secure My Personhood

### **Session 10**

10A/ Vaccination Certificate Chained Credentials Privacy Aware Presentation & Presentation Exchange -over-

10B/ ZKP's & API Access

10C/ DID URLs

10D/ Open Trust Claims - Atomic Trust in a Dangerous World - Interactive Hack  
10E/ VP Holder Binding w/ Session DID Through Capability Delegation  
10F/ DWN Deep Dive - Discussion  
10G/ Interchain Identifiers (IIDs)  
10H/ Credential Formats - What is the Best  
10I/ Domains of Identity - Presentation of Kaliya's Book  
10J/ Verifiable Web Forms  
10K/ Best Way to Work with and Engage Orgs - My Data, MEF, Me2B, Me9...  
10L/ JWT - VC Interop Profile  
Standing Circle/ Interoperability Part 2

### ***Wednesday October 14, 2021 - Day 3***

#### **Session 11**

11A/ How to govern all your personal data in one place?  
11B/ Auto-Generating Language Wrappers for SSI Rust Libraries & What to Expect with DIDcomm V2  
11C/ CESR Proof Signatures  
11D/ NO SESSION  
11E/ NO SESSION  
11F/ Conspiracy Theories about digital ID - What are they? How do we respond?  
11G/ MARKET ADOPTION STRATEGY for Global Standardization (How to get Budget!!)  
11H/ NO SESSION  
11I/ NO SESSION  
11J/ NO SESSION  
11K/ NO SESSION  
11L/Teaching SSI with Political Precinct Caucus Credentialing

#### **Session 12**

12A/ How SSI Will be Adopted (my P.O.V.)  
12B/ USER - CENTRIC REQUEST MODEL  
12C/ NEVER say WebAuthN is Hardware protected unless you check attestations!  
12D/ KEPLER Design Overview: Shallow or Deep Dive  
12E/NO SESSION  
12F/Kim Cameron & The Seven Laws of Identity  
12G/ Can we solve the Bring Your Own Wallet Problem?  
12H/ IdentiTEA for you & Me - The Trust Triangle, Triple Entry Accounting + the New New World  
12I/ Identity in the Age of A.I. - Identity Crisis? "An open conversation"  
12J/ NO SESSION  
12K/ NO SESSION  
12L/ NO SESSION

#### **Session 13**

13A/ POLY: The Game of Community Go Verifiable - come brainstorm a game for communities to create their own rules  
13B/ Tunnel to KERI Island - How can we interoperate with KERI?  
13C/ FIDO / WebAuth for Verifiable Credentials  
13D/ VALUE CHAIN How is value spread across  
13E/ How can we make W3C JSON-LD Credentials sucl less?  
13F/ GLOBAL Covid Certificate Network POC Demo  
13G/ NO SESSION  
13H/ They Might be SQUINTs ?! (or DAPs...)  
13I/ Self Sovereign IoT Decentralizing Sensors w/ Helium, PICOS & DIDComm

13J/ Thoughtful Biometrics - A conversation & Workshop in July  
13K/ Browser API: Fedcom + VC + mDL?  
13L/ NO SESSION

#### Session 14

14A/ Presentation Exchange - over- HTTP(s) +  
14B/ NO SESSION  
14C/ Lets KERI on Together  
14D/ @ Address - Fingerprints #Tags a discussion of identifier classes  
14E/ NO SESSION  
14F/ So I think an Open Space unConference would be good to do for my: Organization, Association, Community  
14G/ LIL & LOL - Building for Humans without Bull-Dozing their Humanism  
14H/ Are you telling the story you think? Communication Workshop  
14I/ The Everything Graph: Building Anything from Identity Primitives  
14J/ SSI and IoT  
14K/ GDPR: Does the G stand for Glitter Nails? A shared Vocabulary  
14L/ Cards Against Identity

#### Session 15

15A/AR - ACDC Reputation - How to build a distributed auto resourcing Algo using ACDC  
15B/ Going to DWeb Camp Aug 24 - 28 Community Planning  
15C/ Discussion: Best Practice & Architecture for Cloud Enterprise Wallet  
15D/ NO SESSION  
15E/ MOONSHOT Ideas to GET DONE by NEXT IIW  
15F/ DIDLANG Language for DID identifiers, documents, clustered DID agents, and DID Objects  
15G/ DID Method Rubric  
15H/ MOBILE CREDENTIALS - wish lists, changes to standards org, how to help each other Hughes  
15I/ Popper's Paradox of Tolerance  
15J/ DIGITAL ID as a Response to Climate Change  
15K/ "The Scout Mindset" Why some people see things clearly, and others do not.  
15L/ NO SESSION





Scott Heger @ScottHeger · Apr 26  
So many options! #IIW



euCONSENT @euCONSENTeu · Apr 26

We're at the Internet Identity Workshop #IIW in the heart of Silicon Valley to introduce @euCONSENTeu to some of the leading experts in digital identity and see what they think about our solution for anonymised #AgeVerification across Europe - and get ideas on how to improve it!



4

10





## Notes Day 1 / Tuesday April 20 / Sessions 1 - 5

### SESSION #1

#### *Verifiable LEI (vLEI) Update and Progress Session*

Session Convener: Karla McKenna, Christoph Schneider (GLEIF)

Notes-taker(s): Christoph Schneider (GLEIF)

Tags / links to resources / technology discussed, related to this session: Organizational Identity, Verifiable Credentials, Persons in roles, KERI, ACDC

Slides available at: [https://github.com/WebOfTrust/IIW34/blob/main/2022-04-06\\_vLEI-Update-Progress-Session-IIW\\_v1.0\\_final-for-publication.pdf](https://github.com/WebOfTrust/IIW34/blob/main/2022-04-06_vLEI-Update-Progress-Session-IIW_v1.0_final-for-publication.pdf)

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

No discussion notes

#### *IIW 101 Session-All About OAuth2*

Session Convener: Vittorio Bertocci

Notes-taker(s):

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

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

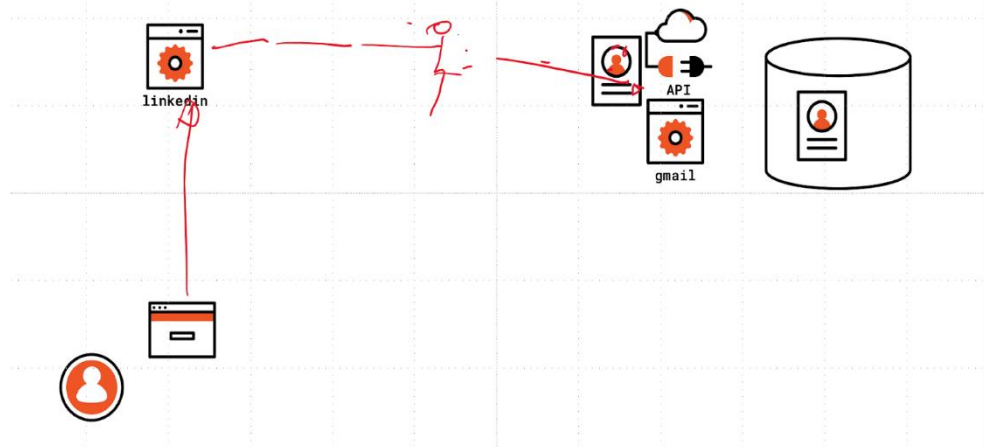
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

NOTES FROM IIW #33 Session led by Vittorio

##### **Scenario 1: Naive Approach**

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

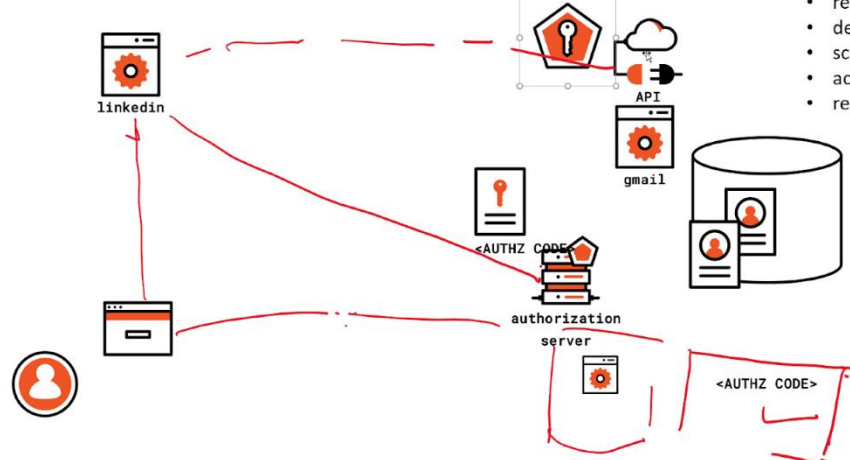
## Accessing Resources Across Apps: Brute Force



### Scenario 2: OAuth 2 Approach (Delegated Authorization)

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

## The Quintessential OAuth2 Scenario



- Concepts:
- OAuth2
  - authorization server
  - clients
  - registrations
  - delegation
  - scopes
  - access token
  - refresh token

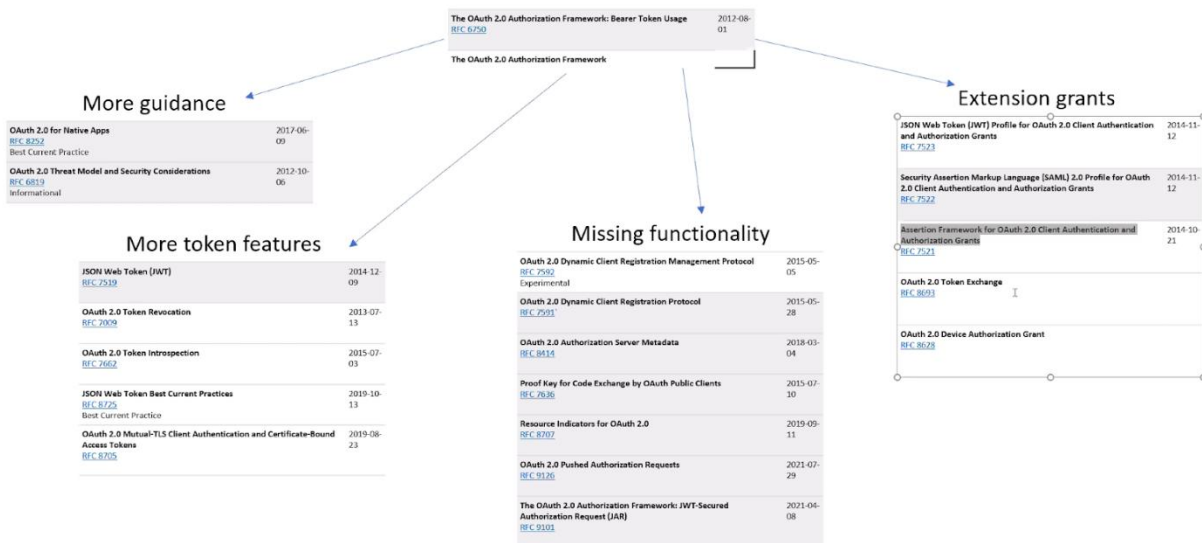
## Comments on standards

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

## Note

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

## Beyond the core



## FIDO 2 101

**Session Convener:** John Bradley and David Waite

**Notes-taker(s):** George Fletcher

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

### FIDO 2

- FIDO 2 is a marketing term for two specs
  - WebauthN - Level 2 in W3C
    - JS API between RP and browser
  - CTAP2.1 - FIDO Alliance
    - Client To Authenticator Protocol (CTAP) - browser to hardware key

### CTAP 2.0

- V2 added multi factor auth and discovery of keys (?)
- V2.1 - cleaned up stuff in V2, added privacy features, fixed stuff for FIPS certification
  - Supported by Chrome on OS x and Linux
  - Microsoft Edge maybe in the fall
  - Apple - unknown date
- V2.2 - just started work on this
- Firefox/Safari at WebAuthn Level 1

### U2F

- Predecessor to CTAP 2.0
- RP's should no longer use the U2F API
- RP's should switch to the new API

### Actors in the FIDO environment

- Relying Party - Server+web/native app
- Client - Browser/OS
- Authenticator - Key/Platform
  - WebAuthN is Javascript API for RP to Browser/OS
  - CTAP is hardware protocols for Browser/OS to hardware Authenticator

### History of FIDO2

- Originally named Nubby - effort between Google and Yubikey

### U2F protocol API

- Make Credential - Invoked by RP
  - Challenge
  - Browser invoked Authenticator with Challenge and adds the AppID (now RPID)
  - Authenticator
    - Challenge
    - AppID Hash
    - Generate key pair based on AppID Hash
    - Generate credential ID
  - Returns...
    - Credential ID
    - Auth Data
    - Assertion
    - Public Key
  - Goes back to RP
- This API is stateless as the key/authenticator doesn't store any data
- When the user wants to authenticate
  - Invoked by RP with challenge + credential ID [] - list



- Browser invokes Authenticator (getAssertion)
  - AppID
  - Credential ID List
  - Browser iterates through the Cred ID list
- Authenticator
  - uses the AppID and Cred ID to see if it's one understood by this key
  - also receives authenticator data hash
  - Decode the Credential ID in order to regen the pub/priv key pair
  - Signs over client data and authentication data hash
  - Send back an assertion
- RP verifies...
  - RP auth data matches it's site
  - the assertion is signed by the correct public key
- Built for second factor use
  - credential data is not stored on the key
  - RP does first factor and then based on that knows the information to send to the browser to validate the second factor

#### WebAuthN W3C standard (level 1)

- AppID -> moved to being origin based (foo.example) -> now RPID
- Backward compatible with U2F
- Add support for the key to manage state and store credentials
- "Does the user have a way to login to my site"? based on data stored in the key
  - Display name for the user provided for the stored data to allow the user to distinguish
    - account id
    - friendly name
    - email address
    - Useful for password less based login
    - Browser will display the "account chooser"
    - RP gets a signed assertion containing the identity the user selected
  - Supported everywhere except Chrome on Android and Firefox on linux and OS x
    - not supported at all on Android
  - Have something in all the browser
- UX is problematic for different platforms
  - OS level UX is required
  - From user perspective the UX is still very confusing
- WebAuthN Level 2
  - Fixing issues found during the rollout of resident credential support
  - RP gets to choose whether the credential should be discoverable
  - In CTAP2.1 added enterprise related features
    - minimum pin length requirements
    - limited to specific enterprise configured RPIs
    - biometric enrollment
  - Set different privacy levels
    - cred protect level 2
    - getAssertion will not find the key unless the user has done some authentication (biometric or pin)
  - Credential Management API
- WebAuthN Level 3 - pushing for broader adoption
  - Goal to migrate off of passwords
  - Make it easier for people to get out of storing passwords
  - RP adoption is difficult and desire level 3 to address these issues

## Intro to Hellō

Session Convener: Dick Hardt  
Notes-taker(s): Steve Venema

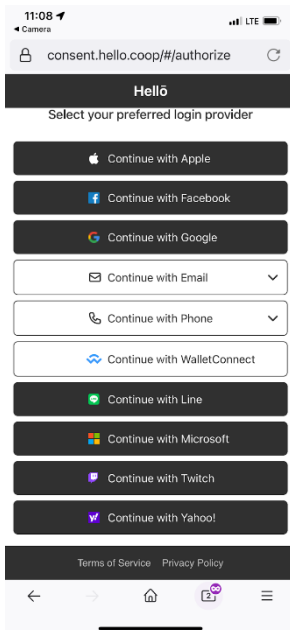
Tags / links to resources / technology discussed, related to this session: <https://hello.coop>

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

First part of the session was just people playing around with the live demo from their phones. You use this QR code (pic from the session whiteboard):



...which takes you to a webpage that looks like this:



The overall idea here is to allow developers to get their app working with one [proxy] IDP which can, in turn, interact with many different IDPs. I tried the above registration flow and found the prompts a bit confusing regarding what data is being shared with whom and what the trust model looks like.

Business model:

- “Revenue” comes from charging RP’s a few cents per verified claim
  - This is in quotes because they only work in a token currency managed through a DAO (Decentralized Autonomous Organization)
  - Vision: Resellers can charge real \$\$’s and convert that money to tokens in the DAO
  - 40% of the “production” will go into the DAO (I didn’t fully understand this)
  - Dick noted that tokenomics is an area of active development so they don’t specifically focus on this except as a consumer of the emerging tokenomics capabilities

Privacy

- One of the technical innovations that Dick claimed is around privacy, but the group got sidetracked before this could be enumerated better.

3 components:

- Orchestration service, what the RP hits it, which starts a session
  - Looks up the RP info
  - User goes to \$Google to authenticate
  - Gets a token from the token service
- Encryption service
- Storage service

Only the user can manage what is stored relative to that user (for a given IDP i think)

When you first use the service, you become a “member of the cooperative” and are emailed a link to their profile management service interface.

## ***CIDPRO: Nonprofit Identity Industry Certification***

**Session Convener:** Sarah Cecchetti

**Notes-taker(s):** Sarah Cecchetti

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

[Idpro.org/cidpro](http://Idpro.org/cidpro)

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

IDPro is a professional organization formed by identity professionals who wanted to share experiences and resources. IDPro started by creating a slack where identity professionals could interact and ask each other questions, then they built a vendor-neutral Body of Knowledge for the identity industry, and when they asked their members what would have helped early in their career, they said a certification would have been helpful so they know what they don’t know.

IDPro developed the CIDPRO exam with five major pillars:

Identity basics

## OpenID for SSI

**Session Convener:** Torsten & Kristina

**Notes-taker(s):** Hannah Sutor

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

<https://de.slideshare.net/TorstenLodderstedt/openid-for-ssi>

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

Want to leverage well known advantages of OpenID Connect - Simplicity and Security

Existing libraries - HTTPs and a little bit of JSON

Great for mobile applications, no firewall hassles

Not about legacy transformation - it's about supporting SSI applications natively

Self-Issued OP v2 - users can control their own authentication methods, key material

Important: To be as broad and flexible as possible when it comes to the rest of the SSI stack

Goal: To be flexible, allow any credential format, mechanism, etc

OpenID connect has a decentralized/federated architecture since the beginning -> not used only by the "big guys"

Important for the design to be as flexible and general as possible when it comes to integrating SSI into OID

Selling points are both self-hosted OPs and edge-based OIPs (e.g., smart cars) -> could be used in LinkedIn for "checkmarked" certificates or working experiences

Key management is different between the standard model and SIOP: in the latter, the user manages their own key, and the website trusts such an identifier. It does not have any mentions of credentials yet, it is just a way for a user to IDENTIFY themselves

Credentials enter the picture with SIOP v2 + OpenID Connect 4 Verifiable Presentations -> The RP needs to verify any details, like the revocation status, which means that the verifier (or RP) has to have knowledge of the tech stack underlying the credential used in the flow

### Use Cases

Why should I move to this model vs the model we have now?

- Completely hosted locally on your device - not dependent on third party hosting
- Authentication as edge
- In one translation, I can present credentials from multiple issuers
  - I as a user, I already proved I work for company X, now LinkedIn can consume that and verify me



### *Self-Issued OP Model*

Instead of having trust in third party, we have our trust in the cryptographically verifiable identifier.  
Opens up for verification via DID

Are DIDs replacing authorization tokens?

No. ID token and Access tokens are inherently different. DIDs are an identifier which just sends out identity token.

#### **Benefits:**

- Format Agnostic
- Passing `presentation\_definition` PE object by value or by reference
- Support for trust schemes -
- Dynamic SIOP discovery and invocation via HTTPS URLs (enables use of app/universal links and web wallets)
- Leverages all OpenID Connect flows. Can be locally hosted, cloud components, or cloud-based
- Cross device flow enabled - "I'm starting here, but I'm presenting a credential that's on my phone"
- Leverages OpenID connect metadata for verifiers and wallet management

#### **Demo**

Extending existing wallet. Built on top of Indy SDK to come up with most incremental solution

-Use Wallet to log into NextCloud

- Goal: all members in consortium can use wallet for logging into NextCloud

- QR code contain SIOP request

- Wallet shows you where data is being sent. Data is sent directly from Wallet to verifier using HTTPS

Goal: Interoperability.

## ***Welcome to Kantara - Active Groups***

**Session Convener:** John Wunderlick @PrivacyCDV

**Notes-taker(s):**

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

<https://kantarainitiative.org/>

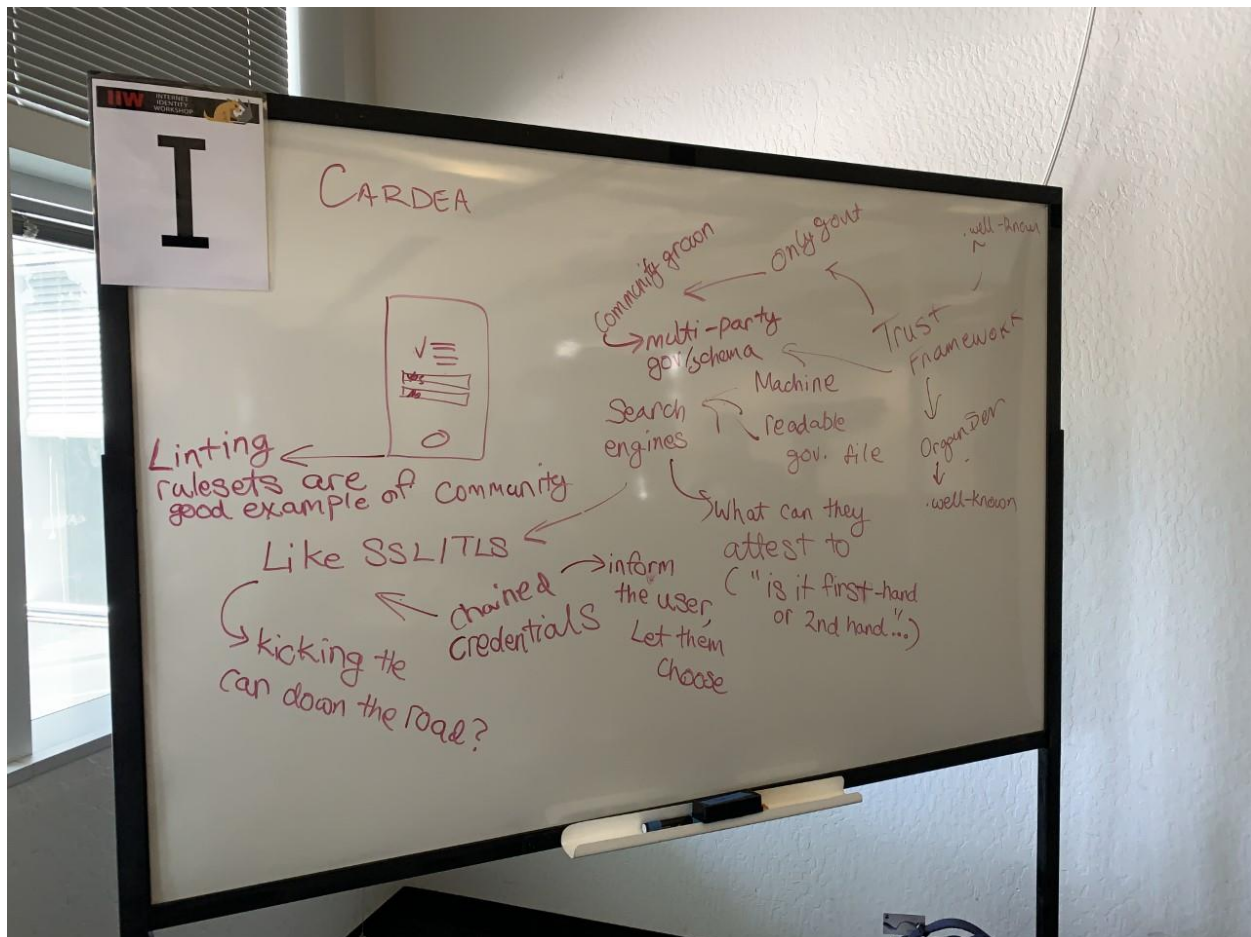
**Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:**

## *Self Sovereign Identity (SSI) is highly 'centralized': How can we fix the rotten core of issuer reputation?*

Session Convener: Ankur Banerjee

Notes-taker(s): [Peter Langenkamp](#)

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



### Basics: what do we mean by "self-sovereign identity is centralized"?

1. There are *two* broad approaches (discussed during the session) on how the issuers of digital credentials get to "trusted" status:
  0. There is a list of "known" or "trusted" issuers, perhaps with trusted Decentralized Identifiers (DIDs) that are shared within an ecosystem.
- 2.
3. How do you determine the issuers that are trustworthy?

Two approaches

- list of trustworthy issuers (list in ecosystem is known)
- Issuer places document on their site, proving they have control over some trustworthy domain
- if i show control over that domain, I have proved you can trust me

Both seem highly decentralized

In most systems there seems to be a list: these are the trustworthy issuers

But how do you get this to scale?

Thoughts & comments

- Trust frameworks
- no solution currently solves the problem at hand

Most systems now need a regulator

It would be great if you could take a credential from one context and use it in another one, how do you make it machine readable?

- Trust framework organizer publishes a list
- Publicly publish a machine readable gov. file
  - since it's a URL there are many ways this can be shared
  - search engines
- The user can select which authority they trust

Suppose

- You install the governance frameworks that you trust
- credentials can be compared against those governance frameworks
  - You can e.g. see that your employer likes / dislikes / no opinion about the issuer
  - (trust framework just about issuer? isn't it about the combination of issuer and credential type? e.g. you may trust me to issue a proof of attendance credential but not a passport)
  - it's not just about who's the issuer, but also about what they issue. e.g. don't trust them for your address but do trust them for something else
  - what can they attest to? ("is it first hand")

In VGE(?), we're working with trusted institutions

- Very different type of trust than SSI trust

An address as issued by the government is different from one issued by your gas or electricity company (the latter do not necessarily know whether YOU live there)

A lot of information is obtained second hand, e.g. through a picture.

- SSI is all about reuse of information
- can I take it and use it in a second, third or fourth place?
- do I know this issuer becomes relevant

What is SSI?

- in the analog world you can have a driver's license or passport, SSI provides a solution for a digital equivalent (you control your data)

Same problem in Germany with a large number of parties that can issue a vaccination credential

- chained solution (trust chain) an authorization credential is included in the vaccination credential that can prove the authority of the issuer

Multi-party governance over (fields in) schema's - Multi-party schema governance  
- e.g. in the health space, collaboration on creating vaccination schema's

About the chained credentials

- the idea is still that there is a centralized authority at the basis of this
- it can be highly effective in many different contexts
- but still highly centralized

Like SSL/TLS?

- Web PKI is a mess, but it works for now
- By moving it down the road, it's now in a context where you can ask different questions
  - different scales
  - different trust roots

It's important to distinguish between the concept of certificate chaining and the method the browser uses to determine what to trust

- Do it in a way that informs the user, instead of letting the software make the choice (inform the user, let them choose)

With DID you can use one DID to prove ownership over another one (different from 'also known as', which you may not want to use all the time)

There's two questions

- centralization problem
- is this issuer supposed to say this in the first place?
  - can probably be solved more easily than the other problem

One authority of a very specific use case, rather than 50 different ones that each try to do all

- Single authority per country might work
  - but then in the US they need to trust the authorities of other countries
- It becomes more complicated when you start mixing contexts

You are missing something, get it somewhere else

Linkrot, something may have been issued and still be valid

Being able to choose which authorities to trust could be a solution, but might run into a similar 'problem' as we see with search engines where many are available but only two have a significant market share (Google and Bing)

Linting rulesets are good examples of community



## ***Platform Decentralization***

**Session Convener:** Adrian Gropper

**Notes-taker(s):** Adrian Gropper

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

Human Rights, GNAP, Decentralization

<https://bit.ly/PlatformDecentralization>

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

## ***Mee.foundation***

**Session Convener:** Paul Trevithick

**Notes-taker(s):** Michael Becker

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

### **Mee.foundation**

Mee Foundation (mee.foundation) Paul Trevithick has founded a non-profit looking to help people get control over a dataset of me (using both technical and legal/governance means)

- He wants to start over again, i.e. the tech, the market model, etc building on earlier work
- Does not believe the market is human-centered
- Status quo has gotten worse “More power in the hands of fewer”
- Personal Data and Identity is too valuable to be commercialized
- People are the ones to release their information
- We are not monolithic, we are highly contextual, “multi-contextually matters”, we should be able to present ourselves as we wish

### **Attendees:**

- Kimberly Wilson - Randa Solutions. credential Publisher in ND and Teacher licenser program
- Alexander Castro - 2060.io CE)
- Randy Farmer, Exec. Direct Spritely. institute
- Michael Becker
- Paul Trevithick
- Jeff Orgel - Computer Guy
- Damon Tinball Randa Solution CIO
- Doc Searls
- Nara
- PhilipP
- Wendell Baker

## What's the idea

- Mee is not a new identity system. It introduces no new technology. It is an identity metasystem.
- It's an extensible software framework that existing technologies can plug into. And a legal framework that supports various levels of governance of personal data from the user's agent.
- Analogous (from an end-user point of view) to Visa. Visa provides an "Interoperability Promise"; it does not provide the cards; the bank does. Visa provides the infrastructure and guidelines.
- Mee logo is a service mark that individuals can see to know a participating service allows for self-sovereign identity.

## Complimentary models

We discussed complimentary models, e.g., Me2B and Irene Ng's Dataswift. There are opportunities to merge this idea with other initiatives, like them

## Relevant technologies

- [Liam Broza](#), Co-Founder at Laguna Labs, LifeScope.io
- [Johannes Ernst](#), Indie Computing Corp., has a solution to pull social data

## Themes:

- Life is local
- Mee assumes a nuanced, contextualized model of a person's data
- Mee assumes a contract between the individual (or more precisely Mee acting as their fiduciary) and the app/business/other. In the discussion we agreed that a contract isn't always needed (e.g. self-governing social groups)
- On the verge to being big: \$0 trillion-dollar industry (so much potential but unclear if anyone is making money)
- Status quo has gotten worse "More power in the hands of fewer"; Just giving power to the billionaires
- What is common about everything is the human being; we are the center of integration
- Opportunity to revolutionize commerce – what would happen if "I were" were in control
- Solution ideas
  - Start with the user
  - Offer a digital twin that knows all about the user
  - This twin is the foundation for Personal AI
  - The twin can express intent, say what we want to buy
  - Let be a conduit of our medical records, government records
- User centricity
- Decentralized architecture
- Power to the people
- Phil Windley Quote: "Networks can not exist without a means to move value from the edge of the network to the center of the network." "The Internet was a happy accident because it had that ability value transaction-billing-at the center."
- Kim Cameron proposed an identity "metasystem," not an identity system. Mee is a continuation of that approach.

## Questions

- How do we build a software framework?
- How do we build the legal framework?

## References

- Filter Bubble Ted Talk: ad systems are built on a bad model of you. Assumption: “Homo Consumerous.” You are always buying.
- IEEE P7012 - Machine-readable personal privacy terms - People set their only terms of service.
- ePrivacy regulations
- The Twitter - the “Fail Whale” - could not handle the number user wants to use the system. Hit a hard wall on millions of users. Put a block on the scope. Once fixed, the Internet did not need to solve the identity problem.

## SESSION #2

### *Use cases for vLEIs*

**Session Convener:** Stephan Wolf (GLEIF)

**Notes-taker(s):** Christoph Schneider (GLEIF)

**Tags / links to resources / technology discussed, related to this session:** verifiable LEI, Business use cases, Annual report, KERI, CCSR-Proof signatures

Slides available at: [https://github.com/WebOfTrust/IIW34/blob/main/20223-04-26 IIW-vLEI-Use%20Cases.pdf](https://github.com/WebOfTrust/IIW34/blob/main/20223-04-26%20IIW-vLEI-Use%20Cases.pdf)

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

## ***IIW 101 Session - Introduction to OpenID Connect***

**Session Convener:** Michael B. Jones

**Notes-taker(s):** Michael B. Jones

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

The “Introduction to OpenID Connect” presentation can be found at <https://self-issued.info/?p=2269>.

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

The discussion of the relationship to OpenID 2.0 and the lessons learned there was very much enhanced by the presence of Joseph Smarr - who worked on it.

Great questions were asked about protocol security features, including using “nonce” to prevent token injection attacks.

There was a great discussion on using the certification suite to test implementations as they evolve - including using it for continuous integration testing. The certification suite can be used for this for free. A fee is only charged when a certification request is submitted. The certification fees are low and are intended to cover the OpenID Foundation’s costs of operating the certification program.

## ***Verifiable Credentials V2***

**Session Convener:** Brent Z and Kristina Y

**Notes-taker(s):** Steve Venema

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

~35 attendees

In Scope:

- Fix issues with previous versions of the VC data model
- What’s the data model for requesting information
- Registries for the data model
- Algorithms for the expression of proofs (missing from older specs)
- Refining multilingual support in the data model
- Explicitly not a req’t that the new specs be fully compatible with past versions

Out of Scope:

- We don't care what ledger to use for VC ecosystem
- The specification of new cryptographic primitives
- The normative spec of APIs or protocols

...still a data model specification

The objects are being defined

The flow is not being defined (though it may be shown as examples of \*a\* way to do something)

## Normative Deliverables

- VC Data model (VCDM) 2.0
  - Next version of the data model.
  - Open questions about data format (just JSON? CBOR? ...?)
- Securing Verifiable Credentials (SVC) 1.0
  - Normatively fill the proof section missing from older specs
  - Cryptosuites for VC-JSON Web Token (JWT): IANA JOSE Algorithms Registry
  - Cryptosuites for Data Integrity: JSON Web Signature 2020, EdDSA, NIST ECDSA, Koblitz ECDSA

## Conditional Normative Deliverables

Depends on progress in the W3C Credentials Community Group, the IETF, and the DIF, this WG may also produce W3C recommendations based on the following documents. This is an example set, may do other things (or not)

- PGP Cryptosuite
- BBS+ Cryptosuite
- VC protection using JWPs
- Koblitz ECDSA Recovery Cryptosuite

Q: List of issues from existing specs

A: We have a list of errata. Please file issues on the spec—you don't need to be a member.

Existing spec issues automatically get promoted

Q: How long is this lifespan before we have 3.0?

A: V2 will come out in ~2 years. So keep using V1

Q: What about chained credentials (AC/DC topic)

A: Nothing in our effort precludes this, but we need participation from people in that space to make sure the new specs support it.

Note: the VC-v2 WG hasn't started yet, so you haven't missed anything (yet)

Kristina: maybe this is happening a bit early, but the forcing function is standardization of the signatures

Q: Does the WG have a philosophy on quantum attacks?

A: We aren't crypto experts, but if there is a signature approach that is quantum resistant, then we can choose this.

Req't from W3C is if we want to refer to an external spec, then it needs to be something that comes from a standards org that issues normative specs



## Registries

The WG may create a set of registries including registry definitions and registry tables to support extension points in the above normative deliverables.

Ex: VC properties that MUST be included in a VC, must have at least one standardized entry.

Motivation: we don't know what will be coming after the WG is done—allows the spec to evolve in a normative way.

MUST have at least one item in the registry—allows for testability and avoid kicking cans down the road

Q: Could this WG support the property graph approach of the AC/DC work?

A: Yes, but we need participation in order to develop consensus

## Other Deliverables

Things we may do some or none of these:

- Test suites for all normative deliverables
- Presentation Request Data Model
- Storage and Sharing of VCs
- Privacy Guidance for Verifiable Credentials
- Extensions for binding multilingual resources for localized user interfaces
- A Developer Guide consisting of one or more notes related to general implementation guidance and best practices
  - One or more HTTP protocols definitions for VC Exchange (such as VC-API)
  - Guidance on VC Exchange offer OIDC
  - VC exchange over Grant Negotiation and Authorization Protocol (GNAP)
  - Other protocols as time and attention and resources permit
- Guidance to enhance VC interoperability
  - VC extension vocabularies (e.g., ISO 18013-5 mDL)
  - Implementation Guides
  - Test Suites

Q: What about revocation?

A: Brent: I would put this under the “Storage and “Sharing of VCs”” topic

Q: Most use cases require revocation

Q: How about VC lifecycle

A: We aren't doing APIs, but it should be possible to use our data models and give guidance on this.

Brent: We need to keep the charter concise; the audience is the AC's who review these. They want something that has a limited lifetime. 2 years is typically the limit. You can ask for extensions, but you need to show great progress before this.

Github repo: vc-data-model

Q: How to approach complexity management – like encoding variants.

A: Brent (personal opinion): I think it should be very limited. But as WG chair I want to encourage other proposals.

A: Kristina: ideally we'd like to have just one encoding

Q: registry for the schemas

A: wouldn't expect that

Comments: <couldn't hear clearly>

Comment: Don't mistake encoding for schema

Q: How can we participate

A: If you are a member of W3C have your AC representative register. If you aren't in a position to join W3C, reach out to Kristina and Brent as there are options to still participate

A: WG hasn't started yet (taking a bit of a break). Expect a weekly cadence.

## ***The Dew***

**Session Convener:** Blaine Garst - Wizard

**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

## ***Create a DID in 5 minutes***

**Session Convener:** Kim and Joe

**Notes-taker(s):** Ashley Snelgrove

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

<https://github.com/digitalbazaar/did-cli>

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

Was in preparation for an upcoming panel discussion. Tried to find it... I *believe* this may be a recording of it (on Interoperable Platforms):

[https://twitter.com/centre\\_io/status/1520113095988944897?s=20&t=5uL4GLJjMZZWXH-oCLipEQ](https://twitter.com/centre_io/status/1520113095988944897?s=20&t=5uL4GLJjMZZWXH-oCLipEQ)

**Methods:**

Did:key

did:ion

Did:web

Did:snail (snail mail)

Did:pkh

Did:ceramic  
Did:GitHub - web ui  
Did:btcr

Assumptions:  
Wallet  
Authentic  
CLI

Properties:  
Available online  
Comparison

[HTTPS://diddirectory.com](https://diddirectory.com)

What can you do with a did once you have one?

- Christine Webber. Mastodon
- Randy Farmer

More about DIDs

- Syntax
- Did doc
- VCs

Accessible

Why?

How to talk about dids session later

DIDComm  $\approx$  VPN

Wallet out of the box:

- Disco - logon w/ eth
- Web wallet

Lifserver:open-source:creates did:web

CLI: transmute, key, web element, photon  
Web UI - GitHub

DIDs|resolves|Apps|  
VCs as interop data format

did:twitter could be a thing

did:indy provides timestamp lookup of signing keys (rotating keys cause a problem where looking up a current key may not match the key used at the time of signing)

## ***DWP The Decentralized Web Platform***

Session Convener: Dan Bluhm

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

## ***vLEI Ecosystem Governance Framework***

Session Convener: Karla McKenna & Drummond Reed

Notes-taker(s):

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

GLEIF vLEI Ecosystem Governance Framework are listed here: <https://www.gleif.org/en/lei-solutions/gleifs-digital-strategy-for-the-lei/introducing-the-verifiable-lei-vlei>

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

## ***Me2B Spec Intro***

Session Convener: john Wundelich

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

## ***Libp2p***

Session Convener: Benjamin Goering @bengo

Notes-taker(s):

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

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps: No Notes Submitted

## ***User Experience - Making the Metaverse Fun***

**Session Convener:** Jonny Howle DISCO

**Notes-taker(s):** Lauren DelFabro

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

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

Key User Experience Topics/Issues in the SSI Space

- Sharing access to resources (data availability)
  - Access control
  - Selective disclosures
  - Revocation
- Account recovery
  - Key management
  - Recovering credentials
- Delegation
  - Responsibility or authority to sign on your behalf
  - Discovery of who has the authority within an organization/community
  - Time-bound nature of delegation
- Giving informed consent
- Inheritance
  - What happens when you die

On Gathering User Insights and Conducting Research in the SSI Field

User insights

- Many different cultures
  - Some are much less comfortable giving feedback
  - Some user research flows use SMS
    - Do not have smartphones
  - Need a user experience that allows delegation to guardians
- Provide users an environment they already know how to use
  - Mobile app with functionality they are comfortable with
  - Skeuomorphism
    - Use cues from the physical world into the digital space
    - Now mobile has been around long enough
      - The more we use something like chat that people are comfortable with, the more we can study the additive behaviors
      - If you can follow the flow of information across chat for interoperability that can be extrapolated to wallet behavior
      - Same type of flow for verifiable credentials
        - Identity isn't the thing, it's the thing that gets you to the thing



- What you get on the other side of the gating is the user behavior
- Groove (sharing system a number of years ago)
  - Could control
  - First time I got a message from you, I would have to decide if I accepted it or not
  - Means that when you are wanting to open a message, you are asked to validate a user
    - Takes you out of the flow of value you were already following
    - Vs sending a secure link to establish connection so now that's out of the way and when you want to message you can message
      - Same privacy but ordered differently (when you do it makes a difference in UX but has the same outcome)
  - For establishing connection between two parties you may need to add a double opt-in
    - Yellowpages exist so this invalidates the double opt-in
      - You can pick any phone number and call it
        - BUT the person on the other side can decide to answer it or not
    - Granivetter Diagram
      - Set of links of connected parties
      - But there's no way to connect the set of links to other sets of links
    - Ex: web3
      - People leave DMs open on twitter so they can get messages even when they don't confirm the sender
      - Also you can show up differently to different spaces (not just your physical face/presentation)
      - Can think about credential gating based on more than formal fields to be presented
        - ie "if works at X" they are allowed to connect with me
        - Currently based on very weak assurances of credentialing
          - "I introduce myself as a person"
            - Account recovery:
              - How to help people who lose their credentials
                - What if you could designate people who will get a piece of your keys and you get enough of these people together who say yes that's really them
                - If you lose all of your identifiers, then you can't prove yourself
- What if all your guardians lose their credentials too?

seed phrase

- People are afraid of holding their own keys and managing that security themselves
  - You have to make it easy

- Normal twitter users don't really care about privacy
    - "Accept all"
    - Clicking the wrong buttons
    - Trying to move fast
  - How do you win over those people? (Kaye Yee)
    - Make the secure way the easy way
- Privacy Paradox
  - Hypothetical Privacy
    - I care about security
  - Actual Scenarios
    - Discount if they sign up
    - Cookies
- Objective disclosures tell you what you are sharing

Relative disclosures share if this is increasing or decreasing your level of privacy

- The thing that got people to actually take more private decisions:
  - Actual situations where you tell that party they are increasing the amount of data shared with an app
  - Showing in human readable text what they are sharing

Best-in-class in this space

- Intelligent conversational agents (chat bots)
- Trinsic (on issuance)
  - Could actually log in and figure it out
- Logging into zoom meetings
  - Request for a credential for email that will allow you to access
    - QR code to phone
    - It's rough
      - UX could be streamlined
      - Sometimes it works - but often people have to be logged in manually
      - "Don't ask me for 7 or 30 days"
        - Doesn't work

## SESSION #3

### *High-security Use Cases in “passkeys” Era*

**Session Convener:** Kosuke Koiwai

**Notes-taker(s):** Nat Sakimura

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

FIDO, passkey, levels of assurance, passkeys, WebAuthN, multi-device credentials, NIST SP800-63

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

The session discussed about multi-device authenticators, commonly known as “passkey”.

The basic question posed in the session by Kosuke was how an application become aware of the change of assurance level with the introduction of the multi-device authenticator. For this, we needed to know more about the multi-device authenticators, so Time Cappali explained the basics. What we have learned were:

- multi-device authenticators are phishing resistant authenticator like the existing FIDO platform authenticators but is synchronized among the devices so the user experience is improved.
- its target is something better than password though admittedly lower than FIDO 2 security keys.
- Old platform authenticators will not be turned into multi-device authenticators so they are not degraded in terms of security level.
- with the introduction of multi-device authenticators, choices that are available to RPs are Create a multi-device authenticator or stop accepting platform authenticators.

Then a very lively discussion on what change in security properties result from it. John Bradley argued that it is isomorphic to federation but it was argued back. However, it was agreed that security properties are indeed changed from what many organizations have been assuming: keys are not exportable.

Then, we also discussed the implication of a new extension called Device public key (DPK). DPK creates a second public-private key pair to identify the “device”. DPKs can be cleared.

We learned that in a few days three major platform vendors will release multi-device credential capabilities to WebAuthN, which is kind of a password manager of FIDO credentials. It will be very convenient in one perspective, but that means now we can't just assume that FIDO credential is bound to a hardware. If your risk profile is not in favor of this change, then you have to do something such as

asking for another authentication factor. It is happening soon but there is no silver bullet. We also talked about the implication of this change to NIST SP800-63.

<https://fidoalliance.org/white-paper-multi-device-fido-credentials/>

<https://developer.apple.com/videos/play/wwdc2021/10106/>



### ***IIW 101 Session UMA (User Managed Access)***

**Session Convener:** Alex Laws

**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:**

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



# Topics

- Overview in OAuth terms
- UMA in action
- The technical big picture
- The UMA grant
- Federated authorization
- Authorization assessment
- Privacy and “BLT” (business-legal-technical) implications

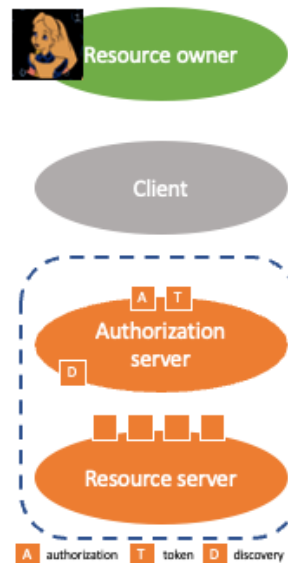
2

## Overview in OAuth terms

OAuth enables constrained delegation of access to apps

Benefits:

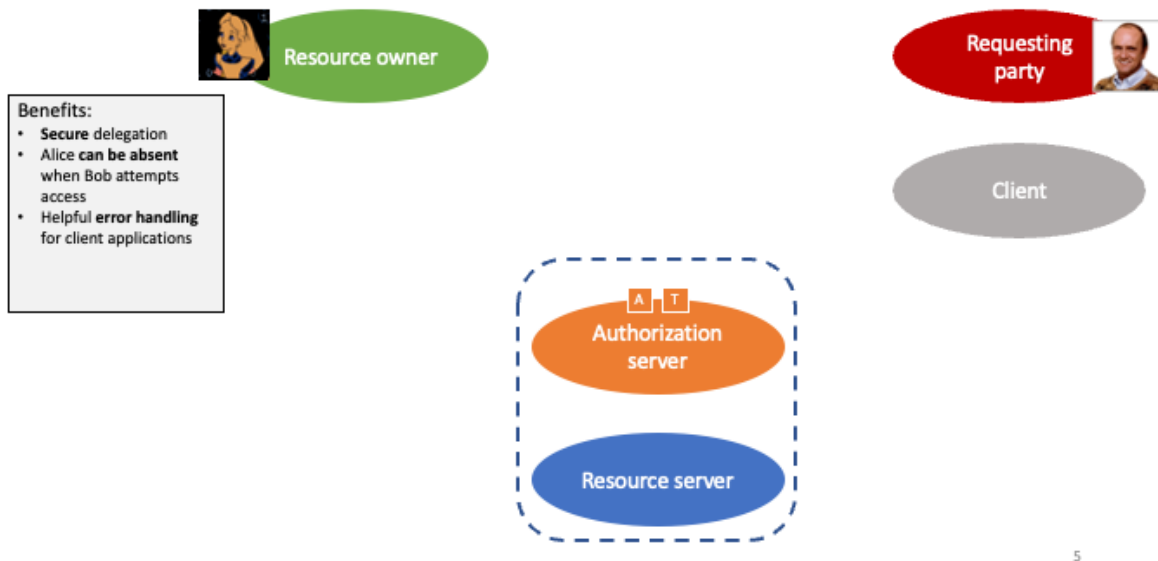
- Flexible, clever API security **framework**
- Alice can **agree** to app connections and also **revoke** them



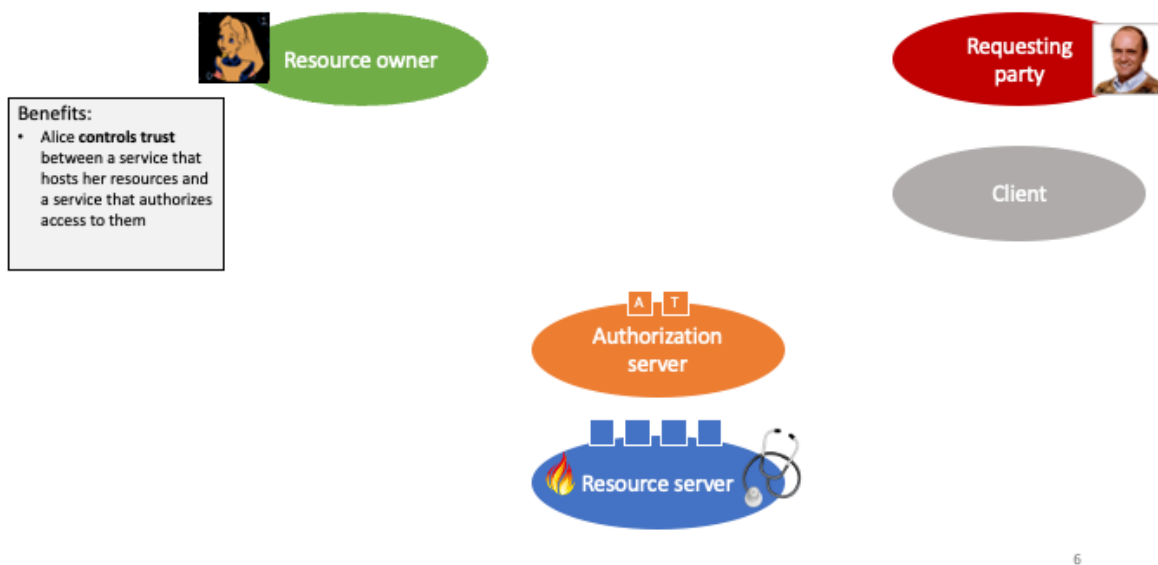
4



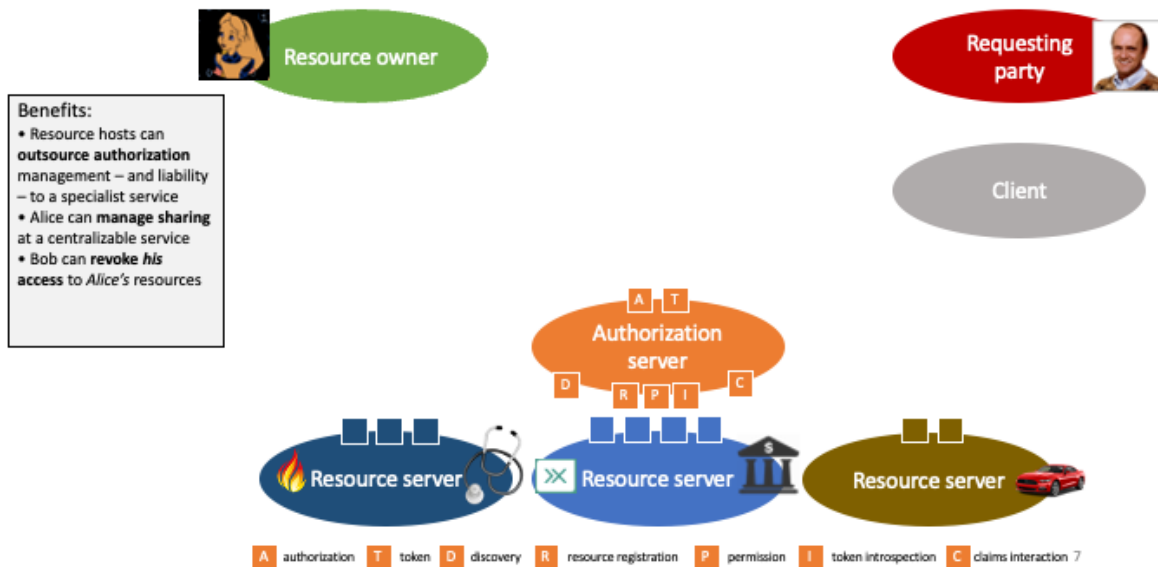
## UMA adds cross-party sharing...



## ...in a wide ecosystem...



## ...of resource hosts

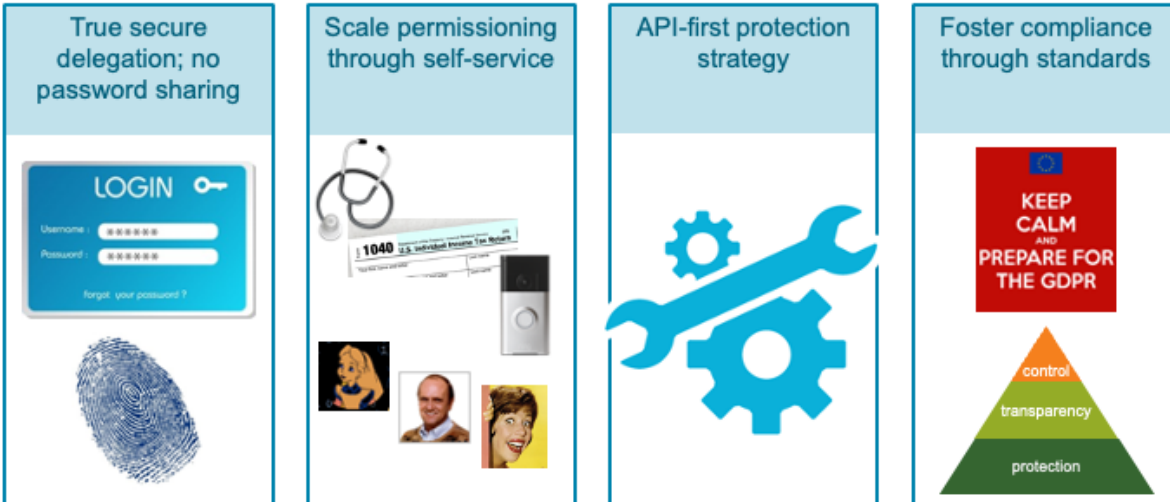


## UMA user experience opportunities



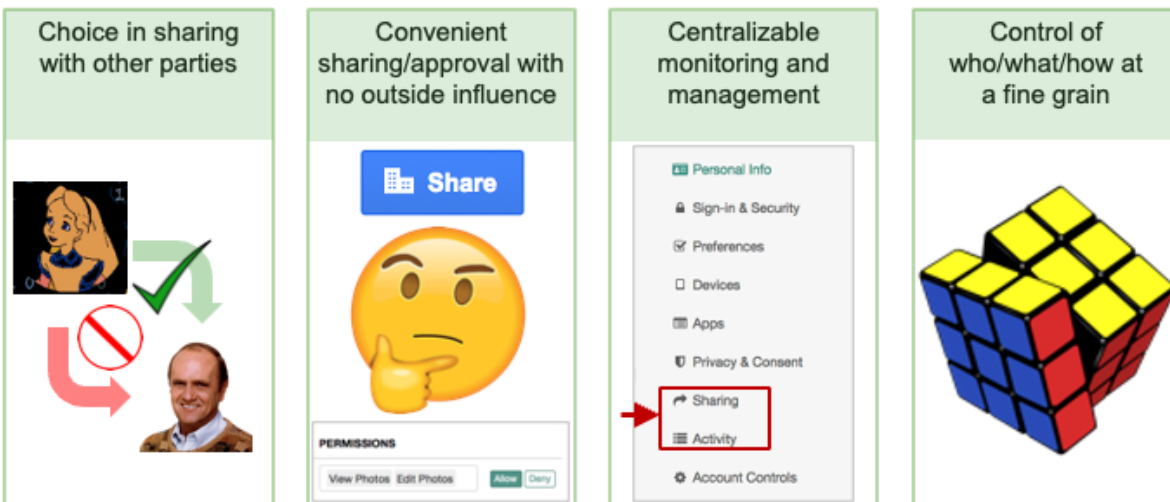
8

## Benefits for service providers: a summary



9

## Benefits for patients and consumers: a summary



10

## Typical use cases

- Alice to Bob (person to person):
  - Patient-directed health data/device sharing
  - Discovering/aggregating pension accounts and sharing access to financial advisors
  - Connected car data and car sharing
- Enterprise to Alice (initial RO is an organization):
  - Enterprise API access management
  - Access delegation between employees
- Alice to Alice (person to self/app):
  - Proactive policy-based control of app connections
- Profiled or referenced by:
  - OpenID Foundation HEART Working Group
  - UK Department for Work and Pensions

11

## Known implementations

(more detail at [tinyurl.com/umawg](https://tinyurl.com/umawg))

- ForgeRock – financial, healthcare, IoT, G2C...
- IDENTOS – healthcare, G2C
- Patient Centric Solutions – healthcare
- HIE of One / Trustee (open source) – healthcare
- Gravitee – API protection, financial
- Gluu (open source) – API protection, enterprise, G2C...
- Pauldron (open source) – healthcare
- RedHat Keycloak (open source) – API protection, enterprise, IoT...
- WSO2 (open source) – enterprise...

12

## UMA in a nutshell

- Developed at Kantara Initiative
  - V2.0 complete in Jan 2018
- Leverages existing open standards:
  - OAuth2
  - OpenID Connect and SAML
- Profiled by multiple industry sectors
  - Financial, healthcare
- UMA business model effort (“BLT”) supports **legal licensing** for personal digital assets
  - Example: Mother (legal guardian) manages sharing for child (data subject); child becomes old enough and starts to manage sharing herself



13

## UMA in action

### PatientShare

A screenshot of the PatientShare authorization interface. At the top, it says 'I, Alice Patient, authorize' next to a circular icon with the letter 'A'. Below this, there are two dropdown menus: 'HealthyMePHR' and 'To disclose my information to Dr. Erica, Lush Medical'. The 'Medical Information' section asks 'Select how you would like to share your medical information' and has two radio button options: 'SHARE ALL information in my medical Record' (which is selected) and 'SHARE SPECIFIC medical data sets'. The 'Consent Term' section asks 'Enter a start and end date during which your medical data will be shared' and shows 'Consent Start 31 May 2017' and 'Consent End 31 December 2019'. At the bottom, there are four buttons: 'CANCEL', 'SAVE', 'SHARE' (highlighted in blue), and 'REVOKE'.

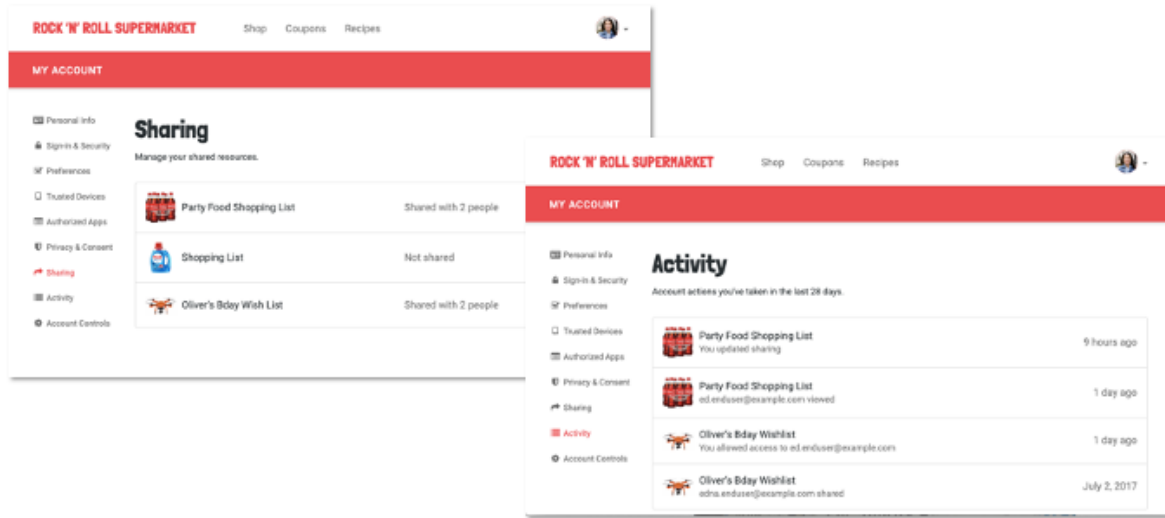
- Patient Alice creates a policy to share with Dr. Erica, she selects her sharing preferences, and presses SHARE

SHARE

- Patient sharing is easy!

15

# ForgeRock Identity Platform

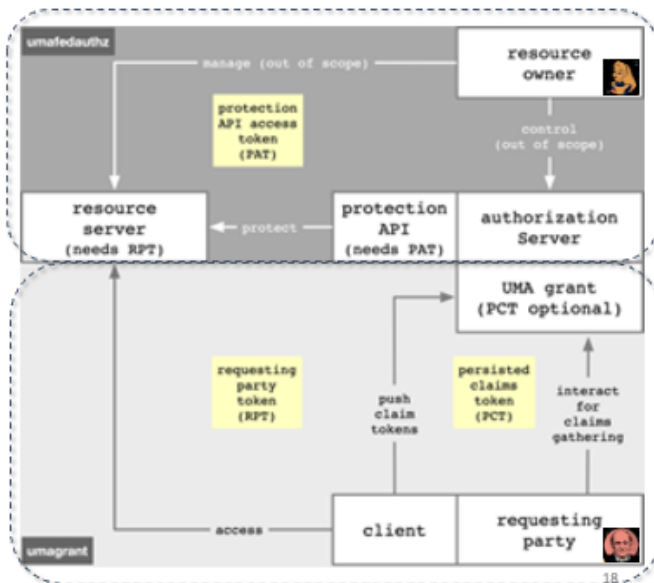


16

## The technical big picture

### The marvelous spiral of delegated sharing, squared

1. The **UMA grant of OAuth** enables Alice-to-Bob delegation
2. **UMA standardized an API for federated authorization** at the AS to make it centralizable
3. There are **nicknames** for enhanced and new tokens to keep them straight





## The UMA extension grant adds...

[docs.kantarinitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html](https://docs.kantarinitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html)

- **Party-to-party:** Resource owner authorizes protected-resource access to clients used by requesting parties
- **Asynchronous:** Resource owner interactions are asynchronous with respect to the authorization grant
- **Policies:** Resource owner can configure an AS with rules (policy conditions) for the grant of access, vs. just authorize/deny
  - Such configurations are outside UMA's scope



19

## UMA federated authorization adds...

[docs.kantarinitiative.org/uma/wg/rec-oauth-uma-federated-authz-2.0.html](https://docs.kantarinitiative.org/uma/wg/rec-oauth-uma-federated-authz-2.0.html)

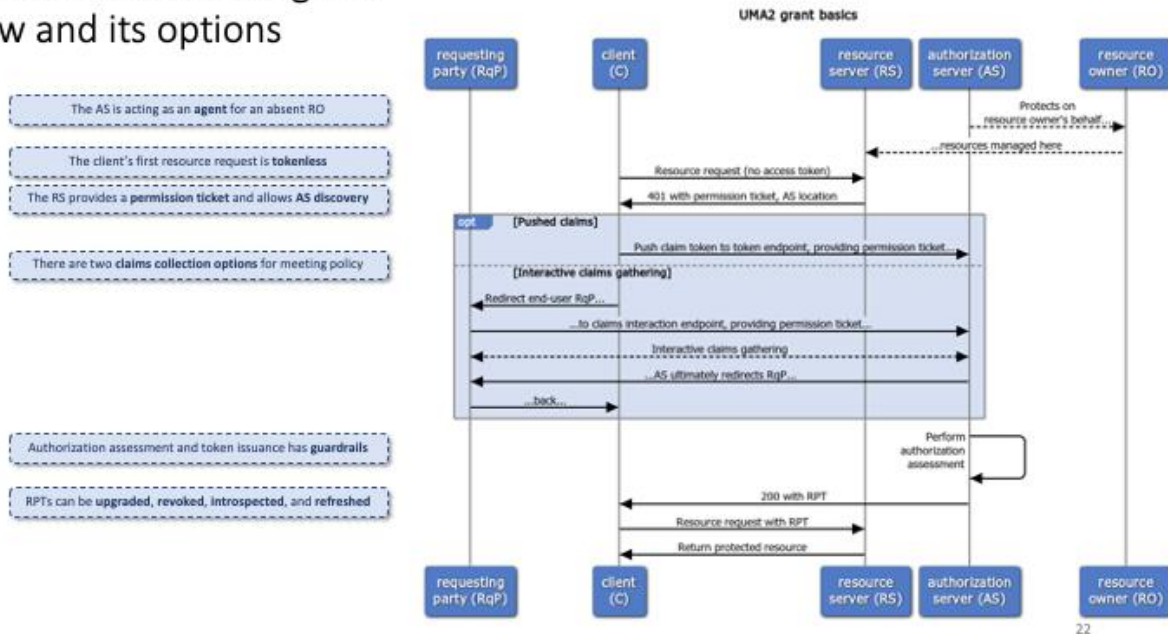
- **1-to-n:** Multiple RS's in different domains can use an AS in another domain
  - "Protection API" automates resource protection
  - Enables resource owner to monitor and control grant rules from one place
- **Scope-grained control:** Grants can increase/decrease by resource and scope
- **Resources and scopes:** RS registers resource details at the AS to manage their protection



20

## The UMA grant

## The UMA extension grant flow and its options



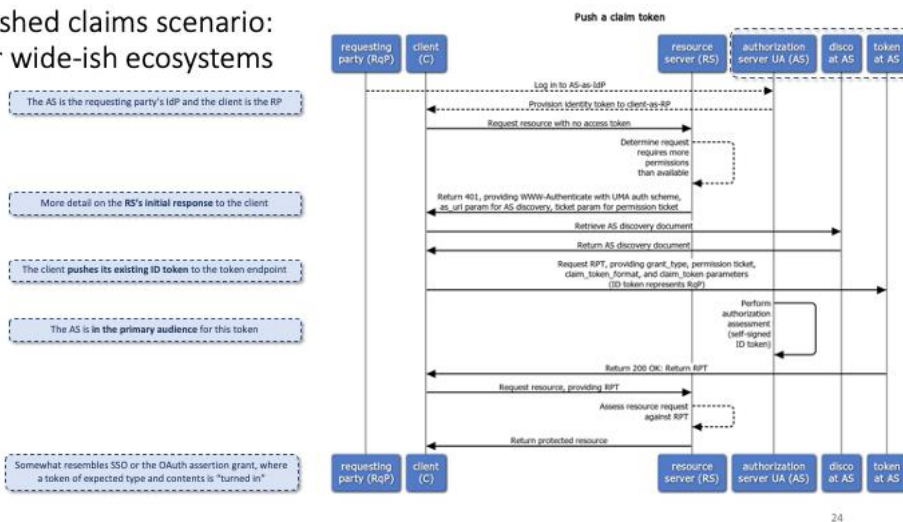
22

## The permission ticket: how you *start* building a bridge of trust

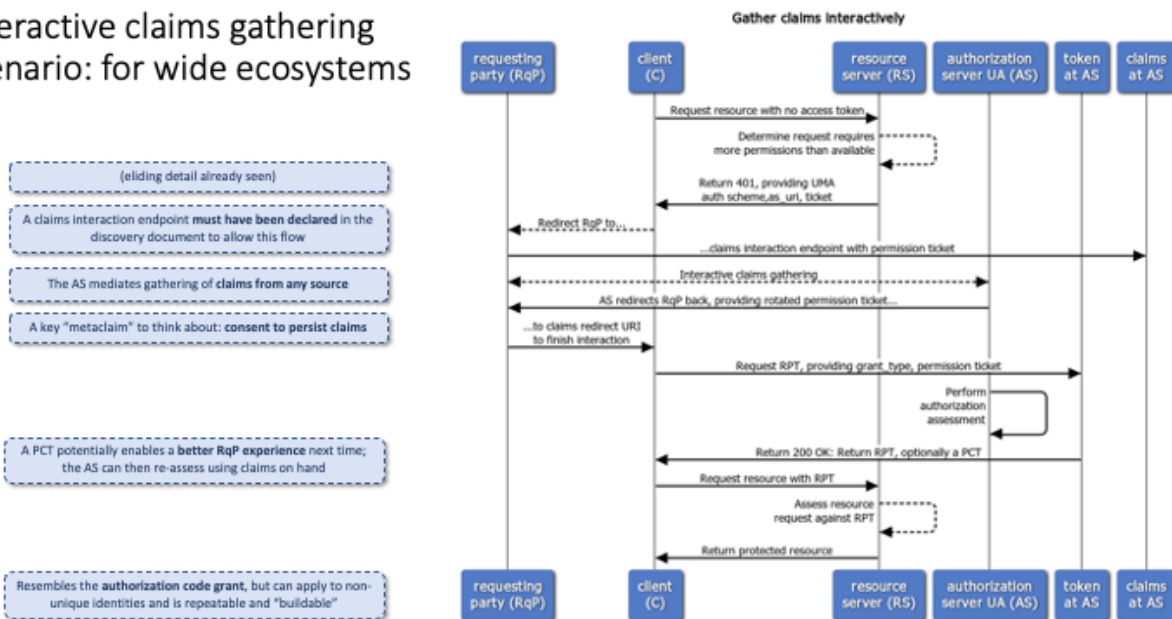
- **Binds client, RS, and AS:** Every entity may be **loosely coupled**; the whole flow needs to be bound
  - It's like an overarching state parameter or "ticket-getting ticket"
  - Or maybe even a bit like an authorization code
- **Refreshed for security:** The client can retry RPT requests after non-fatal AS errors, using either claims collection option of the grant flow
  - The AS **refreshes** the permission ticket when responding with such errors

23

## Pushed claims scenario: for wide-ish ecosystems



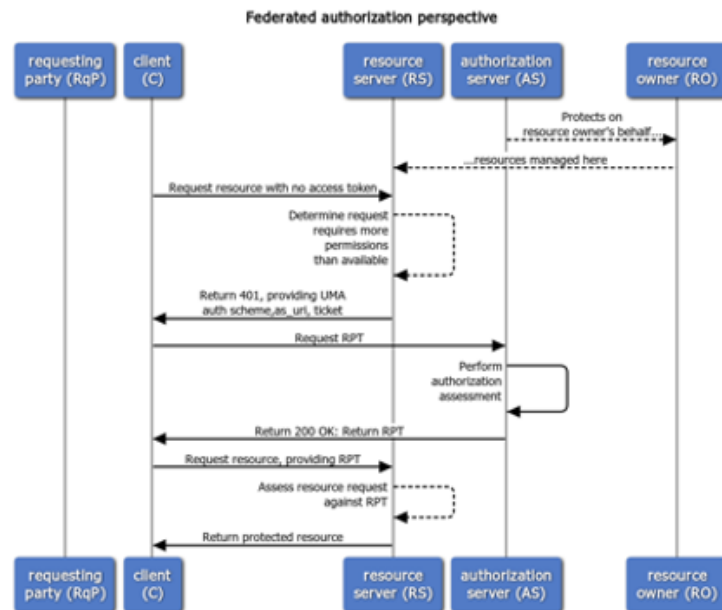
## Interactive claims gathering scenario: for wide ecosystems



# Federated authorization

## A new perspective on the UMA grant

- How does the AS know when to start protecting resources?
- How does the RS know what ticket the AS is associating with the RS's recommended permissions?
- Is there anything special about token introspection?
- Let's standardize an interface at the AS for these jobs



27

## The protection API: how you *federate* authorization

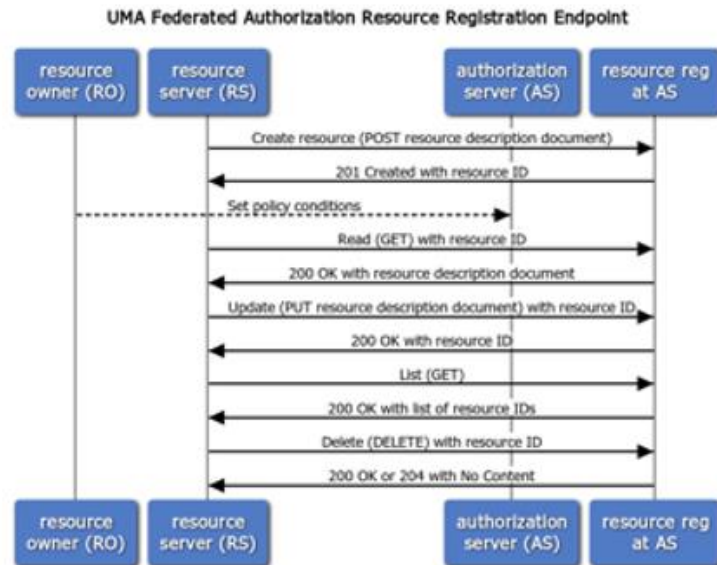
- **RS registers resources:** This is required for an AS to be “on the job”
  - Scopes can differ per resource
  - Resource and scope metadata assist with policy setting interfaces
- **RS chooses permissions:** The RS **interprets** the client’s tokenless resource request and **requests** permissions from the AS
  - The AS then issues the initial permission ticket
- **RS can introspect the RPT:** UMA **enhances** the token introspection response object
- **RO controls AS-RS trust:** The protection API is **OAuth-protected**
  - The resource owner authorizes the scope `uma_protection`
  - The issued token is called the **PAT**



28

## The resource registration endpoint

- Registering a resource puts it under protection
- Setting policies can be done anytime after creation
- Deregistering a resource removes it from protection



29

## Resource and scope registration

- The RS is authoritative for what its resource boundaries are
  - It registers them as JSON-based descriptions
  - There is a resource "type" parameter
- Scopes can be simple strings or URIs that point to description documents

**Create request:**

```

POST /rreg/ HTTP/1.1 Content-Type: application/json
Authorization: Bearer MHg3OUZEQkZBMjcx
...
{
  "resource_scopes": [
    "patient/*.read"
  ],
  "icon_uri": "http://www.example.com/icons/device23",
  "name": "Awesome Medical Device Model 23",
  "type": "https://www.hl7.org/fhir/observation.html"
}
  
```

**Response:**

```

HTTP/1.1 201 Created
Content-Type: application/json
Location: /rreg/rsrcl
...
{
  "_id": "rsrcl"
}
  
```

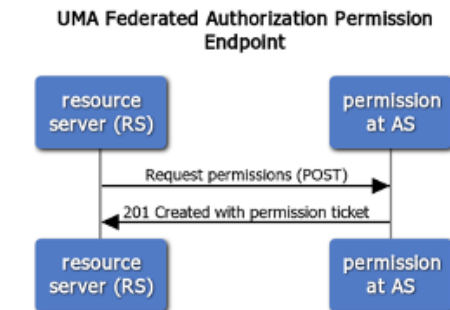
30

## The permission endpoint

- The RS interprets the client's tokenless (or insufficient-token) resource request
- The RS must be able to tell from the client's request context which RO and AS were meant

**Request:**

```
POST /perm/ HTTP/1.1
Content-Type: application/json
Host: as.example.com
Authorization: Bearer MHg3OUZEQkZBMjcx
...
{
  "resource_id": "rsrcl",
  "resource_scopes": [
    "patient/*.read"
  ]
}
```



**Response:**

```
HTTP/1.1 201 Created
Content-Type: application/json
...
{
  "Ticket": "016f84e8-f9b9-11e0-bd6f-0021cc6004de"
}
```

31

## The token introspection endpoint

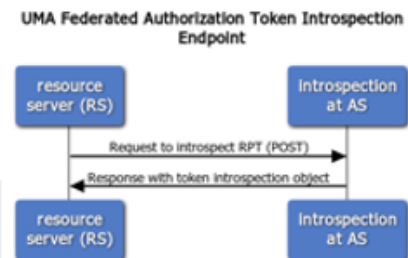
- UMA enhances the token introspection response object
- A permissions claim is added, with resource ID-bound scopes

**Request:**

```
POST /introspect HTTP/1.1
Host: as.example.com
Authorization: Bearer MHg3OUZEQkZBMjcx
...
token=mF_9.B5f-4.1JqM
```

**Response:**

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
...
{
  "active": true,
  "exp": 1256953732,
  "iat": 1256912345,
  "permissions": [
    {
      "resource_id": "rsrcl",
      "resource_scopes": [
        "patient/*.read"
      ],
      "exp": 1256953732
    }
  ]
}
```

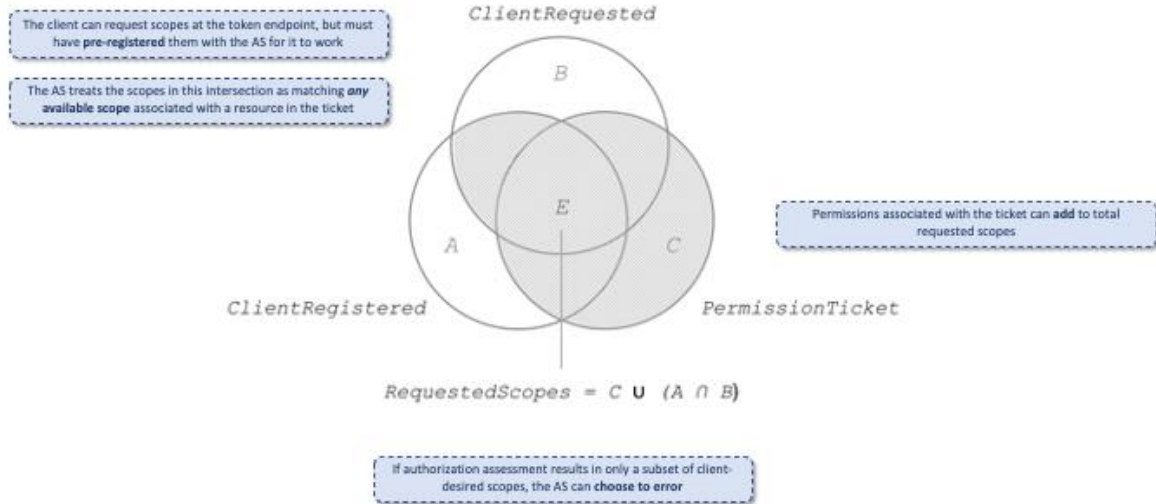


32

# Authorization assessment



## Authorization assessment: how the AS adheres to the RO's wishes in the larger context



34

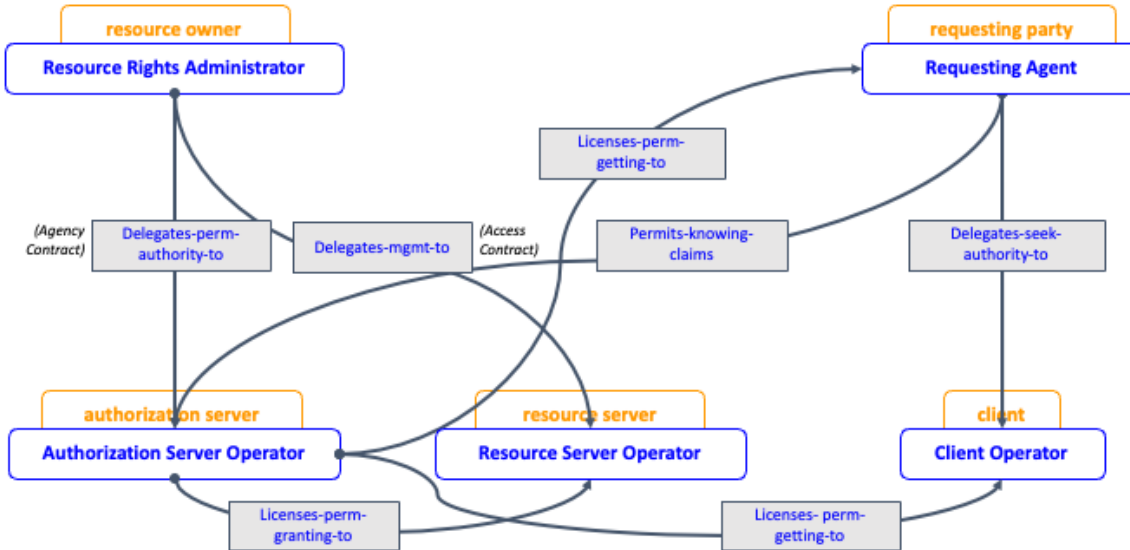
## Privacy and “BLT” implications

### Relevance for privacy

- Features relevant to privacy regulations (GDPR, CCPA, OB, PSD2, CDR, HHS ONC info blocking rules...):
  - Asynchronous resource owner control of grants
  - Enabling resource owner to monitor and manage grants from a “dashboard”
  - Auditability of grants (consent) and PAT-authorized AS-RS interactions
- Work is well along on an UMA business model
  - Modeling real-life data-sharing relationships and legal devices
  - Technical artifacts are mapped to devices
  - Goal: tear down artifacts and build up new ones in response to state changes

36

## (Most) legal relationships in the business model



37

## UMA implications



38



Join us!  
Thank you!  
Questions?

Alec Laws, Kantara Initiative UMA Work Group chair  
@aleclaws | @UMAWG | [thylurl.com/umawg](mailto:thylurl.com/umawg)  
IWWXXXIV | 26 Apr 2022  
[kantara.org](http://kantara.org)

## ***Control Channel for Identity on the Internet - DIDComm***

**Session Convener:** Sam Curren

**Notes-taker(s):** Sam Curren

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

Roughly equivalent slides to discussion: [https://hackmd.io/mDVthuA\\_Sa2sVBVsImD2cA](https://hackmd.io/mDVthuA_Sa2sVBVsImD2cA)

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

## ***How to think about DIDs***

**Session Convener:** Joe Andrieu

**Notes-taker(s):** Antonio Antonino

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

Three different domains with three different trust models:

### **Verifiable Data Registry**

Sovereign System State Management, e.g. Bitcoin, Ethereum, Mastercard.

They do not care about anyone else, and do not want to depend on other systems for any of their functions

### **DIDs**

Use resolver to communicate with the verifiable data registries

Let applications access the state on the verifiable data registry

### **Applications**

Use DIDs as identifier method

The wallet is the point of connection between all 3 domains.

*Q: Where does the trust get established?*

1st trust element is in the resolver to return the ACTUAL document for a DID

The app should run its own resolver, and the resolver should be public and inspectable  
2nd trust element is what DID methods to trust in which application domain

The DID method Rubik can be used as an evaluation matrix depending on the use case requirements

## ***Global Assured Identity Network PoC 101***

**Session Convener:** Torsten L

**Notes-taker(s):**

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

<https://de.slideshare.net/TorstenLodderstedt/gain-presentationpptx>

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

Intro to the vision of GAIN, what nonprofits contribute, open for other nonprofits to join and contribute

Goal of the PoC community group: evaluate and demonstrate technical feasibility of GAIN vision

First IIPs integrated and tested for interoperability

Now working on integrating RPs

Further topics: trust management of the network, other services, different identity protocols

## ***25 Billion Password Compromised - Preventing Account Takeover Using Open ID***

**Session Convener:** Tom Sato

**Notes-taker(s):** Tom Sato

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

[Guide to Shared Signals](#)

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

### **1. What is SSE**

Shared Signal and Events is a communication framework for two parties to share status and security alerts to protect digital identity

Transmitter and Receiver establish secure and continuous communication line starting is OAuth handshake.

It's a secure Webhook so that transmitting IDP can let receiver, usually webapp that after login authentication, should IDP find security breach like password compromise, it can send security warning during session or even out of session.

SSE has two sets of Security Event Token (SET) specification CAEP and RISC.

2. My idea is to two parties, usually two IDPs to share security alerts when IDP-1 end user finds password compromise and changes the password and let IDP-2 know that this password has been deleted and remediation is necessary.
  1. Issue 1. In order to make certain that IDP-1's end users' password is the same as IDP-2's, IDP-1 needs to send a password in plain text, in order to verify that deleted password at IDP-1 is the same as IDP-2.
  2. Sending plain text password, even if it was deleted in plain text is a bad idea and compliance and privacy policy would not allow this to happen.
3. To do this, my idea is to create a verification token out of password that is obfuscated and encrypted using a key that is supplied by middleman. Because of obfuscation, it can't be decrypted back to the original password. If the obfuscation and the encryption is done by same key and method, then IDP-1 can send this verification token to IDP-2 and comparison can be made.
  - A. Why do you need a token used as a key? Why not use industry standards hashing mechanism instead of a token?
  - B. IDP-1 may not have the deleted password in plain text to convert to verification token.
  - C. Do you have to store the verification token at IDP-2 until the end user actually make a login?
  - D. Why it is important to check both the user ID and the password?
  - E. How a password comparison can be made secure and privacy preserving?

## ***What if You Had All Your Personal Data in a Single Place You Control? Demo & Discussion***

**Session Convener:** Johannes Ernst

**Notes-taker(s):** Sean Bohan

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

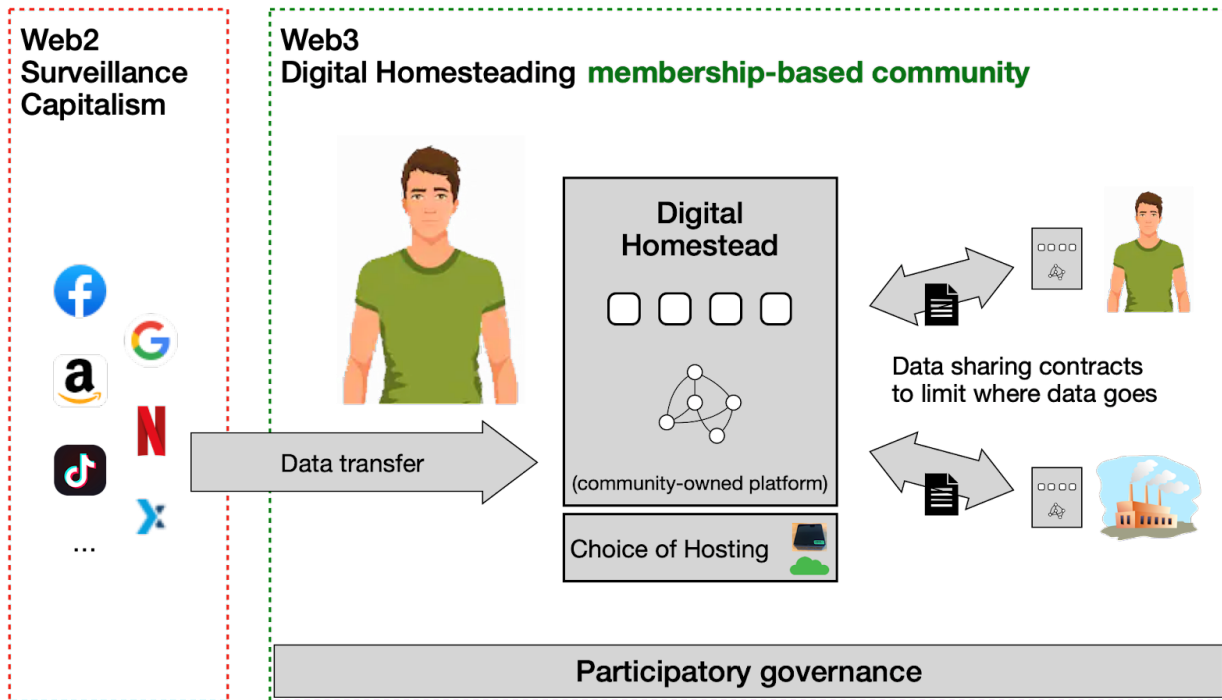
<https://ubos.net/mesh> – what we discussed

[acesstracker.org](https://acesstracker.org) – tracks issues we are finding in company's data access implementations (bugs, omissions,...)

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

**Key slide:**

# Personal data *jiujitsu*



Johannes Ernst

Start a revolution

2 slides

Privacy legislation

Right to access personal data

Legal right, go to any company "give me all the data you have related to me"

EU, US (CA, VA, etc.)

Incredible right, few know about it

In theory - take all the data that exists about you, taken against will in many cases, get hands on it

When you get it - JSON files, not human readable, completely useless (FB example)

Given this, it is unusable what you get

UBOSS Personal Data Mesh

Tech preview, platform, UI, in front to see what's there

DEMO

Not what end user will see - demo

Website - runs on laptop, you as the user decide where to run it (like Wordpress)

Don't have to trust a host

Import data from var places

example: real data, hard to make dummy data

Data categories: fb, amazon, google data

Photos to FB, got them back (if closed an account doesn't lose them)

Data took and put into Personal data mesh

Search your own posts from the past

Full text search

Enter data by category or search

Search "printer", get examples from FB posts and Amazon purchases

Great for transparency

AMZ must upload all advertisers that target you with ads

Advertisers on FB who have uploaded his PII to target him

Pluggable

Bot



Put piece of code (as a dev) sits on transaction log “can I do something interesting with that” - this example is categorizing inbound data

All the American car companies want to advertise to him

Cars targeted from Texas dealers (wasted on him in CA)

FB knows he bought something from Albertsons, but how are they connected? Can’t find the connection between the two

Albertsons doesn’t have data on him

\*Maybe\* FB is buying data about him? But what?

Another bot - when data gets imported, has something about a person, attempts to create address book

Superset of all people he knows

Useful - single best info about people he knows

Parse the email (currently don’t do) -single most useful dataset about you AND it is under your control

Plan - coop - own and govern the system built around this data so no one company takes that data and turns into something evil

Users and vendors - decide collaboratively what should happen

More to say

If YOU had all this data about yourself - what would you want to do with it

If YOU had a customer with this data, and could run an app to access it, what kind of value could you provide to your customer

A lot of this data is unobtainable today

Jeff - how you ingest this data? Adapters for each source?

JE: process is novel, tech involved diff for every single company - auth, identification, real ID challenges around it

Turns out Consumer Reports Digital Lab and MIT: Data rights protocol - hope to turn this into an API and put into regulatory frameworks

EU going in that direction (automate data-out)

Early - not productizable YET

Tech preview

If you go to UBOS.net/mesh - telegram group and access to code, docker demo, build it

Import data right now is command line (geeks for now)

Diagram

Core platform

Converter and difference that allows differential import

Add-on

Blaine WIZARD - platform to store this - home server on RaspPI, socially active social network

Have interests, share interests, find connections (bicycling and chocolate)

Scenario of interacting peer to peer

Icebreaker protocol

Non disclosed common interest algo (see WIZARD)

Innovations currently not possible - find people with similar interests requires FB to create (middleman)

Local innovation

Require to delete that data

Copyright on data with DMCA markers

JE: I have a slide on that :) Digital homesteading

Step 1 - data transfer (import/export/delete/corrected)

Step 2 -share with people and companies, limit where data goes, data sharing contracts, negotiated

Wants personalized services, but can’t . IF they will agree to a data sharing contract

Choice of hosting

Rasp-PI, cloud, coop, commercial provider

Needs participatory governance, needs a community

Internet today - club of values and rules

Identify a set of people “I will do this differently” - tech, transactional standards, safe subset of the internet - new guy “this sounds appealing”, might get more high quality data

Set of all communities - many many sub

Overall ruleset

Business want this, get great branding boost and more data

2022 - we can do this, couldn’t have done this 5-10 years ago

Jeff - cool, get public won’t give a damn, don’t appreciate how much data is out there about them

What if they are incentivized to share and control the data

JE - opinions have changed in recent years (76% say FB is bad for society), high % think American companies not taking care of the data

Bigger thing missing in market - someone showing it could be different - how this will work end to end

Not complete yet

Q - most people don't care, more they don't have control, know what to do, friction so high to do this, what's missing is the tokenomics, reward, people will adopt if there is a reward, can determine who I want to sell it to - another concern is storage

JE: tokenomics - whole thing is highly contested space,

Blaine - could be part of my platform

Q - look at life point and storj, all of this data it is decentrally stored, drive mass adoption, who has my data, know it is secure and trusted

JE - these storage options will emerge -

JE - if you think I am making sense - I want to hear from you and you tell me what you think the interesting thing is here

Q - thoughts - importing as frictionless as possible, web2 will continue over time - what is the method of constant exchange

JE - accesstracker.org - collecting problems with conformance, to your point about incremental -

Q - single point of failure - onus of security is on the individual

JE - many eggs in the same basket is a problem, what we can do here is if you have a choice of host, a host can take care of all of this

Blaine - you need digital ownership of the data - need to sign to say "its mine!"

Q - going from export yourself you don't need verifiability - putting out will require verifiability

JE - who is the source of authority here? Work to be done

Q - trust not mentioned here - why should I trust you, etc. Trust takes time - will all participate? There has to be a right balance, trust and incentives and convenience and redundancy, need choices

JE - may decide somewhere in the future - a directory of services - interesting part - hopping arrow - becomes easy to move homestead from one to another - where all connections you have remain intact

Blaine - I want to share my photos with people in the photos, sharing model underneath is something to talk about

JE - mesh base - in memory multi paradigm graph-centric DB with explicit semantic models, native sharing protocol over didComms - have a graph, correlated and included into one body of integrated data, share a subset -

Blaine - need shared semantic models

Q - share the data and then misuse the data -

JE - trying to figure out what the governance should be

Come up with initial set of mechanics so the whole things doesn't fail

Small set of predefined contracts - can see a reason why I want shoe store to do with my purchase data

Blaine - how do you grow your model? "M-F-X on passports" example. How will that protocol and model evolve

Q - applied to health? Opportunity? Structuring so it can be accessed

JE - bunch of vert use cases, stuff you own, transferring your stuff to next generation - put machine learning into this,

JE - L-apps

## ***Reinventing Digital Identity - Consumer Merchants & Regulators***

**Session Convener:** Parul Sharma

**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

## Where are the Complete EcoSystems?

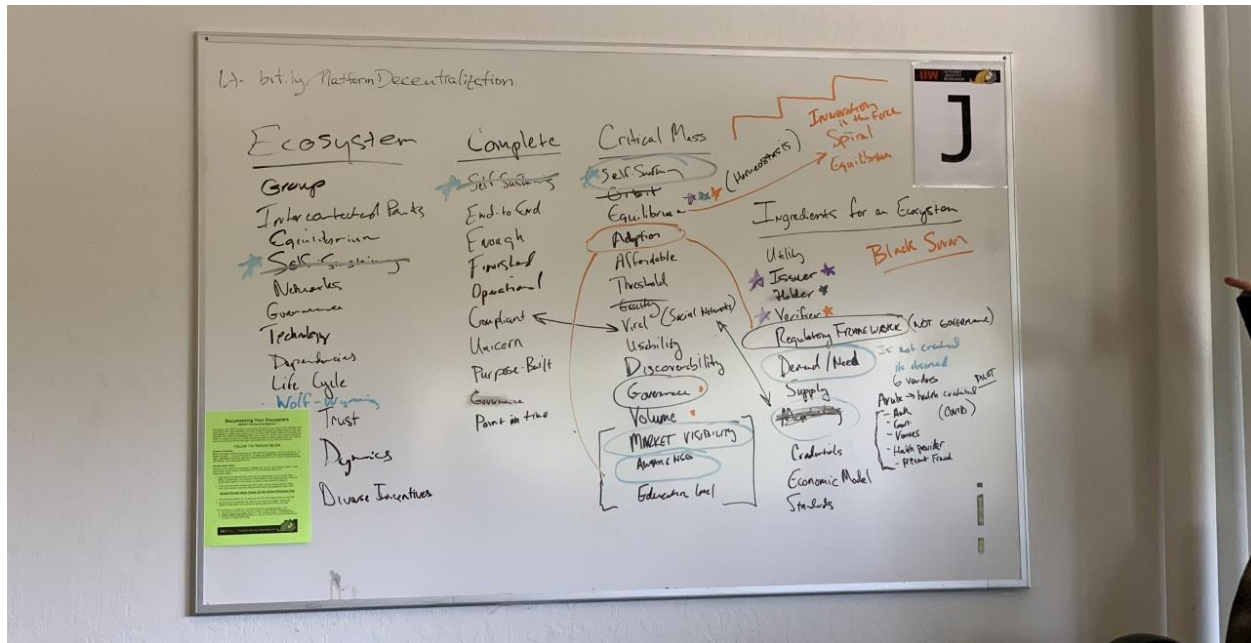
Session Convener: Marty Reed

Notes-taker(s): Peter Langenkamp

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

<https://drive.google.com/file/d/1d2lxQ6J0XXU0aAXJ0oZv6xYEGnnnox8G/view?usp=drivesdk>

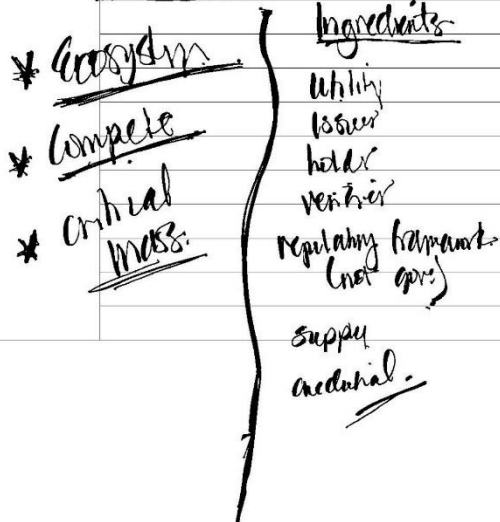
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:



Where are the complete ecosystems?

Ecosystem

Self-sustaining



Complete Ecosystem

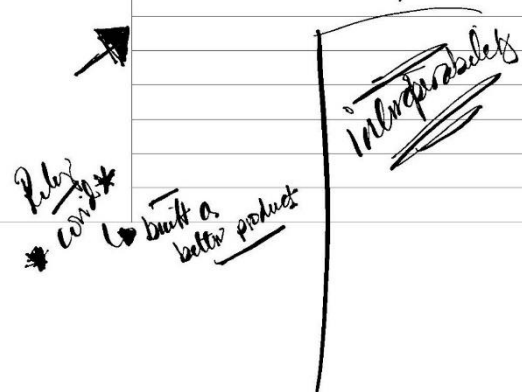
Demand/need

Regulator

Adversary

Adoption - product / comp

Self-sustaining - product



Complete Eco.

demand/need

gap between

"live with the problem"

Solution - need

ecosystems

extensive

Apple

manual on

problem

over time

\* Machine that agreed! \*

Economic Model

regul.

\* Revenue  
\* Reduce  
expenses!  
\* headache  
\*

Nimble

Wagging  
crosses - merged  
reset the balance  
equilibrium

Black Swan.

Well defined.  
demand yields  
issuer holds  
venture.

new quote

\*

~~demand isn't created it's \*~~  
~~observed..~~

BEUBA

health used  
airport

→ cred format  
incentive

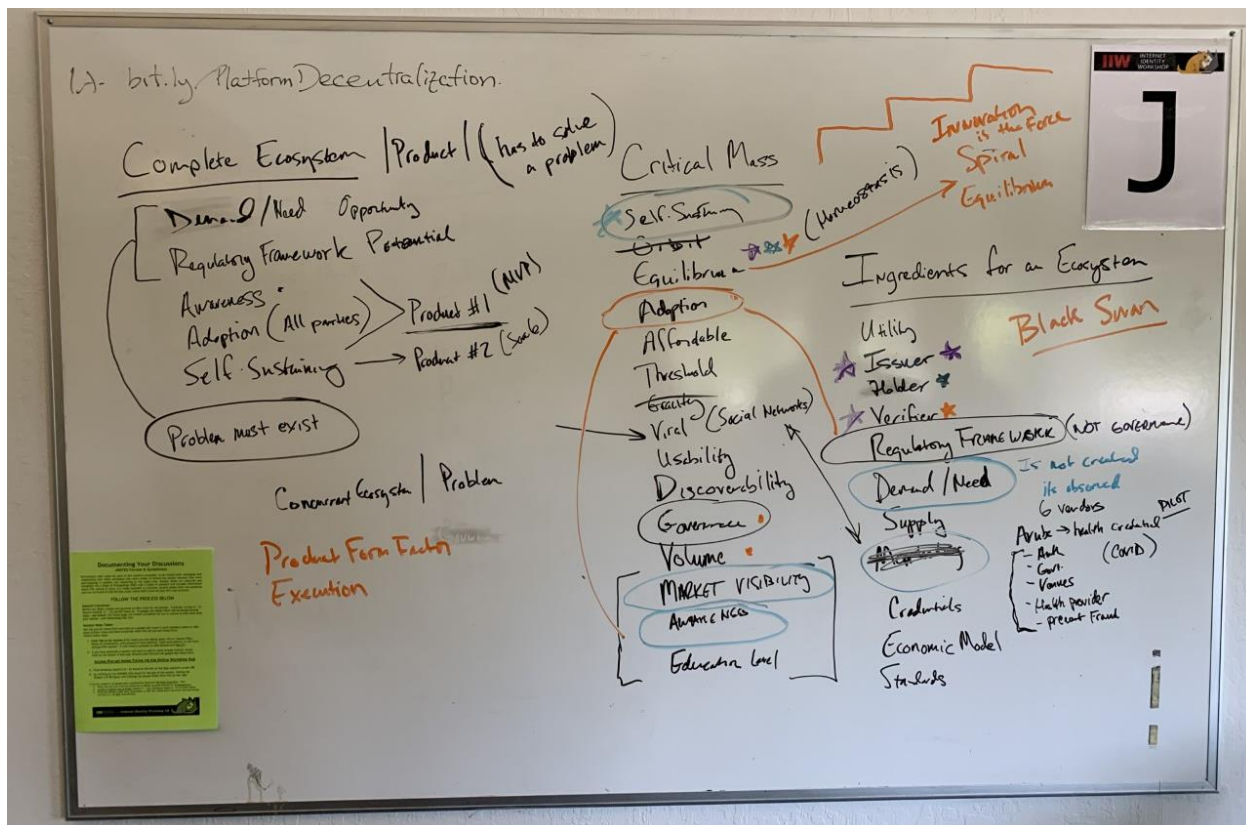
loophole  
fraud

local revenue →  
govt → what into

Trusted Travel

2 cranked revenue





### Session 3 - Where are the complete ecosystems?

Ecosystem (brainstorm)

- group
- Interconnected parts
- equilibrium
- self-sustaining



- governance
- networks
- technology
- dependencies
- lifecycle
- wolf-wyoming
- trust
- dynamics
- diverse incentives

#### Complete (brainstorm)

-----

- self-sustaining
- end-to-end
- enough
- finished
- operational
- compliant
- purpose built (fit for purpose)
- governance
- point in time

#### Critical mass (brainstorm)

-----

- self-sustaining
  - Orbit x
  - equilibrium (homeostasis)
  - adoption
  - affordable
  - threshold
  - gravity x
  - viral
  - usability
  - governance
  - volume
  - market visibility
  - awareness
  - education level
- Move 'self-sustainable' (category of it's own?)

#### Ingredients for an ecosystem

-----

- issuer
- holder
- verifier
- regulatory framework (not governance)
- demand / need (is not credential ...)
- supply
- awareness
- credentials
- economic model

- standards

Black Swan event

Example of use case on Aruba got off the ground by first coming to an agreement with all parties involved

- Health care providers
- Government
- Venues
- six vendors involved in total
- two issuers, two verifiers
- prevent fraud

Complete ecosystem [build a good product] (someone needs to build a product that people like)

-----

- demand / need [opportunity]
- regulating framework [potential]
- Awareness | - [MVP]
- Adoption (all parties) | - [MVP]
- self-sustaining [scale]
- problem must exist

When covid hit, lots of parties started building systems for covid

- 90% failed
- the ones that succeeded, built a better product
- market-made

## ***Consensus - Do We Agree on What it Means to Agree?***

**Session Convener:** Aaron D Goldman

**Notes-taker(s):** Richard Esplin

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

Link to Slides

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

### Context

Let's use a blockchain!

But do we really need one?

When do we need consensus?

What type of consensus do we need?

### Additions to Content in the Slides

Levels of consensus:

Durable = Crash Fault Tolerant

Majority & Finality = Byzantine Fault Tolerance

\* Overlapping quorums such that  $1/3 - 1$  can be unreliable.

Conflict-free Replicated Data Type CRDT

\* Allows a consistent view without finalizing on the total order.

\* Comes at a cost of discovering new data that hasn't been incorporated.

Blockchain consensus / Nakamoto consensus is not actually final. In practice it works, but in theory a different chain could be discovered that is actually the longest chain.

Summary: when you are thinking about non-locality, stop talking about how long it takes to have consensus. Instead be specific about the time necessary to achieve the various states of consensus (local, durability, majority, finality), and expose this information to the application layer so that the user can aware of where their transaction is in consensus: (Local, Durable, Majority, Final)

Unanimity is distinct in theory from Finality, but in practice applications only care about when the transaction is unlikely to be reversed (Durable, Majority, or Final).

Though applications are usually interested in Finality, most of the time there are no cheaters, and we can move forward with Majority consensus that is much faster to achieve. But the application should be able to roll-back the transaction in the rare circumstances where Finality is not achieved.

If your application gives a Majority result without preventing Equivocation (the same node giving different answers to different queries), then the data is only Crash Fault Tolerant.

We need to ask ourselves if our application's goals can be achieved with a lower level of consensus.

Other useful properties of consensus:

\* Conflict detection

\* Recording the history

\* Non-repudiation

When you say "I need a ledger" ask yourself "what is the resource you are trying to mutually exclude". Because if you aren't trying to mutually exclude anything, you don't need a ledger.

Example SQL databases that use autoincrement(ROWID) force a level of slow consensus that isn't needed. Instead you can use unique(ROWID) and it would be far faster.

\* You don't actually need total ordering, you just need a unique ID.

The provided consensus time matrix is as estimate based on reasoning:

\* Local transactions only take a few clock cycles.

\* Durable transactions require communication across the network with another machine in the datacenter, or in another region.

\* Majority transactions require a two way commitment between distributed nodes.

\* Finality transactions require a three-phase of nodes across the globe.

When doing state-machine replication, you could even reduce complexity be only implementing solutions for Local and Final.

## SESSION #4

### *ACDC for Muggles - Authentic Chained Data Containers NO WIZARDS!!!*

**Session Convener:** Drummond Reed and Sam Smith

**Notes-taker(s):**

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

[https://docs.google.com/presentation/d/1mO1EZa9BcjAjWEzw7DWi124uMfyNyDeM3HuajsGNoTo/edit#slide=id.ga411be7e84\\_0\\_0](https://docs.google.com/presentation/d/1mO1EZa9BcjAjWEzw7DWi124uMfyNyDeM3HuajsGNoTo/edit#slide=id.ga411be7e84_0_0)

### *IIW 101 Session / All About SSI*

**Session Convener:** Kaliya Young

**Notes-taker(s):** slide deck

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

Link To slide deck: <https://docs.google.com/presentation/d/1QiETJ-VD8RiWj-AhnhH3RRnrkWiEqA-iLGLsu4rWQ/edit?usp=sharing>

### *Introducing the Spritely Networked Communities Institute: Re-Decentralizing Online Communities*

**Session Convener:** Randy Farmer / Contact: [randy@spritely.institute](mailto:randy@spritely.institute)

**Notes-taker(s):** Randy Farmer

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

<http://spritely.institute> [IIW Spritely Presentation](#) [Longer version of presentation...](#)

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

IIW's leadership in identity and verifiable data is critical, but it's also about behavior (or what others can do with it,)

The Spritely Institute is working to make it all possible (see the presentations above for a preview)

## ***Web Browsers + Identity Flows***

**Session Convener:** Heather Flanagan

**Notes-taker(s):**

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

<https://www.w3.org/community/fed-id/2022/04/21/introduction-to-federated-identity-and-the-fedid-cg/>

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

Group discussed how to identify an identity flow to a browser given that identity flows and tracking flows use the same underlying primitives (e.g., cookies, link decoration, and redirects). One idea was to prevent two-way flows such that the user would go to the IdP, but that the return would be restricted in some manner.

## ***What Credential Format is the Best?***

**Session Convener:** Torstan L

**Notes-taker(s):** Antonio Antonino

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

- Requirements
- Selective disclosure, offline usage, contains claims to identify people, crypto agility, anti-correlation capabilities
- Options

### **Anoncreds**

Advantages: Most mature widely used privacy-preserving credential format used today.

Downsides: Tied to a specific ledger, it does not work offline unless data is cached. It is not yet recognized as a standard, but currently under IETF standardisation led by Steven Curran.

### **LD-proofs**

Can support selective disclosure and unlikable presentations. Generally smaller than Anoncreds, and embed the schema inside the proof, so the schema does not have to live on any blockchain.

### **ISO mDL**

Supports selective disclosure with salted hash mechanism. It is indeed an ISO standard (162 pages), so it went through a lot of reviews by different regulatory bodies. Actual authorities such as US DMVs are already issuing credentials using this standard.

Presentations are correlatable, and there is no de-facto revocation mechanism.  
There are two operating modes: device retrieval (mandatory) and server retrieval (optional).

#### **JWT**

Widely implemented and supports a lot of different cryptographic primitives. Based on IETF specs widely security reviewed. Does not support selective disclosure.

#### **VC-JWT**

Enhances JWTs by letting the credential being issued to the holder instead of to the relying party directly. Does not support selective disclosure either.

#### **JWP**

Goal is to have a simple JSON-based claim representation w/ support for selective disclosure, kinda like an improvement over JWTs. There is a BBS variant of it.  
In general, there are two classes of JWPs, ones that support single presentation (very simple to build) and ones that support multiple unlinkable presentations.

#### **Hash & salt JWT/JWP**

Supports selective disclosure but not unlinkable presentations. It would make more sense to talk about hash & salt JWP rather than JWT, since JWT was not designed for selective disclosure. Advantage would be that, beyond building a layer on top to deal with the selective disclosure, existing JWT libraries can be used to deal with this class of credentials.

#### **CWT**

Similar advantages as JWT, with the advantage that the size is smaller, albeit it requires more code for parsing. mDL uses CWT as its primary representation. EU covid pass is a CWT. It is a standard by IETF. It supports the same algorithms as JWT, minus the deprecated ones.

### ***The ByWay Local - First ECommerce Without BigTech Giants***

**Session Convener:** Doc Searls

**Notes-taker(s):**

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

Slides:

<https://docs.google.com/presentation/d/1LpmuSgQbxKxWRooTllvqaDj7StvusonE/edit?rtfpof=true&sd=true>

## ***On-Chain Application of DIDs (did:sol & Cryptid)***

**Session Convener:** Martin Riedel

**Notes-taker(s):** Phillip Shoemaker

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

**Links:**

<https://github.com/identity-com/sol-did>

<https://github.com/identity-com/cryptid>

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

Martin gave a conceptual overview of the topic:

did:sol is a program on Solana to manage DIDs and their representative state on Solana. There is a resolver library (and unisolver integration) for did:sol to allow easy integration for OFF-CHAIN Use-Cases.

Furthermore identity.com developed and deployed a program on Solana (Cryptid) that allows to access and verify the SAME state from the did:sol to execute any ON-CHAIN Solana Transaction through Cryptid.

Next to DID-State evaluation Cryptid plans to be extended with dynamic Middleware that could add additional verification logic to on-chain transactions (e.g. spending limits, and others).

**Discussion:**

- Is that a good idea? Yes, but the reference to the state on chain should probably not referred to as DID (In Cryptid it's "Cryptid Address")
- Bringing the On-Chain / Blockchain community together with the SSI / off-chain identity community.
- DID specs would also be shaped by on-chain requirements. For example Verification Methods should maybe contain a property if key ownership was proofed when a key was added to a DID.

**Image:**





## ***DIDs + Directories of Trust / Machine-Readable Governance File Basics***

**Session Convener:** Gabe Cohen and Mike Ebert

**Notes-taker(s):** Gabe Cohen and Mike Ebert

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

<https://hackmd.io/@mikekebert/HJBQH-SBc#/>

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

Three main questions:

1. Are you who you claim to be? (and how can we tell)
2. Are you to be trusted for x? (and how can we tell)
3. How do we represent trust lists?

One Approach:

Machine Readable Governance Files published by the “sovereign” entity over a jurisdiction

1. List trusted DIDs
2. List roles
3. Assign roles to DIDs
4. List actions
5. Assign roles to actions

Now you can see which agents the jurisdiction trusts, what actions are available, and what each agent is supposed to be doing.

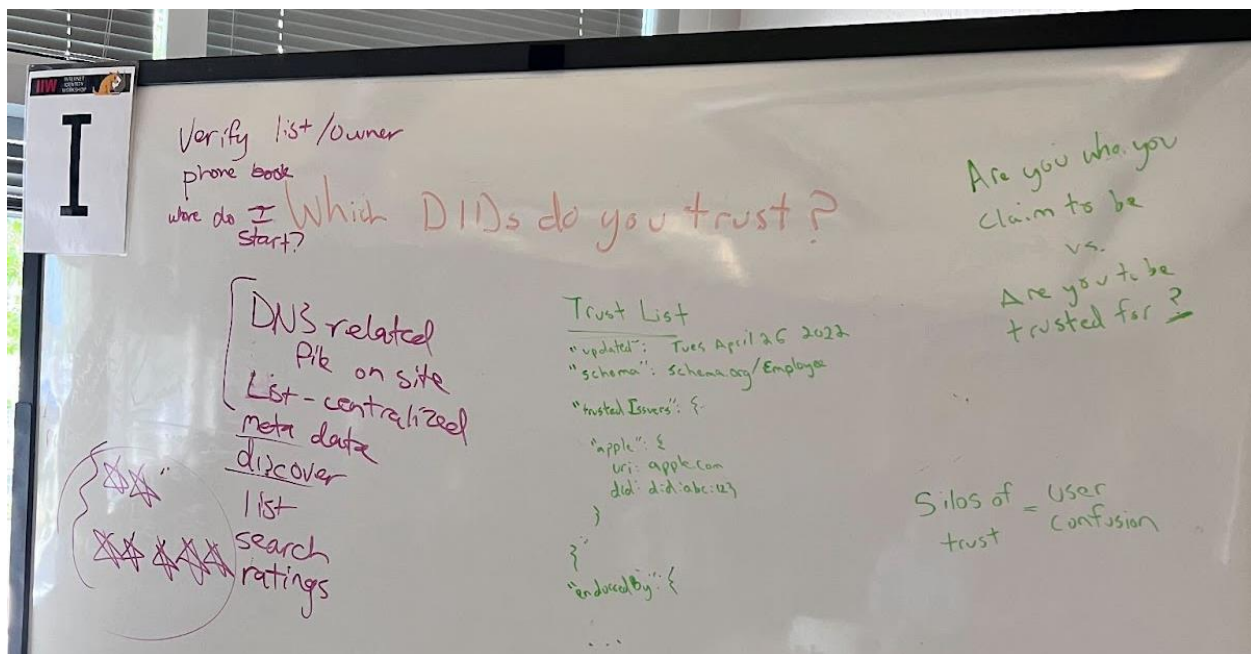
Indicio and SITA implemented a first version of machine readable governance files for the nation of Aruba

- COVID use case
- JSON-LD format

Need to include or stand up other mechanisms of trust: credentials, competing lists or opinions, endorsements, ratings

Need to publish, discover, categorize, list, search, share, distribute governance files

Work will continue in the DIF Claims & Credentials working group to create a standard for 'governance files'.



## Data Monetization

Session Convener: Haydar Majeed

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

## ***SHOW ME the MONEY!!! A Conversation on PD&I Commercial Models /***

**Session Convener:** Michael Becker

**Notes-taker(s):** Michael Becker

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

The talk primarily revolved around our need to have “big tent” multi-party discussions that can focus on the not just the tech, the moving of the bits and bytes around, but also:

- The problems being solved
- Value propositions
- The need to understand the flows of money

Suggestions for why business models and commercial models are not being discussed:

1. People have no clue about the answer
2. Those that have a clue, proven answers, don't want to share. They won't share until they've pulled out all the value from their secret sauce.

## **SESSION #5**

### ***ACDC (Wizards) Authentic Chained Data Containers***

**Session Convener:** Sam Smith, Phil Fearheller, Kevin Griffin

**Notes-taker(s):**

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

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

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

## ***JSON Web Proofs (JWP)***

**Session Convener:** David Waite (DW), Michael B. Jones

**Notes-taker(s):** Michael B. Jones

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

DW explained the representation format

- Payloads separated by ~ characters

- Claims ordered based on issuer metadata

Two kinds of use cases

- Ongoing relationship with issuer

- No ongoing relationship with issuer

There are two kinds of JWPs

- Single use JWPs, which enable correlation if used multiple times

  - Can use standard cryptography, such as ECDSA signatures with P-256

- Multiple use JWPs

  - Use pairing-friendly curves to prevent correlation with multiple uses

Question about differences between "proofs" and "signatures"

Brent Zundel said that a signature is a kind of proof but some proofs are not signatures

- You can prove knowledge of the signature itself

- For instance CL proofs

Tobias Looker described receiving something in an issued form and adding a presentation header

- JWPs issued to the holder are augmented with a presentation header for presentation to a verifier

The same issuer and signature algorithm are used for all payloads

- Attendees said that anoncreds can be used to combine multiple tokens from different issuers

Examples in the spec

- Single-use JWT using ECDSA with P-256

- BBS signatures

GitHub Shortcut

- <https://jwp.tools>

Three specifications

- JSON Web Proof: [https://json-web-proofs.github.io/json-web-proofs/examples\\_tooling/draft-jmiller-json-web-proof.html](https://json-web-proofs.github.io/json-web-proofs/examples_tooling/draft-jmiller-json-web-proof.html)

- JSON Proof Token: [https://json-web-proofs.github.io/json-web-proofs/examples\\_tooling/draft-jmiller-json-proof-token.html](https://json-web-proofs.github.io/json-web-proofs/examples_tooling/draft-jmiller-json-proof-token.html)

- JSON Proof Algorithms: <https://json-web-proofs.github.io/json-web-proofs/draft-jmiller-json-proof-algorithms.html>

Tobias discussed link secrets

- He said their usefulness depends upon what you're trying to solve

## Standards Status

Currently in DIF Crypto WG

Plan to take it to the IETF this year

Will probably need a new working group

A goal is clear separation of the security and application layers

## ***Introduction to the Trust Over IP Foundation (ToIP)***

**Session Convener:** Judith Fleenor, Director of Strategic Engagement Trust Over IP Foundation

**Notes-taker(s):** Judith Fleenor

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

[www.trustoverip.org](http://www.trustoverip.org)

<https://www.linkedin.com/company/trust-over-ip-foundation/>

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

The Trust Over IP Foundation, a Joint Development Foundation project within the Linux Foundation. Trust Over IP is a member organization with 300 corporate members and over 100 individual members. We are an international collaborative community jointly creating specifications, recommendations, whitepapers and guides to assist governments and organizations embarking on the creation of interoperable Trust Frameworks.

In this session, Judith Fleenor Director of Strategic Engagement covered:.

- What is the Trust Over IP Foundation?
- Trust Over IP Dual Stack
- Types of work products ToIP creates
- Organizational structure for collaborative efforts
- How to get involved?
- Q & A

ToIP Mission: to simplify and standardize how trust is established over a digital network or using digital tools. We focus on BOTH...

Interoperability and cryptographic verifiability at the machine layers.

AND human accountability at the legal, business, and social layers.

### **What is ToIP?**

- Collaborative Community
  - International Community meetings happen in various time zones via Zoom.

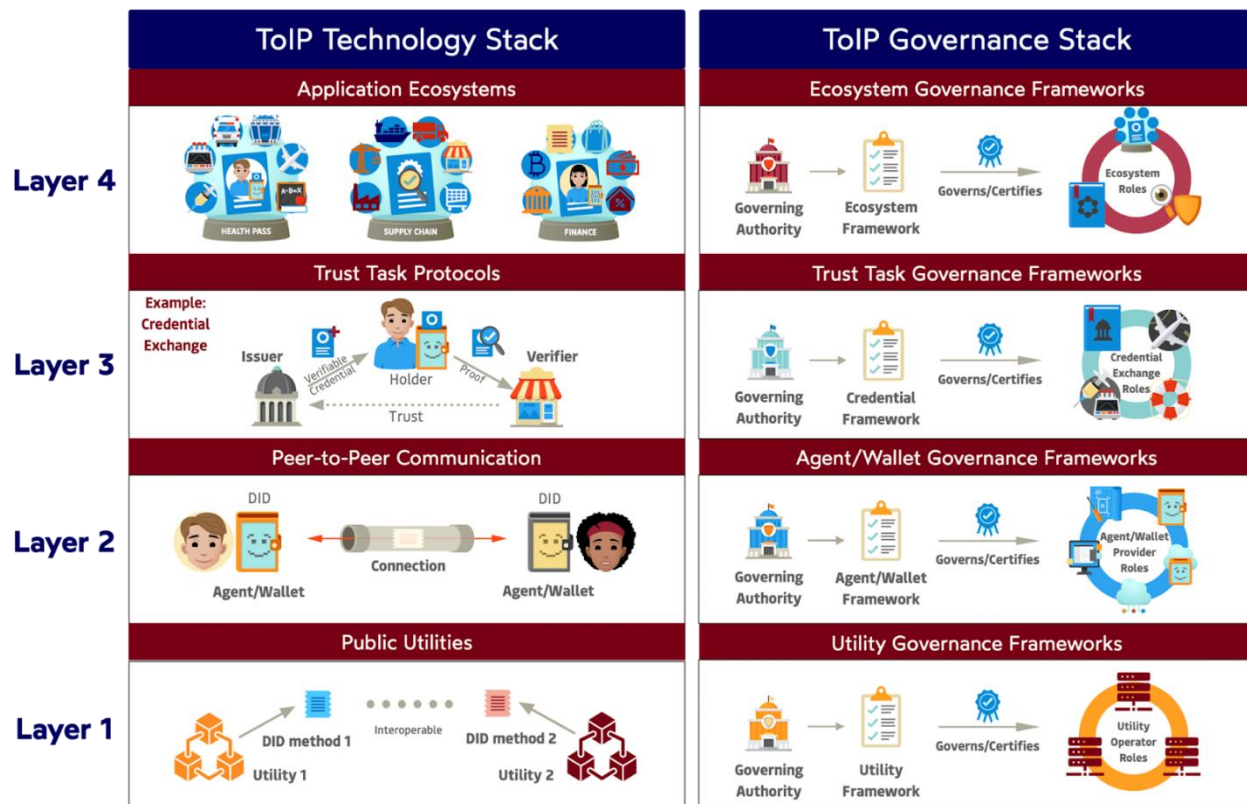


- Asynchronous collaboration via Google Docs and GitHub and the ToIP Slack Workspace.
- It is both for Industry experts and people new to decentralized identity.
- Joint Development Foundation (JDF) project within the Linux Foundation (LF)
  - The JDF is the standards development organization within the Linux Foundation open source community with connections to ISO and other standards bodies.
  - Linux Foundation and the JDF is our fiduciary to manage the ToIP funds and provide the legal structure for the foundation.
  - Linux Foundation provides the infrastructure for our work and is known for collaborative processes.

## Why ToIP?

Because **Trust** is not just about Technology.

- For Digital Trust to be deployed and widely adopted the technology must be trustworthy, but so must the human relationships - business, legal and social.
- Enter the ToIP Four Layer **Dual Stack** ...







## ToIP Work Products

The Work of the ToIP Working Groups is meant to create deliverables!

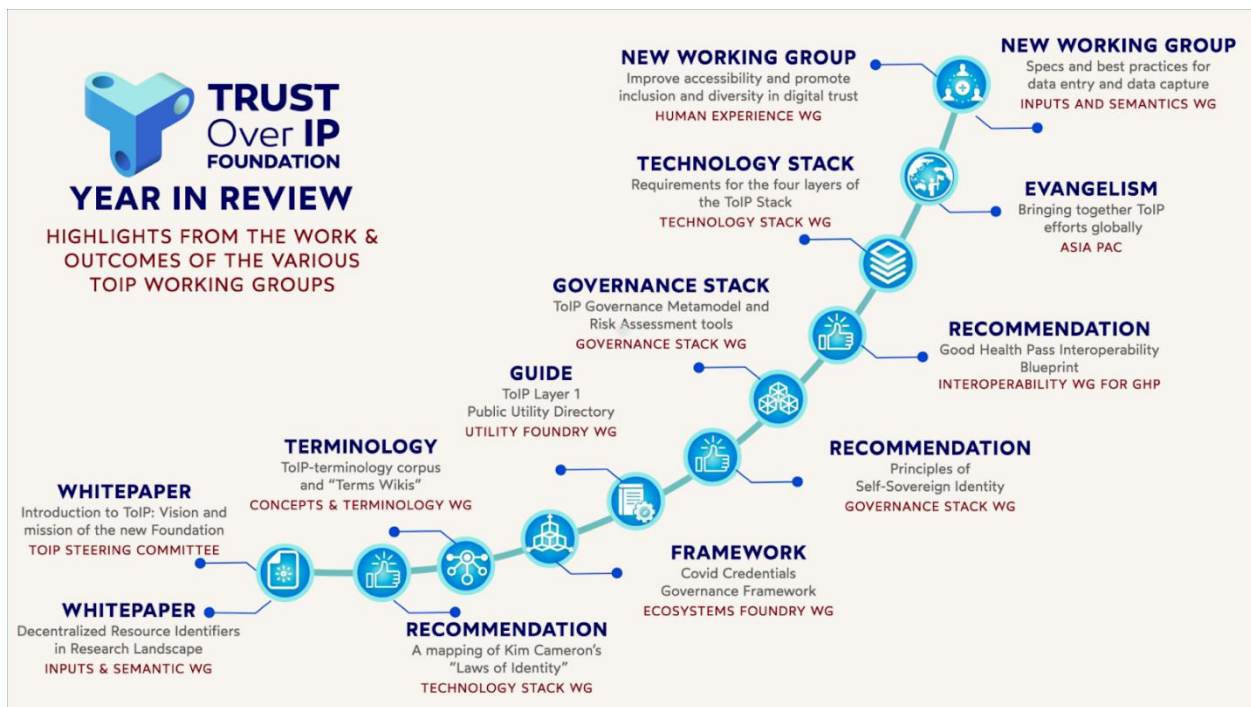
**Yes** - to have interesting conversation and meet intelligent people who are up to changing the Digital Trust Landscape!

**Yes** - to learn and invent new things through the synergy of being together in this space!

But the work of the working groups is  
**primarily to create deliverables!**

## ToIP Work Products

1. Specification – that can be implemented in code
2. Templates – that can be instantiate as documents
3. Definitions – that can be can be incorporated by different organizations
4. Recommendations –that can be that can be followed
5. Implementation plans - that can be executed
6. White Papers – that can be understood to clarify complex issues in the Self Sovereign Identity and Verifiable Credentials space



# ToIP Working Groups

**Primary**

1. Governance Stack Working Group
2. Technology Stack Working Group
3. Utility Foundry Working Group
4. Ecosystem Foundry Working Group
5. Inputs and Semantics Working Group
6. Concepts and Terminology Working Group

**Special Purpose**

Interoperability Working Group for Good Health Pass (GHPC)

**New**

Human Experience Working Group



## How to engage

---

- Joining Trust Over IP is easy
- Go to our website

<https://trustoverip.org/get-involved/membership/>

- Select the membership level that fits your interests.

## How to get Involved

There are three levels of membership at Trust Over IP.

### LEVELS OF MEMBERSHIP

- Contributor Level
- General Membership Level
- Steering Committee Level



## How to get Involved

### **Contributor Level**

This is for companies, organizations, and individuals who want to contribute to our work products by getting involved in one of our various working groups or task forces.

Whether you are new to decentralized digital identity and verifiable credentials or a veteran identity and access management professional who is interested in working with other experts to define and build the future, there is a place for you.

At the contributor level there is no charge and you do not need to join the Linux Foundation.

**Skills Needed:** Writers, Designers, GitHub Experts, Bloggers, experts in Governance Frameworks, those who like to deep dive into inputs and semantics, terminology, and human experience issues.

If you have an interest, there is a place for your contributions.

## How to get Involved

### **General Membership Level**

This is for companies who want to show their support to the work of the Trust Over IP Foundation and get recognized as a part of the movement to build a digital trust layer for the internet that is both privacy enhancing and preventing data risk for organizational entities.

General Members have the same access to be involved in the work products as the contributor level with that added advantage of having **logo placement on our website** and being recognized as a financial contributor to the mission.

There are fees associated and your organization must also be member of the the Linux Foundation.



# How to get Involved

## Steering Committee Level

This is for organizations that want to be a part of the strategic direction of the organization and to be seen as driving change. Steering Committee members have the ability to become voting members of the Trust Over IP Foundation.

There are fees associated and your organization must be a member of the Linux Foundation.

## Steering Committee

accenture

ANONYME LABS

Avast

BRITISH COLUMBIA

CERTIZEN  
TECHNOLOGY



chiway



esatus

FUTUREWEI  
Technologies

IBM

IdRamp

LG CNS

Liquid Avatar™  
TECHNOLOGIES INC.

Lumedic



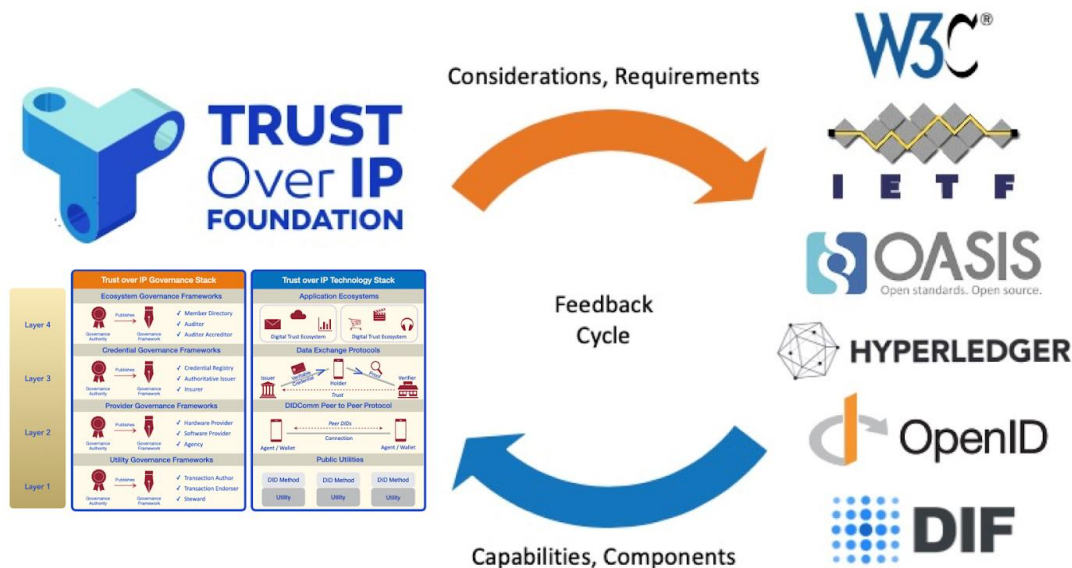
MITRE

schellman  
Quality. above all.

SICPA

Trust is the  
lubrication that  
makes it possible  
for organizations  
to work.

*Warner Bennis*



The Trust Over IP foundation works with other organizations. We are here to replace, but to augment and build the minimum viable specs for interoperability for a digital layer of trust.

Upcoming objectives:

- More Government's involvement
- Specs on a ISO track

## ***euCONSENT - Interoperable, Anonymised online Age Verification Across Europe***

**Session Convener:** Iain Corby

**Notes-taker(s):** Iain Corby

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

[www.euCONSENT.eu](http://www.euCONSENT.eu)

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

The **European Union** has funded a consortium of universities, researchers, tech companies and age verification providers (through their trade body [www.avpassociation.com](http://www.avpassociation.com)) to develop interoperability across age verification providers.

This 18 month project concludes in August 2022. It has already run a **successful pilot** across 5 countries with 1600 adults and children successfully re-using previously completed age-checks, even where these were performed by a different AV provider from the one serving the age-restricted online service they wish to access.

**The network mirrors eIDAS** - the European digital identity scheme. When you complete an age check the providers drops a suite of first-party cookies from a domain on which the AV provider is a sub-domain. The cookies just let other AV providers - each their own sub-domain - know that a user has previously completed an age check to a particular level of assurance, and if that was recent enough e.g. 4 hours, not to prompt re-authentication for lower risk use-cases.

If the check is older than the determined period e.g. 4 hours, then the user is re-directed to the AV provider where they already completed a check, and re-authenticates. That AV provider then confirms to the second AV provider (currently using SAML because eIDAS does), that the user is old enough to access the service (just a “yes” or a “no” - not the actual age or date of birth or estimated age range). If the use-case is higher risk than the existing check, the new AV provider prompts the user to create a new age check to a higher level of assurance as required.

To make this work, we needed to define **standardised levels of assurance**, so AV providers can re-use apples as apples and pears as pears. We have 5, mirroring the identity standard in the UK, GPG45.

We also need a trust framework, with **AV providers audited and certified** before they are admitted to the network, to confirm their data privacy, security and the rigor of the age checks is sufficient.

AV providers need to reach **bilateral commercial agreements** before they can re-use each other's age checks.

We are now considering how to take this forward. Technically we would like to upgrade to **Open ID Connect** not SAML. We need to keep pace with eIDAS as it becomes a wallet itself. And we need a governance framework to maintain the standards and apply the ethical principles such as ensuring all AV providers and their clients are supporting the **UN Convention on the Rights of the Child**. This makes this network a **public good** meriting government support.



## ***Build an SSI Proof of Concept in 30min or Less***

**Session Convener:** Riley Hughes

**Notes-taker(s):**

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

During the session, we built several proofs-of-concept using Trinsic's easy-to-use SSI platform.

The tutorial for doing your own <30 min proof-of-concept, the same one we followed in the session, can be found at this link: <https://trinsic.notion.site/Build-an-SSI-Proof-of-Concept-dae9d6e565eb4770be41b61d55e090cb>

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

## ***godiddy.com***

**Session Convener:** Markus Sabadello and team

**Notes-taker(s):** Markus Sabadello

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

DIDs, Universal Resolver, Universal Registrar

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

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 (<https://uniresolver.io/>) and Universal Registrar (<https://uniregistrar.io/>).

### **godiddy.com Component: Universal Resolver**

The Universal Resolver enables the resolution of many different types of DIDs using a common interface. It offers an HTTP(S) binding to the DID Resolution function, which is defined in the W3C CCG's DID Resolution specification.

The Universal Resolver can return DID documents in various representations (JSON, JSON-LD, CBOR), as well as full DID resolution results (DID documents, plus metadata).

Besides resolving DIDs, another supported function is dereferencing DID URLs, including support for various parameters and fragment.

### **godiddy.com Component: Universal Registrar**

The Universal Registrar enables the creation/update/deactivation of many different types of DIDs, in a universal way, using a common interface.

The Universal Registrar supports both an internal secret mode, where private keys are stored in the Wallet Service, and a client-managed secret mode, where private keys stay on the client side.

DID operations may comprise multiple steps. Before a DID operation can be completed, it may be required to agree to a governance framework, or to provide funds to a cryptocurrency address. In such cases, the Universal Registrar returns the state of an “ongoing job”, which can be used to observe and manage DID operations that require multiple steps to complete.

### **godiddy.com Component: Wallet Service**

The Wallet Service stores DIDs and keys created by the Universal Registrar API. This way clients don’t have to maintain their own key management system.

The Wallet Service supports basic key management operations such as importing and exporting keys, transfer of DIDs, as well as creating and verifying signatures. All common key types and verification method types used in the DID ecosystem are supported. The Wallet Service can also be used for non-DID related operations, such as generating signatures for issuing Verifiable Credentials (VCs).

### **godiddy.com Component: Version Service**

The Version Service offers functionality around versioning, tracking and searching for many different types (“methods”) of DIDs.

This includes looking up historical versions of DIDs and DID documents, searching for DIDs based on the DID (the identifier itself), or DID document contents, as well as various tracking, auditing and analytics functions.

The Version Service, therefore, not only provides a view of individual DIDs at the present time, but makes it possible to access the entire history of a DID, and even events and trends in the global DID infrastructure as a whole.

## What Did You Wish You Knew When You Started Identity?

Session Convener: Heather F IDPro

Notes-taker(s):

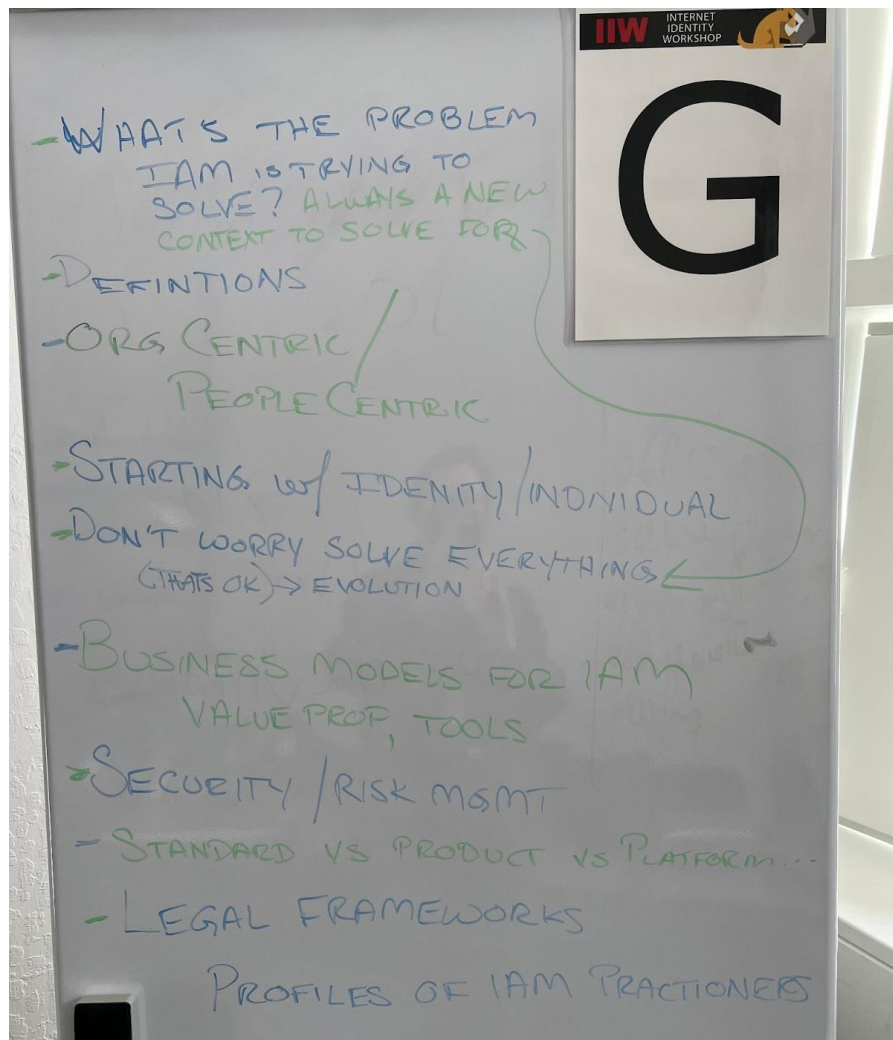
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Notes from the field:

Joe Andrieu -- I wish I knew that identity is how we recognize, remember, and respond to specific people and things. <http://bit.ly/FunctionalIdentityPrimer>

I also wish I knew that different people have fundamentally different mental models of what identity means. And we often talk past each other even as we honestly try to communicate.

<http://bit.ly/FiveMentalModels>







Chicken & Eggs  
verifier to adoption

— meet customers where they are

"proxy issuer"

potential problems

1.) Human

Employee onboarding

Validate — better risk manager

— NIKERAN

— chip in my arm — peren

made claim, dr made credential

2.15 cred — Google

Verifier has been much

quicker

Doing holders

define what the issuers  
need.

---

= Control over all of the  
pieces —

IDP \* Does the solution  
work - can it  
scale?

\* interoperable  
10x better.

as interoperable

Make it BASIC

There will be an envelope:

\* Technology \*

Verifiers — user experience

Verifiers — Integrate

let in — authentication

SDK

Global ID

scan QR code

Web app — express screening

Global

HTML



Teacher wallet  
Product owner



SSI break through —

critical mass —

HOLDERS  
mainline



Credentia

How often do you use

to the app user & over.

MFA

"Multi-Factor Authentication"

Schemas

or asks } BLEAK

W/in ecosystems.

→ Interoperable -

WISE - grow the ecosystem.

~ Verifiers → Identity providers

Value prop w/ Verifiers

→ interoperable -

5 of 5

WISE - grow the ecosystem.

~ Verifiers → Identity providers

Value prop w/ Verifiers

Where do they have a need?

∴ Idealism — pragmatism

A simpler time at IIW!!

xkc

CPROSA  
AR/AR

## ***Self Sovereign IoT Helium, Picos, DIDComm***

**Session Convener:** Phil Windley

**Notes-taker(s):** Sean Bohan

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

Slides:

[https://docs.google.com/presentation/d/1SSzf\\_wT11xXgB8XUeo\\_bUmr7KWJWFIIr/edit?usp=sharing&oid=114869174347229543921&rtpof=true&sd=true](https://docs.google.com/presentation/d/1SSzf_wT11xXgB8XUeo_bUmr7KWJWFIIr/edit?usp=sharing&oid=114869174347229543921&rtpof=true&sd=true)

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

Insteon - went out of business, won't keep lights on, employees removed from their LinkedIn

Retina manufacturer went out of business

How do we get out of that

Current model - manufacture, device, data about you

Compulsive of things

Alt model

You - data about you - manufacturer

Detail

Phil's cabin

Pump in pump house 100 yds away

20-25 below in the winter

Would love to know temp in pump house

Something happens to electric heater - bad things

Antenna

Options for temp sensors

1 Device from Scott Lemon (WOVYN) - wifi - power hungry, limited range, run hub, etc.

2 Sensorpush - bluetooth, out of Boston, simple, year on battery, great api, great app BUT limited range

3. LoRaWAN - long range wan - lot of companies making hubs, lots of sensors, GPS and accelerometers - if you look at the space, still early days, lots of room for improvement  
Expensive? Some - more exp than Wifi modules but if you need 5 not a prob, deploy a million is a problem

LoRaWAN - interesting LoRaWAN system called Helium

Helium - blockchain and token, proof of coverage, also built into the hotspot, triangulation and time for radio signals to prove a hotspot is in a place, you get paid in tokens for hotspot service

Good example of a blockchain use case, not making up an ecosystem

700k deployed

Phil made \$30 in a month

Adrian - Example of decentralized finance - kickstarter - use prepayment as avoiding SEC regs for selling stock - Only viable example of decentralized finance in the wild

Interesting global network

Didn't do any good at the cabin because it is in the middle of nowhere

Adrian - LoRaWAN is a MESH whereas Bluetooth and wifi need backbone

Lot of coverage in Bay Area - yes

LoRaWAN - 10km range

You don't have to worry about infra about backhauling data out of the sensor

Connects and senses stuff

Global thing

Privacy model ? Proximity detection?

Unknown re: privacy model

Connection itself is 2 hotspots

Payloads not encrypted

Adrian: anyone studied apple tag protocol? Privacy issues? - tool for cyberstalking - curious

how Helium will address that?

Helium console

Device keys - registered with network - helium running consoles vs others running consoles

In helium console - essentially UI to Helium Router (what device is connecting to)

Devices send data 3x an hour (reduces battery life if more frequent)

HTTP and MQTT integrations

Popular platforms

URL

Logging

Payload - 11 bytes - standard LoRaWAN packet is less than 23 bytes

Base 64 encoding

Take payload, take it apart

Adrian - for 11 bytes 3x an hour, how much?

You pay \$0.00001 - for one year \$2.42 per sensor - if you look at the bandwidth, more expensive than phone, but you don't need a SIM card for each sensor, a per use basis, tradeoff, not using LoRaWAN to transmit ZOOM sessions even if the network could support it - economics make sense

Payment

Heartbeat is JSON structure

Has lat/long of the proof of coverage

ID for the hotspot

Could do triangulation on it

Downlink and uplink same price

Adrian - how fast can you connect? Drive-by?

It doesn't transmit when driving

Doesn't transmit while motion - GPS better than that? Don't know

Q: protocol/handshake? Don't know

Control Channel

LoRaWAN - and Helium

Helium is a specific implementation of LoRaWAN

Willing to send a couple of bytes really far you can

Most LoRaWAN will look for response, or doesn't come back will knock down spreading factor and send again

Trying to keep it open

Blindly transmits

Extra implementation to send data down - considers like an unprocessed packet

## Helium Economy

Dual token model - data credits or Helium Network Tokens

Mint and burn equilibrium

Hotspots earn tokens from 2 sources, proof of coverage and data transfer

Mint and burn

Helium used to buy data credits is burned

Using more data credits than you are minting? Price fluctuates

Data credits linked to dollar

Always .00001 of a dollar

Large network of sensors - buying data credits as used,

Adrian - wants to do this decentralized finance model - is smart contract open source and accessible?

Several papers on mint-burn equilibrium model

Dual tokens - sam smith

Helium blockchain

Paid by hotspot for proving coverage and by data transfer

Helium recently announced hotspots with 5g and announced deal with Dish Network will have helium 5g nodes in them - higher data transfer rates

PICOS

LoRaWAN Device->Helium Network -> Helium Router -> Webhook -> PICO

Data flowing

Adrian - what does Phil think, app platform model on top of picos - a generalization of Eth smart contracts, receipt tokens as if they are gas, not worrying about infrastructure

Phil - hold that thought

Doesn't think Helium wants to be in the business of running router program - thinks they limit you to how many devices you build on their console - both open source -

This model: Phil runs Helium network, connect to PICO cloud, use manifold to create PICO too tell it what it is, exchange keys, uses router to register so auto connected to Helium

PICO engine building PICOs

6 sensors out there, 6 independent sensors - if they are thought of as PICOS can connect to do interesting things

This particular network - a temp network example (dist systems class)

Point it - programmable, do interesting things with them,

Phil has planned but hasn't gotten to

Find students to use DIDComms as the primary messaging channel for PICOS than

HTTP - end goal would like to build a mesh of engines (PICOS don't care what engine) -

goal - picos moving between engines

Connected together

Maybe use tokens to pay for computation

Consent addressable network

SamC - Things Network,

Phil - a business, LoRaWAN and especially HELIUM allows to just deploy sensors without having to worry how to connect, business that opens a lot of IOT use cases, before were too heavy - imaging deploying it, with enough hotspots, nice thing is not just relying on having enough hotspots - now covered

Adrian - you have to have competition for 5g - will never have self-sovereign 5g - once you lose ability to control router and use faraday cages to control house, lost firewall and packet analysis - ultrawideband meshes cannot have an economic model means that equiv of ham radio on top of telephone network - developed a resilience component

Sam - building house, putting in zwave switches, this LoRaWAN is closest thing he has. Buy LoRaWAN and Helium falls apart can redeploy to The ThingsNetwork (TTN)

### ***Twitter (What could twitter be?)***

**Session Convener:** Johannes Ernst

**Notes-taker(s):** Danielle

**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 asked "what is twitter?" and what could it be.

Twitter is a place to be heard and to listen.

We discussed ways users could flag posts, which could trigger an encapsulation with context like sources. We talked about blurring tweets or not, making them smaller with context around, or putting context below.

We brainstormed what we would want twitter to be

- a set of communities that have their own moderation settings
- a way to facilitate divergent brainstorming and consolidation through upvoting ideas, eg for policy decisions
- more of an inbox than an infinite scroll
- a way to use pluggable algorithms
- ability to defer tweets by topic to a separate feed, like triggering or heavier material for deliberate review away from the main feed



## ***When Do We Need a Ledger? (KERI, ORB, DID:WEB, IPFS)***

**Session Convener:** Richard Esplin

**Notes-taker(s):** Benjamin Goering

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

KERI <https://github.com/decentralized-identity/keri>

Orb <https://github.com/trustbloc/orb>

did:web <https://w3c-ccg.github.io/did-method-web/>

did:key <https://w3c-ccg.github.io/did-method-key/>

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

### Summary

Ledgers are needed when:

- The DID Controller should not be able to change what they said about their DID Doc
- Non-repudiable history is needed.
  - Key was rotated, but the cred wasn't revoked.
- Provable certainty of the current state is needed (as opposed to KERI's probabilistic statements about state).
- A common understanding of state, not based on a specific selection of peers
  - Governance framework
  - A schema attached to a framework
- Censorship resistant data availability
- Publicly auditable history

Also had a discussion about ORB vs KERI

- Orb: consensus set consists of peers in the checkpoint blockchain
- KERI: consensus set consists of peers that have your event log

### Detailed Notes

\* Attendee intros

\* Aaron: dweb projects use consensus more than is required. Only maybe needed for namespace mgmt

\* So, time travel: How do you verify credentials that may or may not be revoked

\* Richard: Proving a did doc is true at some point in time, censorship resistant, nonrepudiable is hard. (Time matters). Revocation registries might make more sense on a ledger.

\* CharlesCunningham: I agree

\* Richard: Starting with a use case where a ledger/consensus is required. 1 is time travel. (Verifying credential when issuer is down)?

\* Rouven: Do we have consensus of the latest state of my DID document

\* Chris: You can make a probabilistic argument, not a million percent certain.

\* Rouven: How do I know that my friend didn't get hacked, rotate keys, and someone comes later. Including key recovery use cases.

\* Aaron: How do we define the consensus group.

\* One option is authoritative. e.g. the UN. Or you could say that the object creator decides what the consensus group is.

\* Charles: This is how KERI works

\* Rouven: If you have network of friends that are my witnesses, can power this. But you still then have to trust your friends.

\* Shannon: I'm saying the same thing. If you don't trust, then there is a use case for consensus.

\* bengo: got it

\* Richard: keri/orb aren't as much for distributed consensus as much as a ledger

\* Charles: If you want to update your DID doc, then you need a ledger or other mechanism of linked signed events that provide atomic updates

\* bengo: like sidetone

\* Charles: Even if the person that owns the did document could lie to me. You could have an issuer that just lies to you.

\* Steve: Duplicity game. Alice is communicating with Bob and Charlie. Alice is consistent with each of them, but not the same.

\* Rouven: There are other ways that can happen, e.g. software updates across multiple devices

\* bengo: The software update supply chain problem

\* Steve: Watchers watching the watchers.

\* Bengo: but who's watching the watchers

\* Steve: different kinds of events in KERI are given more credence

\* Charles: It depends on what we mean by sovereignty. It's a matter of sovereignty. Is it ok for an issuer to 'lie' about the did doc? In ETH, the scarce resource is Did Documents. In KERI, the public keys are the scarce resource. You can either have one set or a different set. You could have two separate logs for the same identifier. They started with the same private keys. But they wouldn't be a 'good issuer'. Verifiers wouldn't like.

\* Richard: Does ORB help with this?

\* Dmitry: ORB is fairly simple, and I don't know KERI. ORB does atomic updates by writing a record into whatever database it's relying on.

\* Richard: IPFS?

\* Dmitry: There is still a database, it's up to each node, or a distributed database

\* Dmitry: Does that have an inherent risk: yes

\* Dmitry: Network of issuers is a network of trust issuers. They're all reputable issuers that don't want to do evil.

\* bengo: It makes trust nonbinary, but instead asymptotic

\* Richard: And you're saying orb publishes those events using ActivityPub?

\* bengo: /thumbsup

\* Rouven: If I now need to make sense of 'can I trust this'?

\* Rouven: Passports are an important use case. And we want to make it easier and more standardized for countries to verify them, and global consensus is kinda like that

\* Rouven: Don't want everyone to use the universal resolver

\* Aaron: Like Metamask

\* Rouven: We need to narrow down the number of DID methods so it's less likely for people to centralize the verifier

\* Dmitry: One of the reasons we made ORB. A Verified network. We launched it 3 years ago with banks and govt starting 4.5 years ago. Uses JWT for VC. Uses Anonymous identifiers. Use blockchain. Uses hyper ledger fabric. 7 years ago that was a very decent project. There weren't so many back then. Solid enough, lots of contributions. Then we figured out that sovereign

place, they're skeptical of using Fabric/IBM. Maybe we can use bitcoin? All banks and governments say "We're not touching that". We have to design something that has two options. You have either have the blockchain independence, meaning you can use whatever blockchain you want. If you are completely against the blockchain, you could survive without it.

\* bengo: (or if it's not accessible to you)

\* Richard: Use case where you need to have a list of trusted issuers. You don't want to go to the whole world. You want a narrow list. That's one example I had for wanting a ledger. Government frameworks that don't allow for repudiation. And I don't think KERI has that property.

\* Charles: KERI people would say that that's a problem for another layer, like an automated governance network.

\* Rouven: Register machine readable government network which has policy. Then one ledger.

\* bengo: heirarchical consensus

\* Aaron: like the olympics logo

\* Rouven: It requires a lot of effort to keep the network going. If someone withholds an event, it's really hard to survive that.

\* bengo: Eclipse attack.

\* bengo: Gossipsub?

\* Dmitry: Does not solve the problem all the way, for example the 'cost of computation' issue.

\* Rouven: You have timestamping, execution. KERI is simple. Anything more complicated reduction rules after that get way harder. The third problem is data availability.

\* Rouven: With zero-knowledge rollups, we can do computation off chain, which helps a lot with cost of computation.

\* Aaron: Then you need the whole blockchain though off chain

\* Bengo: not with recursive zk proofs

\* Rouven: yeah

\* Rouven: In a recovery network. I can configure a way of doing recovery anchored on-chain. Only revealed later (via ZK) when recovery is strictly needed

\* Charles: Can you have divergent state?

\* Richard: One goal we had in indy was to replay the ledger from the beginning. It was useful because we wanted to rewrite history to preserve trust

\* bengo: that's not what most people think is trust.

\* charles: something insightful (sorry)

\* Dmitry: That was insightful. One question. For many operations, classic schema is issuer issues to holder. Credential is shared many times. One other reason we created ORB was that in the business world we had situations where issuers wanted to issue credentials on the spot based on the RP wanting to know how much is in your bank account. e.g. how many points you have on your drivers license. How does KERI work in this 'just in time' context.

\* Charles: Verifier would need to get data from you or one of your witnesses

\* bengo: The blockchain project shouldn't decide what the policy is, the end-user should.

\* Aaron: How can I verify with 'finality' within 5min

\* Rouven: Isn't that user-centric if just my witnesses need to have consensus as to the data that helps verify.



**LedgerDomain** @LedgerDomain · Apr 26

...

Excited to sponsor this year's Internet Identity Workshop! Our very own Leonid Alekseyev is onsite today to discuss our work on [#verifiablecredentials](#) for [#DSCSA](#) [#IIW](#)

Internet Identity Workshop

# IIWXXXIV

## INTERNET IDENTITY WORKSHOP 34

### QIQQO WORKSHOP HUB

#### IIWXXXIV Open Space Workshop April 26, 27 & 28, 2022

Welcome to the IIW Workshop Hub  
Connect with Other Attendees \* Session Note Forms \* Agenda Walls \* 3 Day Schedule  
Find out everything you need to know about IIWXXXIV!

IIWXXXIV  
INTERNET IDENTITY WORKSHOP 34

**Sponsors:** Microsoft, Google, Hellō, GS1, Spruce, identity, Avast, AWS Identity, HYPERLEDGER FOUNDATION, DANUBE, trinsic, WORLD COIN, LedgerDomain, esatus, IEEE SA, yubico, ANONYME LABS, TRUST Over IP, LEI, IDPRO, JOLOCOM, AyanWorks, Indicio.

**22 Present**

**280 Participants**



## Notes Day 2 / Wednesday April 27 / Sessions 6 - 10

### SESSION #6

#### *Use cases for vLEIs*

**Session Convener:** Stephan Wolf (GLEIF) **Notes-taker(s):** Christoph Schneider (GLEIF)

**Tags / links to resources / technology discussed, related to this session:** verifiable LEI, Business use cases, Annual report, KERI, CESR-Proof signatures - Slides available at: [https://github.com/WebOfTrust/IIW34/blob/main/20223-04-26\\_IIW-vLEI-Use%20Cases.pdf](https://github.com/WebOfTrust/IIW34/blob/main/20223-04-26_IIW-vLEI-Use%20Cases.pdf)

#### *DIDCOMM Super Stack*

**Session Convener:** Michael Herman (mwherman@parallelspace.net)  
**Notes-taker(s):** Michael Herman (mwherman@parallelspace.net)

**Tags / links to resources / technology discussed, related to this session:**  
Presentation: <https://github.com/mwherman2000/VCTPSPrototypes/tree/main/doc>  
Demo Repository: <https://github.com/mwherman2000/VCTPSPrototypes>

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

DIDCOMM Super Stack (DIDSS) - Creating highly scalable DIDCOMM Agents using .NET, Trinity, and Okapi with Ease (Ft. VCTPS Protocol) - Application framework for creating Verifiable Capability Authorization-enabled, highly scalable decentralized agents using .NET and DIDCOMM (featuring the VCTPS DIDCOMM Protocol)

#### *Advanced Syntax for Claims*

**Session Convener:** Daniel Fett, yes.com **Notes-taker(s):**

**Tags / links to resources / technology discussed, related to this session:**  
Slides: <https://danielfett.de/talks/2022-04-26-openid-advanced-syntax-for-claims/>

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

Notes - Claims - extension to OIDC for requesting & receiving claims can include transforms + functions ie birthdate->years ago -> over 21?



## ***Common Features & Requirements of SSI-based Storage***

**Session Convener:** Charles Cunningham

**Notes-taker(s):** Dan Ostrovsky

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

- At least 5 SSI projects have converged on similar implementations... why? And how to share components?
- The most important components
  - Internal data model
    - IPLD - it's what IPFS uses to create a json data of CID hash links to where data is stored, solving the problem if limited block size
    - What does IPFS add? Bitswap, a protocol to coordinate sharing of data.
    - This module could be shared across all projects, but it could have different feature sets that make it more complicated (i.e. fission does something different)
  - Authorization style
    - OCAP - object capabilities
    - ACLs don't CA (access control lists don't control access)
    - This module could easily be consumed across all projects
  - Identification style
    - DIDs are the industry standard
    - This module could easily be consumed across all projects
  - Replication style
    - When and how should graph synchronization happen?
  - Consistency
    - When and how should graph synchronization happen?
    - Projects implement eventual consistency
    - There are some issues with this, specifically when talking about authorization since more server attack vectors are introduced

Why are there 5 different projects with exactly the same styles (save Textile using ACL instead of OCAP for authorization style), and how could we standardize the formats/contents of implementations to interoperate between them?

Question was asked about EDV, which concerns itself with providing an https API

## ***IDPro AMA and What is the Future of the IDENTITY Profession?***

**Session Convener:** Heather Vescent IDPro Exec Dir **Notes-taker(s):**

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

Discussed IDPro, mission and objectives.

- The need to have vendor neutral educational material.
- The challenges of having teams use the same terminology even internally in order to communicate about the tech.

Join IDPro: <https://idpro.org/membership-individual/>

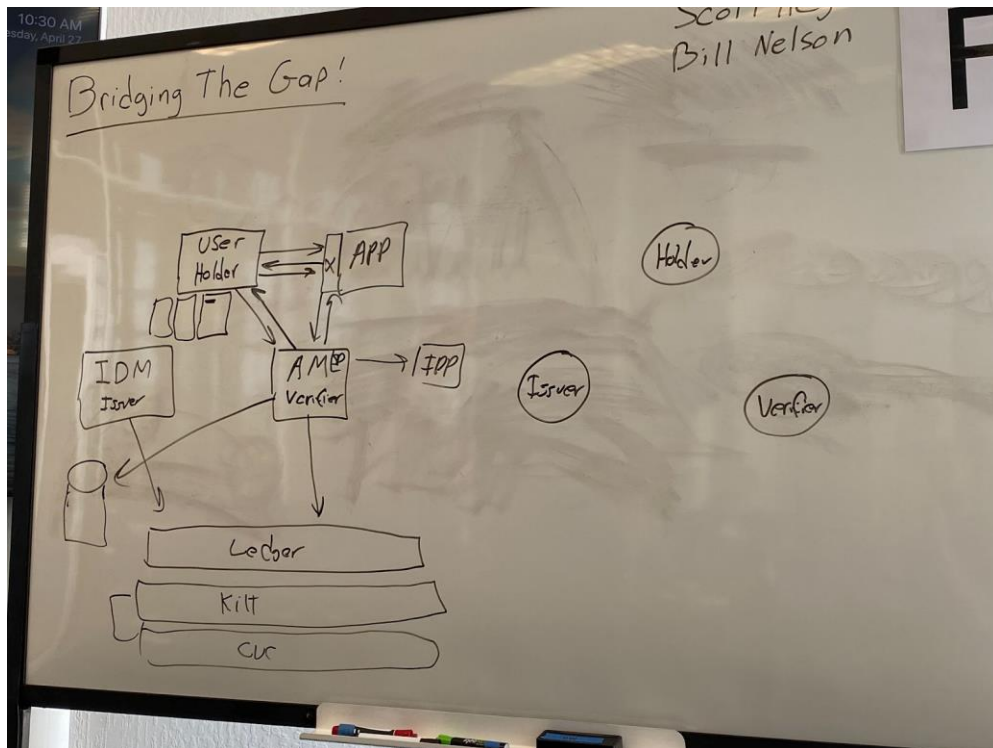


## Bridging the Gap (Between Traditional IAM and SSI)

Session Convener: Scott Heger & Bill Nelson (Identity Fusion)

Notes-taker(s): Bill Nelson, Steve Venema

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



Traditional IAM solutions involve three components (IDM, AM, and User). Is there a correlation between the three components of the trust triangle and if so, does it make sense to use existing IAM implementations as a bridge to SSI adoption?

There was a lot of “passionate” discussion around the feasibility of this, some for and some against. There are existing solutions that are attempting to address the “bridge”.

In general, the main topics of discussion included:

- The bridge is possible from a CIAM solution, but not necessarily from a workforce solution.
  1. Approach a particular industry
  2. Identity specific use cases where SSI might apply
  3. Perform a POC with forward looking companies
- Relying Parties need to see value in the solution

### Steve's Notes:

Topic is how to transition between traditional identity to decentralized identity

Traditional: showed diagram of IDM & AM, with storage repo (e.g., LDAP) under IDM

User accesses an app, redirects to AM for authN and returns session token

Compare to...

Issuer - Holder.- Verifier

IDM adds Issuer

- It would be connected to public ledger

User is holder, with their own repo (Wallet)

AM adds verifier roll

Q: Yair Sarig @ VMware: Why would a business do this

A: removing liability of data in ldap repo

C: Vittorio: New system offers new opportunities and scenarios, doesn't look like a migration, more like an augmentation

Ledger could be a private ledger or public

- Kilt, CVC

Stephan Baur: Using US Healthcare as a canonical example, we can't have every hospital create an account for every patient

Andre

George Fletcher; lets separate workforce and consumer

- I think about this from a RP perspective
- What is the business justification for RP to support SSI
- As a RP in CIAM, you always have to manage identity,

Nitov P: <emphasized the number of systems a typical (hospital) and investment behind it  
We need incremental value

?? how can we enable the benefits without requiring expensive changes to customer apps ??

## Human Rights by (Protocol) Design

Session Convener: Adrian G

Notes-taker(s): Hannah Sutor

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

<https://docs.google.com/presentation/d/1jcVpPm0YAhYSqeYjg0DTxKhqH7KXKH12kXHiB7uK-LE/edit#slide=id.p>

<https://blog.petrieflom.law.harvard.edu/2022/04/12/a-human-rights-approach-to-personal-information-technology/>

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

Regulatory approach in EU is based on human rights - third slide is a link to the EU privacy directive  
Message to take away: their framing is a human rights framing

Separation of concerns across levels -

1. Sign-in and signing
2. Requests for information
3. Storage of the result

This would accomplish human rights by design.

**Scope along with purpose and identity** become the request.

They are established at different points in time by different actors.

Result is what gets presented to that resource server.

ACDC - graduated disclosure. "If you use my data, these are the restrictions i have on the usage of my data"

Delegation happens in what policies you put in to layer 2, which doesn't store the data, only stores the policies:

	Platform	Decentralization
1. Sign-in	Sign-in with Facebook	Sign-in with Apple Self-Sovereign Identity VPN

<b>2. Request</b>	Search Notification Shopping	Tor
<b>3. Storage</b>	Posting Purchase	IPFS Apple Pay

Surveillance and profiling should be as expensive as possible...period. This isn't something that is easily sold. How cheap do you make it to have secondary uses?

As long as you can keep an individual accountable, regardless of the delegation that has been introduced, consent is not achieved through prior blanket consent but through delegation.

Ricardian contract for requestor liability

Separate vocab SDO from state machine SDO

XAML PDP - PEP separation

Q: Who is enforcing accountability?

A: In these protocols you lose the ability to have a firewall because now every single resource server, wallet element, etc is its own domain. One of the things we do to keep people accountable in the paper world is to use a notary. Very inexpensive way of authenticating a transaction. Taking it the other way, breaking the glass, is much more expensive. As long as on the average, notary is cheap, but holding them accountable is expensive, this is a separation of concerns. Can we introduce in the protocol a similar thing to a human notary?

Q: Is the whole "black box" of the way things work a concern for users trusting these systems?

A: Because of the visibility of software,

Q: When you say sign in and signing, is choosing session duration part of this?

A: Yes, this would be part of it. ZTA - zero trust architecture. Scope and purpose. Scope has nothing to do with purpose. Scope is established by the resource owner. Ex: Scope is defined by patient (health record). System that stores the health record has it segmented and has tags for things that have sensitive data. Patient decides what to disclose based on purpose.

Q: Scope is about access to data?

A: Scope is which part of the record do you actually want? Any auth app has ways of handling scope.

Q: OAuth 2 scopes exist today. I'm imagining that eventually you'd want to be able to define even more granularity to try to convey intent. Is this where you're heading?

A: No. We are dealing with 2 different domains:

1. Vocabulary issues
2. Protocol - who sends what to whom, when

---

### Whiteboard Transcript:

<https://bit.ly/PlatformDecentralization>

- Session duration (ZTA)
- Request > Authorization Capability
- Request components
  - credentials (who is accountable)
  - scope (all or some of the resource)
  - purpose (a GDPR human rights requirement)
- Vocabulary interop vs. State machine interop
- ACDC Graduated Disclosure (as serial requests)
- No consent for secondary use, period
- Notaries for accountability
- AI > Federated Learning from personal data (education)
- Ricardian Contract for requester liability
- XACML, PDP and PEP
- HIE of One demo project

## ***Indy DID Method & Network of Networks***

**Session Convener:** Daniel Bluhm

**Notes-taker(s):** Markus Sabadello

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

Hyperledger Indy, DIDs, Sovrin, Indicio

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

<https://github.io/hyperledger/indy-did-method>

Goals:

- Align Indy networks with W3C DID spec (original HL Indy existed before DID standardization and had earlier concepts)
- More and more Indy networks (Sovrin, Idicio, Findy, IDunion, Candy) -> desire to use VCs issued on one network on another network
- DID URLs for Anoncreds objects

Example:

did:indy:indicio:...

Who decides what the names under did:indy are? -> That's a question of governance frameworks

- Could be built into a resolver similar to hosts.txt file
- Could be resolved dynamically using a config file from a Github repository

Example DID URL:

did:indy:example:123abc/anoncreds/V0/SCHEMA/seq\_NO

Also for CLAIMDEF, RevRegDEF, Deltas

This didn't require any changes in HL Indy, only in resolvers.

Has been implemented in indy-vdr library.

Introduced a new "didDocContent" ATTRIB.

Now we have explicit rules for how to join data from NYM and ATTRIB into a DID document.

Updates are possible -> you rewrite the whole DID document with a new ATTRIB transaction.

Question about scale, what if I want to create a million DIDs?

-> HL Indy networks may have to be tweaked to support scale, but it doesn't really affect the DID method rules.



In HL Indy, personal DIDs are not written to the ledger; instead, peer DIDs as implemented in HL Aries are typically used.

The namespacing inside the did:indy method opens up the possibility of the “network-of-network”.

This also made it easy to add a driver for the Universal Resolver.

If you want to add a network to did:indy, there’s a Github repo where you can raise a PR with the new network. This repo is managed by the did:indy community.

There is an idea of cross-registration, so on one network you could have a directory where you look up other networks. Is this still the plan? This pattern may also apply to other networks.

Maybe the network name “local” should be reserved.

At some point there was also a proposal to use hashes of genesis files, instead of human-readable network names.

Maybe HL Indy will become popular as “government networks”.

## ***Open ID & SSI Credential Issuance***

**Session Convener:** Torsten, Kristina, Tobias

**Notes-taker(s):** Antonio Antonino

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

*Problem:* identify a protocol that includes all the different types of identity credentials, e.g., mDL, VCs, etc.

*Goal:* A protocol to issue identity credentials that 1. has strong foundation, 2. is format agnostic, 3. supports credential refreshing, and 4. supports multi-credential issuance

- The core flow can be extended to accommodate different security requirements for, e.g., wallet binding, and also to result in the issuance of credentials of different formats.
- The authorization request is only concerned about WHAT credential is requested, not in which format
- Considering to add FIDO keys in the credential request step

## ***Access Control Use Cases***

Session Convener: Alan Karp

Notes-taker(s): Alan Karp

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

[https://docs.google.com/document/d/1jr1MM6Sjf4f2Y9JjJLOsAxTv2TYNuE\\_Ck0kMuI589I/edit](https://docs.google.com/document/d/1jr1MM6Sjf4f2Y9JjJLOsAxTv2TYNuE_Ck0kMuI589I/edit)

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

Several groups are adopting capabilities for access control, but I am concerned that the use cases they are considering are too simple. I'm hoping that considering the use cases in the above document will lead to better designs.

In the session I discussed those use cases.. Please add comments or suggest other use cases.

Many of the use cases involved ad hoc delegation, which led to a question about enforcing enterprise policy. Aren't there some situations when you should prevent delegation? Perhaps, but doing that leads to a system that is both harder to use and less secure. The problem is that people will share credentials if that's the only way they can get their work done.

## ***Building privacy-preserving payment rails: without commercial models, SSI will fail***

Session Convener: [Ankur Banerjee](#)

Notes-taker(s): Ankur Banerjee

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

1. [Seven Deadly Sins of Commercialising SSI](#): A session from IIW 33 with background on discussions during this session
2. [Business Models of Identity](#): An overview of how existing commercial models are in digital identity businesses - and extensions that could be applied to make the same work in self-sovereign identity.
3. An [example of decentralised payment rail models](#) (there could be many approaches possible)

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

1. We discussed the basic context of how identity attribute validation/verification is currently done, and it often relies on expensive, centralised services.

## SESSION #7

### *verifiable LEI (vLEI) Update and Progress Session*

Session Convener: Karla McKenna, Christoph Schneider (GLEIF)

Notes-taker(s): Christoph Schneider (GLEIF)

Tags / links to resources / technology discussed, related to this session:  
Organizational Identity, Verifiable Credentials, Persons in roles, KERI, ACDC

Slides available at: [https://github.com/WebOfTrust/IIW34/blob/main/2022-04-06\\_vLEI-Update-Progress-Session-IIW\\_v1.0\\_final-for-publication.pdf](https://github.com/WebOfTrust/IIW34/blob/main/2022-04-06_vLEI-Update-Progress-Session-IIW_v1.0_final-for-publication.pdf)

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

### *Introduction to G NAP*

Session Convener: Justin R

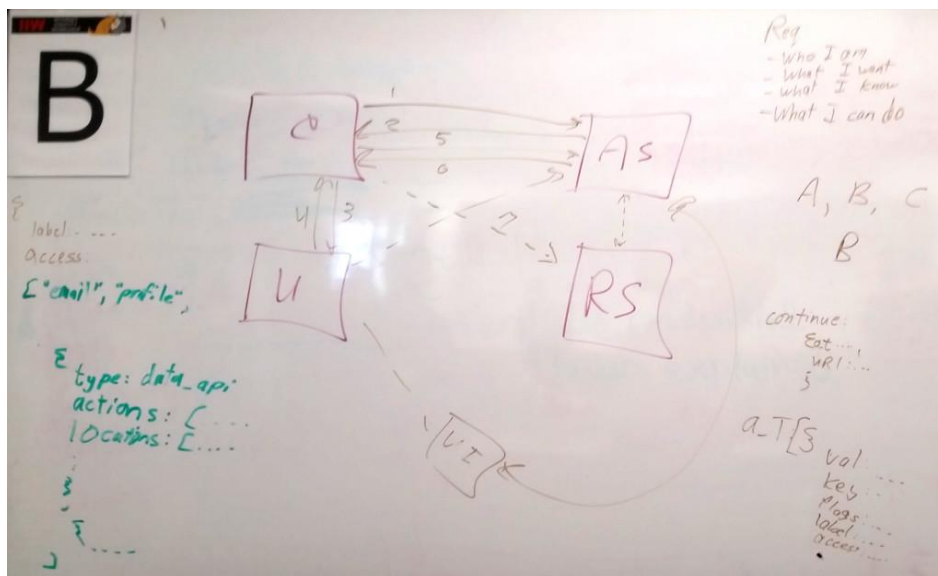
Notes-taker(s): Charles E. Lehner, Steve Venema

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

<https://oauth.xyz/>

<https://celehner.com/2022/04/27/gnap.txt>

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



Speaking to OAuth2 limitations and things bolted on  
GNAP: looking for common abstractions in those bolt-ons

Primary design pillars

- Consistent protocol across many different use cases
  - OAuth: too many flows, lots of questions to ask in order to decide which flow
  - Desire a protocol which allows you to start things the same way and then decide further in the flow

Client (C) always starts with a call to AS (http POST)

- Who I am, what I want, what I know, what I can do
- In OAuth, the who is clientID. Its a bad abstraction. Big topic of conversation at OAuth WG in last IETF mtg

Next pillar: Avoid expensive discovery operations in the protocols

- Ex: mobile device can generate device attestation along with self issued key in an MDM env.

What I want:

- Ask for an access token

RAR-kind of info in the request

- RAR is a backport of this piece of GNAP (speaker is coauthor on RAR as well)
- JSON array of objects, watch with...
  - Type [ ... ]
  - Actions: [ ... ]
  - Locations: [ ... ]
- Gives you a very rich set of expressions without having to cram it into scopes

When the RS might be getting different information (that the client never actually sees)

In GNAP we make subject info is its own first class citizen

Situation: Client may already know who the user is — say, a VC

- Simplifies the flows

Grant types

Q: How do we start

A: One way is that the RS can redirect the client to the AS

Also have a provision to allow AS and RS to communicate (client never sees this)

Most common will likely be that developer just specifies the AS

“What can I do”...

- Client can say I want to do A, B, C
- AS can reply with only B, depending on resource you want

Response:

- Continuation, which is used for interaction with RS?

Status:

- Core spec has been stable in terms of syntax and core functionality for 6-9mo now (lot of churn before that)

- Biggest recent change: user code split into two things
- Security considerations in work with security researchers
- Stability: core spec stable, but will probably see some changes as implementations move forward
- Biggest ref implementation is the XYZ impl by Justin (oauth.xyz)
- Google : "GNAP IETF Hackathon"
- SecureKey is using this as part of a nextGen of one of their products

## ***Keep - UX design for the vLEI Ecosystem***

**Session Convener:** Janet Gonzales, Kevin GRiffin

**Notes-taker(s):**

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

For GLEIF we had an ecosystem governance framework that provided the technical requirements and constraints, the user types and regulatory use cases, and of course a strong development team, but the challenge of it was how do we work within this framework to create an experience recognizable to users. This presentation will provide a brief overview into some of the challenges, pain points and breakthroughs we experienced when working through the UX design process to this point for GLEIF.

### **Goals–**

As mentioned, we had to work within the ecosystem governance framework which clearly defined the user types and had specific instructions for what parts of the experience should look like, designing recognizable UX flows to different user types (both technical and non-technical) were equally important, and working within the security of the KERI protocol.

### **User Flows**

Trying to make sense of the different user flows for me started here–taking into account who would be receiving credentials, presenting credentials and issuing credentials and what the edge cases would look like.

### **User Personas**

There are several different user types in GLEIF's case–enough that there is a glossary, but simply stated, there are GLEIF employees, authorized persons that issue credentials (QVIs), authorized users (ECRs/OORs), and individuals looking to verify credentials. When I was working through the persona process, there were a few things I identified:

- Not every user is going to be a technical user, this needs to be simple, for even non-technical employees to understand.

- In industries like finance, this will be a piece of the broader due diligence process, it's important to guide individuals through the process, ideally with some tutorial and understanding of their role, since they won't be in this day in and day out.

### **Out of Band/Swimlane Diagrams**

Part of the verification process is done out of band, and because of this it became important to do some in band/out of band, swimlane diagram creation.

### **Iterations of Dashboard**

Trying to produce an ideal dashboard is only one issue tackled here. Credential issuance, revocation, key management, etc. are far larger issues, but just to show an example of some of the iterations of some of the screens, I'm going to walk you through some considerations taken when developing the dashboard.

### **Focus on User Friendly Terms**

Working with the acronyms at first seemed daunting, and to make it easier on users, we thought using more basic terms on a simple dashboard would be easiest, but when presenting it to GLEIF, it seemed to cause more confusion. "Connection" proved to be too general a term, tasks as well, there needed to be more contextualization around this.

### **Focus on Visual Hierarchy**

With that in mind, we tried to contextualize more and provide all available options to verify, share and issue credentials, and emphasized the tasks section since this is where we envisioned more users would be spending their time. Keys and credentials would be managed from the dashboard as well across all identifiers. This also was still not the level of contextualization that was needed and we needed to make sure that it made sense for all user types, technical, non-technical, GLEIF employees, non-GLEIF, etc but we also wanted to future proof the designs to allow for users to use the Keep for other purposes. We found that balance to some degree in the next screen.

### **Focus on Contextualization**

Here contextualization went almost a little too far, though the terms came direct from the ecosystem governance framework, but that works off of the assumption that even non-technical employees would read the glossary, and even so, in some cases it doesn't provide the right context for the task itself. We added a short onboarding flow that each user type would have to go through to also help with this issue. We also created a sidebar with generic actions here though that we continue to use in the current form.

### **Current Dashboard**

The current dashboard, accompanied by an "Intro to Your Role" tutorial provides the right balance of contextualization and user-friendliness to navigate through the basic tasks (but it's fair to admit this is still being worked on). Currently we're working on screens for iOS and for Desktop.

Brief overview of Keep architecture electron, mirthil, keripy - repo :  
[github.com/weboftrust/keep](https://github.com/weboftrust/keep)



## ***Identities for the Martian smart home: An urbit discussion self-sovereign IoT***

**Session Convener:** ~pilwyc-fastec (urbit ID)

**Notes-taker(s):**

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

Slides: [https://docs.google.com/presentation/d/e/2PACX-1vRLcdOHZzF0K-pvBcDMWF1Q1Ur98t9K\\_9jB577irG6hiLs1hQ3IXdx0wHO7-ipVxArXjxwk6AxAeJrt/pub?start=false&loop=false&delayms=3000](https://docs.google.com/presentation/d/e/2PACX-1vRLcdOHZzF0K-pvBcDMWF1Q1Ur98t9K_9jB577irG6hiLs1hQ3IXdx0wHO7-ipVxArXjxwk6AxAeJrt/pub?start=false&loop=false&delayms=3000)

Urbit IoT: <https://urbit.org/blog/iot>

Communal computing on urbit grant: <https://urbit.org/grants/communal-computing>

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

“Baked in identity” means through communication through nodes.

Not surprising - SSI/DID lack of knowledge.

House wiring is considered safe - analogy - needs to build trust over time - 100 years? - when did the breaker box become standard after so long?

Moving out issue - needs to be built in from the beginning.

“Delete” is the most expensive feature now - due to prioritization of data retention for decades - now it is an issue due to things like GDPR

Spruce - delegate permissions - shadow identities if not able to assign one - need something to delegate to - root identity

Should we use presence or time spent by a person in a room (or with a device) equal the identity (identities?) of that space? Need to do more research on this!

Implicit vs. explicit identity creation

Difference between provisioning a device with its own identity, logging into a device, and sharing from one identity to a device.

## ***Sign in with Ethereum 101***

Session Convener: Oliver Terbu

Notes-taker(s):

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

<https://docs.google.com/presentation/d/1wancsZLn0hYk7n2sMS3-moWiexiYcy-6ke1VJdYhWg4/view>

## ***Wallet Security - the overloaded trust relationship***

Session Convener: Paul Bastian

Notes-taker(s): slide deck below

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

<https://nextcloud.idunion.org/s/r9Lkk4TQRJTBxR7>

## ***LEAKED CREDS 101 - How Leaked Creds are Used to Compromise IAM Systems?***

Session Convener: Stan Bounev

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

## ***Backchannel Logout and SSE***

**Session Convener:** Heather Flanagan, Vittorio Bertocci

**Notes-taker(s):** Heather Flanagan

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

As browsers kick in new privacy requirements, underlying primitives that let federated identity work will break. Some technologies may serve as alternatives.

Backchannel logout is still in draft.

In front channel, OP will have iFrames with 3pc to each RP that used it to login in order to then logout.

In Backchannel, the RP will have to expose an endpoint. The RP will clear its own cookie, and then the OP will do a server-to-server communication to the other RP endpoints to logout.

Challenges:

- the endpoint need to be visible outside firewalls;
- the RP needs to be stateful (save the SID and wait for the browser to touch it so it can then do the logout)

This can be packaged into an SDK but it requires RPs to have infrastructure to do this. Of course, not everyone has infrastructure, and not every infrastructure is the same.

Adoption rate? Mostly adopted in the financial industry, but otherwise not broadly adopted.

Use case that caused the spec to happen: a person from a brokerage house in the OID workshop said he had a use case of stock trading on a website, but the bond trading happens in an iFrame with a third-party vendor. When you logout of the stock trading site, want to be certain that logout has also happened with the bond trading site.

It is not considered a developer-friendly solution.

Shared Signal and Events (SSE) is a large stack of specs across different standards orgs:

- CAEP and RISC, (OIDF)
- SSE, (OIDF)
- RFC 8935, RFC 8936, Subject Identifiers (I-D), (IETF)
- RFC 8417, (IETF)
- Jose Family (IETF)

A true browser-based logout event, SSE could be a good option, though it is also a bit heavy weight

One group is trying to bring together OIDC, SCIM, FastFed, and SSE as a complete identity stack. This is definitely complicated.

Unclear how this will work with SAML.

The majority of requirements for SLO in the enterprise is based on on-prem services. If the OP is in the cloud, it might not talk directly to the RPs in the enterprise.

Parts of the SAML ecosystem no longer have developers working on it; putting changes into a SAML stack is formidable.

Logout is an asynchronous problem, and both OIDC and SAML try to handle it in a synchronous way.

The solutions between the new app-driven world and traditional webSSO is a mismatch.

For deployment challenges - percentage that's solved for enterprise using device management? It varies by sector.

Alternative directions: user preferences and controls; browser APIs are another, to help developers expose the options. There is more acceptance of a managed profile in the browser than a managed device; the user can always use a different browser for different purposes. There needs to be other ways to push the policy. Should an IdP host a well-known file that holds that profile for the browser? That might be an option to explore.

With on-prem constraints (which include a lot of SAML) then the only thing that has access inside the firewall is the browser; there is no direct communication between the OP and the RP. Backchannel logout would therefore not be viable. SAML is also an entirely a non-started, and SAML is the larger use case (larger than OIDC) in this case. In one case, "enterprise apps" are just another name for SAML services.

What's urgent for browsers - any new changes require redeployment of the RP, so if 3pc are going to be killed in Q32023 (which is an absolute) can Backchannel be deployed by then? No, absolutely not. If there is an option that allows the functionality to work even if there is bad UX, that's ok, because that will just be incentive to move.

The assumption is that it's easier to change the IdP/OP than it is to change the SP/RP. So if the API is something the IdP would call that would result in an interaction with the user "would you like to log in" that might be more deployable.

FedCMs goal is for the API to give the browser all the URLs and load them in parallel as if they were iFrames. Right now, they are GET requests, but doesn't allow the RP to use JavaScript to clear the code (and that's critical to some, not just to clear cookies but also to clear browser local storage). There will be more value when FedCM can take over some of the responsibility for logout. If the browser knows what's supposed to logout, it can keep trying to logout until successful. As long as the RP sees exactly the same thing it sees today so they don't have to make changes.

Backchannel won't save everything. What can we put into the OP/RP interaction that will provide enough friction to support the privacy requirements while still allowing existing functionality to work.

Would like to not live in a world where vendors ask customers to remove protections.

To continue the conversation: <https://www.w3.org/community/fed-id/>

## ***Reference Architecture or Trust over IP - Universal Interoperability***

**Session Convener:** Wenjing Chu [chu.wenjing@gmail.com](mailto:chu.wenjing@gmail.com)

**Notes-taker(s):** Wenjing Chu

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

How to achieve trust over the Internet AND universal Interoperability/Connectivity.

Please access the presentation slides here:

<https://docs.google.com/presentation/d/1QpC7G4dM-4DTcnsnPAHxun4CYHtveQYj6YcSVk1TUBI/edit#slide=id.p>

If you missed the session, Wenjing discussed the same topic previously which has similar information and a recording available here:

<https://wiki.trustoverip.org/display/HOME/2022-04-21+TATF+Meeting+Notes>

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

This session introduces/discusses a Reference Architecture for establishing Trust over the Internet unifying diverse designs and solutions. It is a work currently ongoing in Trust over IP (ToIP) Technology Architecture Task Force.

- What is a Reference Architecture, why do we need it?
- The most important objectives
  - Universal interoperability
  - Trust
  - Decentralization...
- Hourglass - why a minimal function trust spanning protocol for maximum interoperability
  - The Neck and Waist shape of the stack
- The Reference Architecture that consists of decomposition by locus of control
  - End systems
  - Supporting Systems
  - Intermediary Systems
  - And protocols between them:
    - End system to end system protocol
    - End system to Supporting system protocols
    - Intermediary system protocols
    - Interfaces between layers

The example case studies: Indy/Aries, Keri, DIDcomm,...

### **Notable Questions/Discussions:**

- How to implement Message Storage/Delivery Service:
  - In this architecture, that would be considered an Intermediary System
- How to evolve to that ideal goal from what we have today:
  - Discussed examples and how we may start by demo of interoperability
  - Discussed right organization to standardize, e.g. IETF for reach all of Internet

- Is Interoperability dead?
  - We believe not. We believe it's our future to fully realize the benefits of our labor. But there is a competing session later today for that topic.
- Why not just use HTTPS and enhance it?
  - It is in a way THAT - because it's a common transport.
  - Changing HTTPS is itself a difficult process. Don't know which is harder.
- Keri questions
  - We didn't have time to dive deeper into it but there are quite a few sessions by Sam and others in this IIW.
- How to get involved and continue to have these kinds of discussions:
  - Please join our Task Force's weekly meetings (2 sessions: 7am Pacific Time, 1pm Pacific Time, on Thursdays).
  - Here is the link:
   
<https://wiki.trustoverip.org/display/HOME/TSWG+Technology+Architecture+Task+Force>
  -
- I probably missed many great questions here - those above just came to my mind right now.
- You can also ping me [chu.wenjing@gmail.com](mailto:chu.wenjing@gmail.com). Or LinkedIn, Slack, Twitter @wenjing.

Thank you to all participants.

## ***BBS+ Signatures***

**Session Convener:** Vasileios Kalos

**Notes-taker(s):** Vasileios Kalos

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

Link to presentation:

<https://docs.google.com/presentation/d/1hSRragNccMmmUnSorpQOnNsRBI5VLTB3/edit?usp=sharing&ouid=114694734233211540431&rtpof=true&sd=true>

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

BBS+ is a digital signature cryptographic scheme that supports several unique properties. Notably, the scheme supports signing multiple messages whilst producing a single, constant size, digital signature. The possessor of a signature is also able to derive proofs that selectively disclose subsets of the originally signed set of messages, whilst preserving the verifiable authenticity and integrity of the revealed messages. Furthermore, these derived proofs are said to be zero-knowledge in nature as they do not reveal any information about the underlying signature or messages chosen to not be disclosed; instead, they only reveal a proof of knowledge of the undisclosed signature.



BBS+ are based on the work of D. Boneh, X. Boyen, and H. Shacham, titled: “[Short Group Signatures](#)” of 2004. Later they were re-visited by Man Ho Au, Willy Susilo and Yi Mu on their work titled: “[Constant-Size Dynamic k-TAA](#)” of 2006 and they were visited again by J. Camenisch, M. Drijvers and A. Lehmann on their work: “[Anonymous attestation using the strong diffie hellman assumption revisited](#)” of 2016 (this is the version that the draft specification mainly uses). The signature scheme is currently under standardization on the applied crypto working group in the Decentralized Identity Foundation.

BBS+ draft spec on DIF: <https://github.com/decentralized-identity/bbs-signature>

### ***Bottom-up trust structures w/ KILT VCOs***

**Session Convener:** Antonio Antonino

**Notes-taker(s):** Antonio Antonino

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

Slides link (feel free to comment): [https://docs.google.com/presentation/d/1Um-f2UO-sQ3Z4dxy0ZG4Sc3iKe\\_glK3eDMlyEMgXodg/](https://docs.google.com/presentation/d/1Um-f2UO-sQ3Z4dxy0ZG4Sc3iKe_glK3eDMlyEMgXodg/)

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

- There are edge cases to smooth out in terms of abuse by malicious curators, and what governments can do to a VCO as part of the regulatory process.
- Potential for application in a lot of use cases, where trust in the organization can be used by the single members (experts).
- Changing the structure of the bonding curve after the VCO creation might be a good way to adjust the structure of the VCO “on course”, like in real companies.

## SESSION #8

### *ISO Mobile Driving License - Convergence for Adoption? - Fireside Chat Format*

**Session Convener:** Andrew Hughes

**Notes-taker(s):** Tobias Looker

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

Convergence?

Divergence?

Coexistence?

Andrew Hughes

- Introduction on the current state of ISO mDL 18013-5 work and the adoption going on within the U.S DMV's led by AAMVA
- However ISO mDL 1013-5 being CBOR based is often difficult from an adoption perspective particularly in the web

Wayne

- We are working on open source mDL implementation
- Topics that we want to discuss is verifiable credential interoperability

Loffie

- \*Andrew introduced\*
- As a representative of AAMVA, what the issuing authorities are looking for is something that is interoperable
- If we go digital I want to have the same assurance, if i follow this standard I should be interoperable
- Needs to work in attended and un-attended usecases, un-attended still working on
- Recognition that "MDL" can be in multiple formats

Kristina

- Lets not limit to drivers license why not other forms of government ID?
- 18013-5 is strict towards drivers license but ISO 23220 is more general
- mDL is mainly about proving driving priv's not factoring in that it can also be used for strong identification purposes

Wizard

- What happens when someones driving priv's are revoked?

Adrian

- In the U.S context we have the concept of notary
- How do you think we factor in this important aspect?

David

- There is some work going on with ISO 18013-5

Paul

- My observation is that is coming from a usecase of offline attended and VCs are in online and the technologies are coming together

Kristina

- I dont think comparing VC data model and mDL is not a direct comparison, mDL also defines a protocol

Nikihl

- I suspect some form of digital drivers license credential that will have a bunch of usecases where it will be applicable, who do I need to influence to bring the relying parties and what is the roadmap.

Loffie

- The iso work recognized that it goes beyond a drivers license
- Multiple other states are in progress to roll out

Kerrie

- my question was related to realid but we can move on

Andrew

- If you are getting the impression the deal is not done about mobile eID, then your right you have a chance to influence it
- For example if there is an openid issuance protocol that can be taken back to ISO then we should have that conversation

Gail

- OpenID has a liason agreement to ISO if you want to participate

Paul

- Comments about cross-jurisdiction trust of that mDL

Loffie

- I have more to

Wayne

- I want to talk about holder empowerment
- Very difficult to access all the API's required to ISO mDL implementation, differs across Android ISO
- These are operability interfaces can we come up with a wish list

Gail

- I think from a first principle about what government ID is utility of government ID's

Kim

- Talked about concerns around apple control aspects and some of the concerns around the CCG

Loffie

- Issuing authorities have the exact same view, they are concerned about the market share
- The idea that perhaps these vendors need the DMVs more than DMV's need them

Chris

- Anyone here from blueink.ca? \*no\*
- We did an interop project on aries and blueink.ca ISO mDL 18013-5

Kristina

- How did you interop?

Chris

- Blueink.ca were and bridging to VC

Andrew

- Means they are not signed by the original issuer

Nickel

- Quick question for David, you're working with the DWV in UTAH what is the top issue the DMV is kept up at night

David

- What is keeping them up at night, there is massive mis-understanding about what they intend to do with drivers licenses
- DMVs don't want to track users where they use their drivers license or state troopers don't want to persist the information after the transaction

Kristina

- To follow up on VC mDL, the issuers issue credentials in multiple formats, CBOR for inperson and some other form for over the web because CBOR is less adopted or understood
- Maybe issuers do not want to issue two in the beginning but that seems like the pragmatic solution
- Where you get the public key to verify a drivers license AAMVA is working on that
- 23220 is where over the web mDL is being shaped

Kaliya

- I want to just state, super concern this real deep worried that apple and google own the mobile operating system and therefore limiting the options around wallet and holding choices in the ecosystem
- Encourage you to look at some of the work going on at TOIP about metatrust systems including john walkers work with GCCN

Gail

- I think there is a real recognition that there is a real tension in the technologies being proposed and also the principles we want it to yield
- How do we solve for the public private conversation we need to solve for both.

Brent

- I wondering two things, is there a set of capabilities that would be needed to change to the verifiable credentials spec to just be a VC, is the mobile drivers license meant to be a identity credential?

Andrew

- Yes no maybe depends on your def of identity credential

Adrian

- I want to put a privacy spin on what david said about Utah DMV, is that the standards are going to make surveillance more do-able, even if their stated intention is not

Loffie

- Building on top of the ISO 18013-5, AAMVA has published a document that stipulates some of the privacy safe guards like you should not track

Kaliya

- I think the conspiracy theory in identity is growing and we need to tell a better story to dispell these myths
- We need to look at things like what BCGov did with their public services card to increase transparency in the public about how these technologies work.
- We have to fight the conspiracy theories with open information

### ***TPM Tutorial - Using it for User ID and Device ID***

**Session Convener:** Monty Wiseman

**Notes-taker(s):** None

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

**This session was a tutorial. All attendees agreed posting the slides with links to convener for questions would be sufficient.**

**Link to slides:**

[https://drive.google.com/drive/folders/11xHShre\\_Q9S9YEdCwrqEYcMzXWxWEluW?usp=sharing](https://drive.google.com/drive/folders/11xHShre_Q9S9YEdCwrqEYcMzXWxWEluW?usp=sharing)

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

## ***SSI Solutions: Risks, weaknesses and trade-offs***

**Session Convener:** Mawaki Chango

**Notes-taker(s):** Mawaki

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

A dozen people got together to discuss the topic of this breakout session. In the end, we couldn't dive into the full range of sub-themes (risks, weaknesses and trade-offs) but mainly adoption and roadblocks to adoption.

Three main levels of deployment were identified as needed for SSI implementation/adoption:

1. Organizational and enterprise level for their employees;
2. Nation-state governments for their citizens; and
3. The Internet users at large.

Each one of those levels will need a specific approach for adoption. The first one (organizations and enterprises) might be relatively easier, at least wherever the terms of a cost-benefit analysis are quite obvious.

The second one needs appropriate answers to governments and policy makers, in line with their "traditional" concerns for control, security and legal accountability.

And the last one may still be the wild card here, as it obviously requires intermediaries one way or another (just like the first two levels) but so far, only digital wallets hold that place. Will digital wallets be enough to also fill the institutional vacuum or replace it altogether?

In the end, it was observed that significant progress is still needed on three main front:

- a. Solidification of standards (keep building, improving and consolidating the standard/logical infrastructure);
- b. Improving interoperability; and
- c. Major vendor involvement.

Participants in the session are welcome to add more from our proceedings, which might be missing from the above notes (wasn't easy to hear everything, as we were in a corner of the open space) and the Workshop attendees are welcome to comment.

Thank you!



## ***KERI and/or Ledger (Part 2)***

**Session Convener:** Richard Esplin

**Notes-taker(s):** Richard Esplin

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

Continuation of the discussion in Session 5 Breakout K.

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

### Intro

I need to advise my clients on when, if ever, they should use a distributed ledger. And I need to advise my clients on when, if ever, they should use DID:KERI or other ledgerless DID method.

In our discussion yesterday, we listed some reasons to prefer a ledger to alternatives such as KERI and Orb. These reasons each leverage the fact that ledgers contain a publicly auditable history.

We continued the discussion at dinner yesterday, and we learned that the KERI event log is sufficient to meet many of these use cases. So I'm back to wondering how to advise my clients.

What is a blockchain?

KERI uses a BFT consensus mechanism to ensure that witnesses and watchers have a common understanding of the current state of the event log. But each collection of witnesses store their own chain of events. The Key Event Log (KEL) for each DID is like a blockchain which only allows a single author. The witness pool is a set of nodes that manages multiple KELs.

The relevant characteristic for this conversation is that blockchains have shared data and shared governance.

### Conclusion

It doesn't have to be an either / or. Often customers will use KERI to store DIDs on a ledger.

Customers should use KERI when they are concerned about ledger independence.

- did:keri lets you store DIDs on any ledger or no ledger, and you can migrate DIDs between ledgers without having to reissue credentials.
- did:keri is a protocol, and not a storage format. It might be easier to get an ecosystem to standardize on a protocol, and you don't have to argue about which blockchain is the best.

You get these benefits with an increase in complexity that is largely encapsulated within open source libraries such as those provided by GLIEF.

Customers should prefer KERI when they are suspicious about ledgers.

- KERI witnesses can be hosted in cloud infrastructure, and not require any ledger. This avoids the conversation about web3, ledgers, tokens, and regulatory concerns.

Customers should use a ledger (maybe with did:keri) if they don't want to setup their own witnesses or watchers.

- Or they could use a public watcher network (once one exists).

Customers should use a ledger (maybe with did:keri) when they need to leverage other ledger capabilities beyond DID Docs, Revocation Registries, and Service Endpoints.

- Smart contracts (often for automated ecosystem governance)
- Token incentivizes
- Payments

If your ecosystem has already settled on a ledger, then KERI might not be worth using.

### Other findings

KERI and Orb were both created to solve “the ledger adoption problem”. Many organizations are hesitant to adopt a ledger, and those that are willing need to agree on which of the many options they will use.

KERI solves this problem by creating a protocol that has many of the aspects of a ledger. But as a protocol, it is more flexible. Each protocol instance can have its own governance framework.

- KERI consensus can be simpler because the DID controller is the only writer.

However, KERI does introduce some of the complexity that a blockchain already addresses.

- Our community needs more cryptographers and security people to help audit protocols and how we use ledgers.

KERI is vulnerable to “eclipse attacks” where the attacker prevents the client from seeing part of the network when making a query. But so are ledgers.

It is expected that people will create networks of watchers (super watchers) who publicly monitor as many KELs as possible in order to detect duplicity.

- This would be similar to services like the SSL Certificate Transparency Project currently run by Cloud Flare, Google, and others.
- KELs have state proofs, so can provide assurances to clients who are not running their own nodes.

KERI does not allow anchoring an issuer DID on multiple ledgers at a time (that would fork the event tree), but the KEL can be updated to change DIDs from one ledger to another in a serial manner.

KERI doesn't provide the economic incentives that token enabled ledgers address. Those incentives will need to be provided outside the protocol (governance framework, business model, commercial service, contracts).

Orb supports the same features as KERI except for:

- Presigning the next key for rotation (need to confirm that it isn't there)
- Multi signatures

## ***DiD Science an analysis of global DiD Data***

**Session Convener:** Zaida Rivai

**Notes-taker(s):** Markus Sabadello

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

DIDs, DID methods, data science

**Slides can be found here:**

<https://drive.google.com/file/d/1Giob9K3AtLGJ8PajMrqoZr4RUhPLpcSE/view?usp=sharing>

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

Presentation of global DID data:

- Pie charts (e.g. distribution of verification methods within a DID method)
- Time plots (e.g. popularity of a DID method over time)
- Error rate in DID documents
- Duplicate key detection

This is only possible for DID methods where all DIDs are globally visible (e.g. blockchain-based)

Discussion if statistics are also possible for resolvers (e.g. what DID methods are commonly being resolved). Answer: Statistics could be generated for individual DID resolvers (e.g. <https://dev.uniresolver.io/>), but that would only be a local (not global) view.

Why are there so many errors in DID documents, how do communities respond to that?

Suggestions:

- Could differentiate based on testnets and mainnets
- Could create a timeplot of errors over time

## ***Webauthn, WebOTP, FedCM, Password managers - what is their relationship(s)?***

**Session Convener:** Heather Flanagan, Tim Cappalli

**Notes-taker(s):** Heather Flanagan

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

ICloud keysync security white paper - useful reading

To continue the conversation, the W3C Webauthn working group allows anyone to post in the repository.

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

Webauthn - most people in the room are familiar with this

WebOTP - one time passwords that will let phone numbers and email addresses be verified by exposing web platform APIs. Currently over SMS but there is a proposal for email. Launched and in production.

FedCM - a browser API being developed by google to allow federation (OIDC, SAML) to continue to work as browsers overall move towards more privacy protection. It does this by preventing tracking from impersonating themselves by using the API. In Chrome Origin Trials on Android; will be on desktop in next

What do password managers have to do with this? They also help manage credentials.

We have a spectrum of credentials and accounts

```
Assertion with claims
  Assertions about authZ
Credential <----- (what gets returned) -----> Account
PW manager      FedCM
OTP              OIDC
Webauthn (1:1)   SAML
SSI
```

With Webauthn, they wanted to make the credential usable across platforms and devices. Account recovery and cross-ecosystem authentication should be covered by FIDO. They have to be presented across platforms, but not moved across platforms. Portability of keys is not in scope.

WebOTP is a way to bring it full circle; it's not an authentication. It's form-fill, and closer to password managers.

NASCAR wallet / IdP selection? FedCM will partially address this (?) Idea to take the FIDO stack, run the browser side in parallel to invoke a wallet and allow the CTAP to present it from other devices.

Webauthn lives in W3C with a dotted line to FIDO  
CTAP (browser to client)

If Webauthn and pass keys become broadly used, does that replace the NASCAR problem entirely? Webauthn are not identity. Identity attributes need to be verified in a way that Webauthn couldn't handle.

You can ask for FedCM and Webauthn at the same time.

Worth noting that the “credential” in the name Federated Credential Management is about the idea of a browser credential, which is not the same as an identity credential.

Regarding the idea that Webauthn replacing federation - even with first party relying parties, you're still going to be using federation between those entities. You want people to log into Google, not YouTube.

When pass keys are awesome, will we still expect to see “sign in with Google, Facebook, etc”? Yes, you're just pushing to a different part.

As a student that gets an email that says “come get your credential” and then the user has to pick what wallet to store it in - how will that work? The OS will need to understand the basic PE response and respond with the right wallet. Can this be handled at the browser level instead? Maybe. It could be both, but for consistency, probably want it at the OS level so that apps and browsers behave the same.

Why is it compelling for RPs to get their claims in new ways rather than in ways they've already implemented? They're getting claims from multiple sources at once and not the same place at once. This is a completely new mechanism; if we added something like a wallet picker to FedCM, RPs could use existing mechanisms. It needs to be compelling to RP developers. It will also allow RPs to use “expensive” credentials (like driver licenses) that they wouldn't otherwise be able to use. The existing claims are coming as SAML assertions, id tokens, and they contain claims that the IdP is asserting. We're talking about new kinds of claims offered by new sources; that distinction matters because we don't have that ecosystem today. If RPs want new, verified sets of claims, they will write code. The IdP won't have to hold all the info.

What is the compliance statement? What is the risk? What kind of regulations will impact this?

Why wouldn't we reuse OIDC to transport verifiable credentials? Because of the NASCAR problems.

Credential Handler API (CHAPI) is in browserland, existing as a polyfill (JavaScript code that mimics browser UI), exposes 3 API calls - register a wallet and get a credential and store a credential. Would be another thing to explore.

The term “wallet” is getting overloaded. You shouldn't have to be a wallet but you can be an app that can serve wallet content (e.g., Avis app holds insurance info and acts as a wallet for this particular piece of info)

## ***Identity in the Supply Chain: GS1 Verification Library PDC and Future Use Cases***

**Session Convener:** Yousuf Hossain, Andy Meyer, Paul Nicolard

**Notes-taker(s):** Andy Meyer

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

GS1 US Verification Library

Question How do you prove the authenticity of your pharma product through the supply chain.

Proof of concept project.

Built a library of data that was created by the product owner and made accessible for verifiers of data.

Pharma ledger is EU based blockchain project.

Why build the library at all, to create a verifiable chain, that would denote which world region / company / product through chain of custody, to prove out that the product is safe and correct for customer use. if one data point was off the product would not pass verification.

Technical:

Key vault: store key for the manufacturer

Credential server: Allows the push pull of credentials used for verification.

Pharma ledger App: for customers to fetch and verify the credential

Utilize digital bazaar. Default web SSLs

Went with index based revocation list which is cached on phone.

Challenges:

Ecosystem is in flux so which DID method to use? Went with DIDWeb.

No standard wallet because most are custom built and mission specific.

Time to market.

Library challenges:

Mobile use and inherent size restrictions, used webpack to overcome.

Revocation:

Approach to credential chaining and the AC DC discussion have been very interesting.

API responses: originally used default responses and have had to evolve.

Private Key management: currently use Azure Key vault but is not scalable.

Caching: had to develop homegrown caching process.

Q: Did GS1 look at a GS1 DID method? No time to market was key.

Q: Why does GS1 develop standards for this are they planning to move this past proof of concept?

If more companies are willing to adopt and more use cases are identified, they will move past proof of concept.

-

Any feedback on verification libraries?

Q: What is it that you are adding on top of the digital bazaar?

Certain standards around verification and the caching method. Additional standards related logic.

## ***We ran a survey for SSI vendors: Find out what we found!***

**Session Convener:** Fraser Edwards **Notes-taker(s):** Fraser Edwards

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

<https://blog.cheqd.io/understanding-the-ssi-stack-through-5-trends-and-challenges-b15e911b4989>

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

- Session used the blog published above as the base material
  - The blog also references the underlying data we collected

**Questions:**

- Who participated:
  - 0. Participation was anonymous but cohort came from existing cheqd partners which should be easy to find on the website / cheqd materials
- Should we just move to OIDC SIOP over DIDcomm?
  - 0. Largely down to requirements / functionality required. OIDC SIOP appears to be seeing adoption due to potential to make adoption for relying parties easier but it ultimately comes down to requirements / functionality
- What are the equivalent 5 blockers or enablers for web3 / crypto adoption?
  - 0. Awareness, web3 / crypto is not aware enough right now
  - 1. Easier development experience, reason NFTs are seeing adoption is ease of creation
  - 2. Right use-cases to drive viral adoption
  - 3. *Only hit 3*
- Is the data available?
  - 0. Yes, please see the blog posts
- Did certain countries or industries use specific libraries or protocols?
  - 0. I don't believe we have this but we plan to run the questionnaire again so can include questions like this if there is demand

## ***Machine Readable Governance Code***

**Session Convener:** Mike Ebert **Notes-taker(s):** Peter Conerly / Mike Ebert

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

<https://hackmd.io/@mikekebert/rysGp88r9#/>

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

Some contributors to the session:

Shannon Wells

John Hopkins

Peter Conerly

Ben Goering

Daniel McGrogan



Mike talked about the structure used in the Aruba Health Travel system.

First, there were many pieces of info that could be attached to a user, but it would end with a “trusted traveler” certificate.

There were discussions around the roles in the system and the permissions for each actor or group of actors. I.e. border customs agents would be full access to a traveller’s health data, but a hotel or restaurant would only have access to the “trusted traveller” final result.

It was recommended that Mike’s project could use more standards from NIST.

The discussion wandered into talking about machine readable law and jurisdictional issues.

Here is a list of ideas that were brought up as we reviewed the file format:

Version numbers/linking/lists

Could be quicker to avoid linked lists?

UUID - Why UUID? Could be a DID:Peer?

Topics/Tags - use existing standards/ontologies

Jurisdiction - How to specify? GLEIF?

Geos: specify with GIS/polygons

Activity Streams W3C - Also for actions

Super class actors/properties

Edge/content

Privacy policy URL

TOS URL

Icon/Avatar

TPM/HSM hardware providers?

Governance - include validation of hardware providers and their support of governance frameworks

How do roles work with delegation, large numbers, levels?

ZCAP-LD

UCAN Working Group

DWebNodes (Ask Daniel Buchner)

Actions

Utrecht Netherlands--Using Ontologies for Comparing and Harmonizing Legislation

Computational law

IPLD.io--encode/embed objects in URLs

NIST - Ontology for durations?

Finite state machine

Chain of responsibility

Secure Governance Working Group

## ***Credential Manifest + Wallet Rendering: Getting to V1***

**Session Convener:** Jace Hensely (Bloom)

**Notes-taker(s):** Jace

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

<https://github.com/decentralized-identity/wallet-rendering>  
<https://github.com/decentralized-identity/credential-manifest/>

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

We discussed what would be good to get into the specs before cutting V1 releases. We came up with a few tickets to be discussed further in DIF's "Presentation Exchange/Credential Manifest" WG call.

<https://github.com/decentralized-identity/wallet-rendering/issues/18>  
<https://github.com/decentralized-identity/wallet-rendering/issues/15>  
<https://github.com/decentralized-identity/wallet-rendering/issues/16>  
<https://github.com/decentralized-identity/wallet-rendering/issues/17>  
<https://github.com/decentralized-identity/credential-manifest/issues/89>

**The PE/CM call happens every Thursday at 10am PT, please join!!**

## **SESSION #9**

### ***How to store all your personal data in one place - technology***

**Session Convener:** Johannes Ernst

**Notes-taker(s):** Johannes Ernst

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

Digital Homestead, UBOS Mesh [ubos.net/mesh](https://ubos.net/mesh)

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

Johannes briefly gave the demo again of the UBOS Mesh with his Facebook, Google and Amazon data. Then explained how it works under the hood, and why.

## Dealing with a 1000 SSI Wallets and many more credentials

Session Convener: [Peter Langenkamp](#)

Notes-taker(s): [Peter Langenkamp](#)

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

Link to slides: <https://www.dropbox.com/sh/ndtw8sm8iekktaC/AADl-Fersz0ko8oTqCRYFvLQa?dl=0>

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

Discussion on the idea of an **SSI Wallet Gateway** and need for a **credential catalog**.

**The SSI Wallet Gateway** service facilitates the adoption of SSI by providing an easy to use API, that allows credential issuing and/or verifying organization to integrate multiple SSI wallets—that may be based on different underlying technologies—with a single interface, taking inspiration from the payment service provider model for online payments.

The approach in our current implementation to letting the holder select a wallet might not pass the grandma test. Especially as the number of supported wallets grows.

A more manageable approach would be to support ‘profiles’ instead of wallets

- More wallets speaking the same language → same number of profiles, so scales way more favourably (also for keeping the interface clean)
- How to do this with an intuitive UX is an open question (a normal user will not necessarily know which wallet(s) can be used with which profile)

A browser polyfill extension could maybe help solve the problem

Experience acquired in the process of making this Gateway service work could be very helpful in standardization efforts, like work on a Verifier Universal Interface started under eSSIF-Lab which was recently transferred to DIF

**A credential catalog** helps facilitate the discoverability of credentials on offer by issuers. It should list not just the schema of credentials (*credential type*), but also their technical implementation for specific protocols (*credential implementation*) and importantly relevant information about assurances, liability of the issuer and other details specific to the credential type as offered by a specific issuer (*credential offer*).

Figure out status of VC Marketplace and get in touch!

Challenge in identifying schema’s that are essentially the same in meaning

The credential catalog is meant to list what type of information issuers issue, not details about individual issued credentials.

## ***CESR - Composable Event Streaming Representation / CESR Proof Signatures***

**Session Convener:** Sam Smith, Phil Fearheller

**Notes-taker(s):**

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

[https://github.com/SmithSamuelM/Papers/blob/master/presentations/CESR\\_Overview.web.pdf](https://github.com/SmithSamuelM/Papers/blob/master/presentations/CESR_Overview.web.pdf)

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

## ***Hyperledger 101***

**Session Convener:** Daniela Barbosa, Hart Montgomery, Sean Bohan

**Notes-taker(s):** Sean Bohan

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

Website: <https://www.hyperledger.org/>

Wiki: <https://wiki.hyperledger.org/>

Discord: [discord.gg/hyperledger](https://discord.gg/hyperledger)

GitHub: <https://github.com/hyperledger>

Deck: [Getting Involved With Hyperledger](#)

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

- Hyperledger Foundation: hosts open source enterprise blockchains projects, from DLTs to tools
- Most relevant to IIW, we host Hyperledger Indy, Aries and Ursa
  - We also host Hyperledger Besu, Fabric, Sawtooth, FireFly, Caliper and others
- Hyperledger Foundation is part of the Linux Foundation
- All of our code is Apache2 licensed, free for anyone to take and use
- The projects are powered by contributors, maintainers and members. Anyone can contribute to a project and contributions are welcome.
- Hyperledger has a steering committee which drives the technical direction of the entire org
- Within each project, the maintainers/contributors are responsible for project health, determining direction and roadmap
- Many projects have a “good first ticket” in GitHub

## Web3 Credentialing for TODAY's Webb Wallets

Session Convener: Oliver Terbu  
Notes-taker(s):

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

WEB3 CREDENTIALING  
W3C CREDENTIALS

Rea:

- optimize for DevX
- optimize for UX
- leveraging existing web3 wallets

Potential User Stories:

- 1 (d)App b Blockchain Acc issuance
- 2 Blockchain Acc to Blockchain Acc iss.
- 3 ~~Blockchain Acc~~ b (d)App ~~iss.~~ pres.
- 4 DAO b Blockchain Acc iss.
- 5 DAO rep to (d)App presentation

Signing JSON RPC:

- EIP-191 personal sign
- EIP-712 sign typed data
- EIP-4361 Sign-in with Eth

\* *Ethereum EIP712 Signature W3C CCG 2021*

① (did:pkh:eip155:1:0x...) — *W3C CCG*

- 1 connect WALLET → Eth Acc
- 2 ~~TRANSFER~~ Eth Acc as did:pkh
- 3 (d)App issue VC b did:pkh

②

- 1 connect WALLET → Eth Acc
- 1.1 LOGIN w/ Eth Acc
- 2 TRANSFER Eth Acc b did:pkh
- 3 Create VC payload acc. EIP-712
- 4 Vg. 712 sig

②

- 1 eq
- 2 eq
- 3 ~~CREATE~~ Create or obtain delegator DID
- 4 SIWE + new DID + permissions

⇒ ZCAP: did:pkh b new did w/ permissions

5 issue VC: iss: did:pkh  
sub: did:pkh  
pref: ZCAP

③ Same as ② but w/ VP instead of VC

③

- 1 CONNECT
- 2 eq
- 3 SIWE + delegation
- 4 Retrieve from VC Store
- 5 CREATE VP w/ ZCAP for HOLDER BINDING

④

- ④ EOA from Delegation Binding to ~~signatures~~ issue ②
- ⑤ EOA VCs from SAFE owner

⑥ ~~old more validation methods b no doc~~

## ***Blockchain vs. “The Right to be Forgotten”***

**Session Convener:** Jeff

**Notes-taker(s):** Peter Conerly

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

**\*\*slides exist\*\***

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

“The right to be forgotten” is referred to as “the right of erasure” in europe

1. The inherent conflict between blockchains and privacy.
  0. Privacy vs. immutability
2. Rethinking immutability
  0. “Versioning” on the blockchain
    1. Can it be like a yearbook?
    2. What about a bank statement? Bank statements have “closing statements”, and they have records of them, but they’re only showing the last ones.
3. Devil in the details
  0. Anytime you change records, the hashes don’t match :(
4. Can you Reshuffle the deck?
  0.  $5 + 0 = 5$ ; but how do you prove [invisible]  $+ 0 = 5$  ?
    1. Can we use Net State at  $t_0$  and  $t_2$  to make sure that the total number of tokens is the same?
    2. Don’t remove any users that don’t have a zero balance? Or you can burn them
5. Receive request to remove user from blockchain
  0. Create new net-state TRX, and append it

“Do we have to hard fork every time we get a request to be forgotten? Because the historical hashes won’t match up.”

“Blockchains have checkpointing, which this first solution is proposing”

Public blockchains may never be regulatable, because there’s no owner. This solution might be more relevant to private blockchains administered by a company.

Is the right to be forgotten more possible in “proof of stake” blockchains? Or at the time of a rollup– a user and their request to be forgotten would no longer exist after a rollup. [Check with Aaron that I got this right.]

You can de-anonymize people like 80% of the time with their age, work zip code, and home zip code.

Practical considerations:

1. These solutions can work with most blockchains
2. To implement, needs approval of the group that governs the blockchain.
3. Covering the cost of the reshuffling will need to be solved by the blockchain governors.

“The thing is that all of these hashes rely on– there has to be an incentive to remine the entire chain. And you have to do it within a certain timeframe. So let’s say that once a month you have to recompute the last 30 days. That’s a lot of compute!”

“I’m worried that the blockchain that implements the right to be forgotten will become less secure. To me it introduces a whole lot of security holes, because the point of the chain is that you can’t change it. Your solution will be way more palpable if we secure what can go onto the blockchain in the first place.”

Aaron talking about using a merkle tree of transactions do potentially support deletion?  
Keep a tombstone of the deleted transaction that records the hash of what the deleted txn was  
Once the block is final, then don’t need historical data and just reference the rollup  
Maintaining the integrity constraints is difficult

There’s a PhD thesis out of Georgia Tech about redactable medical records.

[https://smartech.gatech.edu/bitstream/handle/1853/31676/bauer\\_david\\_a\\_200912\\_phd.pdf;sequence=1](https://smartech.gatech.edu/bitstream/handle/1853/31676/bauer_david_a_200912_phd.pdf;sequence=1)

## **VC in edu**

**Session Convener:** Kerri Lemoie (kerri@openworksgroup.com)

**Notes-taker(s):** Heather Flanagan

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

- [Task Force Page, Meeting Info & Archives](#)
- [HTTPS://gainforum.org](https://gainforum.org)
- [Building a Skills-Based Talent Marketplace: Verifiable Credentials Wallets for Learning and Employment](#)
- [VC-EDU Use Cases Document \(Draft in Progress Google doc\)](#)
- [Open Badges 3.0 Proposal](#)
- [Open Badges 3.0 VC to DCC Learner Wallet Demo](#)
- [Inclusive Design Principles for Learning and Employment Records: Co-Designing for Equity](#)

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

What’s going on in education with verifiable credentials.

This is a task force of the Verifiable Credentials CG, currently working on:

- use case doc
- Recommendation as to how those use cases could be applied as VCs

It’s a mix theoretical discussion and field reports. Focused on education in a very broad way. Education is broadly defined as lifelong learning, informal learning, formal learning, etc etc etc. The work is global in scope.



Some consider the VC space “not fully baked”. That is a common perception, and so the pilot projects have focused on on-ramp and interop with existing systems.

The standard for VC is not seen as fully-baked because the spec itself is not well-specified, much is marked non-normative, and the normative text is not prescriptive enough for companies that need stability to trust it or to understand how to implement it.

Open Badges is a related spec, possibly considered a use case; VCs could align to Open Badges, but that’s a work in progress.

On the CLR side, North Dakota uses it for K-12 transcript. It is comprehensive in that there is more than one assertion for the learner.

There is also development being done around an endorsement credential (HR Open Credential). Endorsement required cross-credential crypto binding. Verifiable Presentation does not actually allow for this - they are authenticating the holder, but not the issuer, and it does not provide crypto binding between two credentials.

Student id as an example: some deployments implement as a model of a credential, and some implement a student ID as several interlinked, cryptographically bound credentials.

The Diploma Supplement in the EU is active work going on with the crypto bound assertions that’s tied to the euro pass work.

Focus seems to be on transcript issues, but the higher ed space needs a much broader set of use cases. Example: interactions with content publishers. Publishers are still largely using IP addresses to authorize access to content. We have to look at ways we can solve problems like that, too.

There also use cases focusing on the licensing of teachers.

People are digitizing all the things, so it’s in our interest to get that into individuals’ control.

Are there trust registries for issuers? Haven’t solved it, but have bumped up against it. There is a project called GAIN (see link above) that might be of interest. Also, should education accreditation bodies be the same entity of entity that should act as a trust registry for VCs?

Considering large publishers as an unethical model, we should be supporting OpenAccess publishing. So let’s not talk about how to support publishers with VCs and instead focus on more interesting use cases that support humanity.

Is there any discussion about how to transition the earlier versions to newer versions of OpenBadges? Yes, they are backwards compatible.

There are levels of interoperability, the issuer and the skills.

A question about if/how AC/DC relates to this work (re: issuing linked credentials). The VC group is focusing less on the envelope and more on the content.

## ***Presentation Exchange W3C VC's***

**Session Convener:** Daniel Buchner

**Notes-taker(s):** ?

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

<https://openid.bitbucket.io/connect/openid-connect-4-verifiable-presentations-1.0.html#name-anoncreds>

<https://openid.bitbucket.io/connect/openid-connect-4-verifiable-presentations-1.0.html#name-iso-mobile-driving-licence->

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

- Presentation Exchange is designed to work with W3C Verifiable Credentials
- Implementation Experience shows it can be used with other credential formats as well, examples are AnonCreds and mDL
- In order to support other formats, PE should have some extensibility to allow implementers to define no format and proof type identifiers
- Discussion of use of IANA registries for that purpose
- Daniel Buchner agreed with this way forward, Mike Jones offered help as he has done this several times already

## ***Interoperability is dead! Long live interoperability! An open discussion***

**Session Convener:** Alexis Falquier, Riley Hughes

**Notes-taker(s):**

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

<https://blog.cheqd.io/understanding-the-ssi-stack-through-5-trends-and-challenges-b15e911b4989>

ToIP architecture interoperability working group

<https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf>

<https://www.convenience.org/TruAge/Home>

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

**Slides:**

[https://docs.google.com/presentation/d/1-BngvjuopbE0T7BF7\\_x-29FXSX4ArRvduz1uaWh9G5w/edit](https://docs.google.com/presentation/d/1-BngvjuopbE0T7BF7_x-29FXSX4ArRvduz1uaWh9G5w/edit)

- With so many standards and protocols it is unreasonable to expect full interoperability
- Pragmatism vs idealism
  - Pragmatic approach to building solutions
  - Make credentials and credential solutions usable first then we can focus on interoperability
- Interoperability is still important, but must not bog down development of solutions
- What does interoperability mean?
  - Lower the scope of interoperability to basic ecosystems
  - If you're not interoperable with everyone that's ok!
  - Focus on your use case, then your ecosystem, then your industry, then anything beyond that
- Interoperability as a view of islands
  - Be interoperable with your island
  - Don't shun and shame other islands (other standards)
- Architect your solution to be interoperable in the future
- Another way to view how we should view interoperability:
  - Practical portability



## ***Supply Chain Traceability***

**Session Convener:** Nis Jespersen (Transmute), nis@transmute.industries and Mahmoud Alkhraishi (Mavennet), mahmoud@mavennet.com

**Notes-taker(s):**

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

Supply chain schemas, built from existing vocabularies. Interoperability proven with continuous integration.

supply-chain, traceability, did, vc, json-ld, json-schema

### **Links**

<https://github.com/w3c-ccg/traceability-vocab>

<https://w3c-ccg.github.io/traceability-vocab/>

<https://github.com/w3c-ccg/traceability-interop>

<https://w3c-ccg.github.io/traceability-interop/>

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

Join the repos and Tuesday meetings!

## ***Verified Connections***

**Session Convener:** James Ebert **Notes-taker(s):**

**Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:** No Notes Submitted

## ***How To NFT ME! - Secure My Personhood***

**Session Convener:** Pamela Norton **Notes-taker(s):**

**Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:** No Notes Submitted

## SESSION #10

### ***Vaccination Certificate Chained Credentials Privacy Aware Presentation & Presentation Exchange -over- http(s)/ Ronald Koenig***

**Session Convener:** Ronald Koenig

**Notes-taker(s):** Ingo Wolf

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

Covid credentials, privacy aware

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

Ronald presents the background and outcomes of our intermediate project results within the IDUnion project in Germany.

Privacy issues today exist when you have to proof your vaccination status e.g. going to a restaurant and additionally disclose your identity from your passport. Furthermore there is a central service signing all covid certificates, which provides no utils to revoke those certificates on an individual basis.

Within the project we developed a prototype, that enables:

- combine credentials via holder binding in order to have a single presentation (id credential + vaccination credential)
- selective disclosure with BBS+ signatures concerning your personal data (no need to provide your name, when entering the restaurant)
- using an indy ledger as a trust anchor for issuers (root of trust)
- credential chaining applied to express the delegation of authority to issue vaccination credentials from a single root of trust to all doctors' agents

Questions:

Chris asks: is this applicable to distributed/not centralized regional health structures (like in UK)?

Could you technically delegate the authorization with multiple chain elements?

Ronald: yes. You can do that.

Luke: is it comparable to X.509 certificate chaining?

Ronald: It's similar, but technologically different, based on VCs/VPs. Authorizations are more explicit.

How do you know that the data belongs to the person presenting to the verifier?

This is realized via device binding and the device is protected by biometric authentication of the user.

Is this also usable for the EU certificate actions? Not yet, this is a research project. It is currently a prototype, but not in production.

Is this applicable to other scenarios than issuance at the point of care?

Yes it is possible to extend the use case, but we started with the approach of integrating it into healthcare systems at the PoC.

What challenges did you phase?

Heterogeneity of technology in the SSI techspace (many solutions with limitations and rare interoperability)

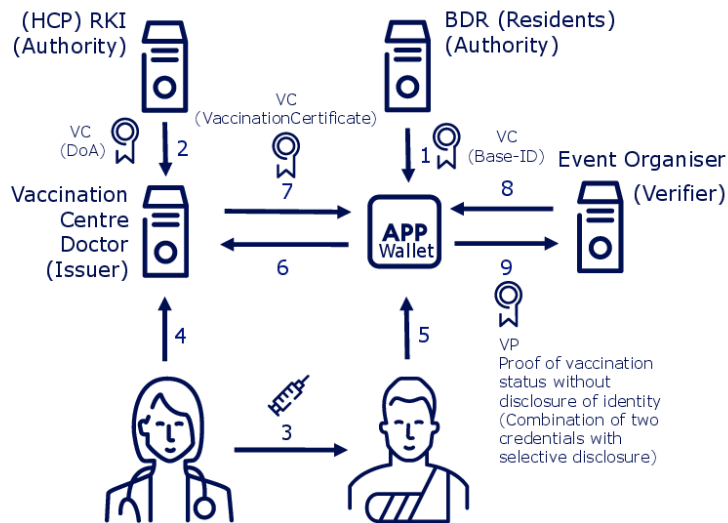
How does the solution impact the workflow in the doctors office?

Minimally: the doctors document the vaccination event as before and a QR code is presented to the patient, that scans it to import the credential into his wallet.

Presentation exchange over https was not presented due to time restrictions.

Slides:

## SSI vaccination certificate



gematik

28.04.2022 Use of chained credentials in vaccination certificates | Berlin

1

## Added value



### One wallet for all credentials

- User acceptance
- Operational and maintenance costs
- Increased security



### Combination of credentials

- Automation of verification - reduced verification effort
- Increase of level of assurance for verification
- Increase of user acceptance



### Selective disclosure of personal information

- Informational self-determination
- Increased user trust
- Increased user acceptance



### Reuse of standards (DIF, W3C, Aries)

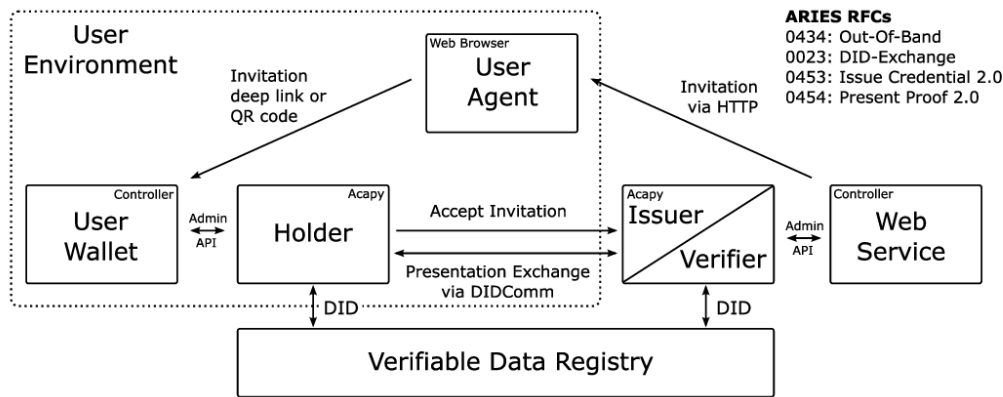
- Interoperability
- Reusability
- World wide community

gematik

28.04.2022 Use of chained credentials in vaccination certificates | Berlin

2

## Aries protocol stack

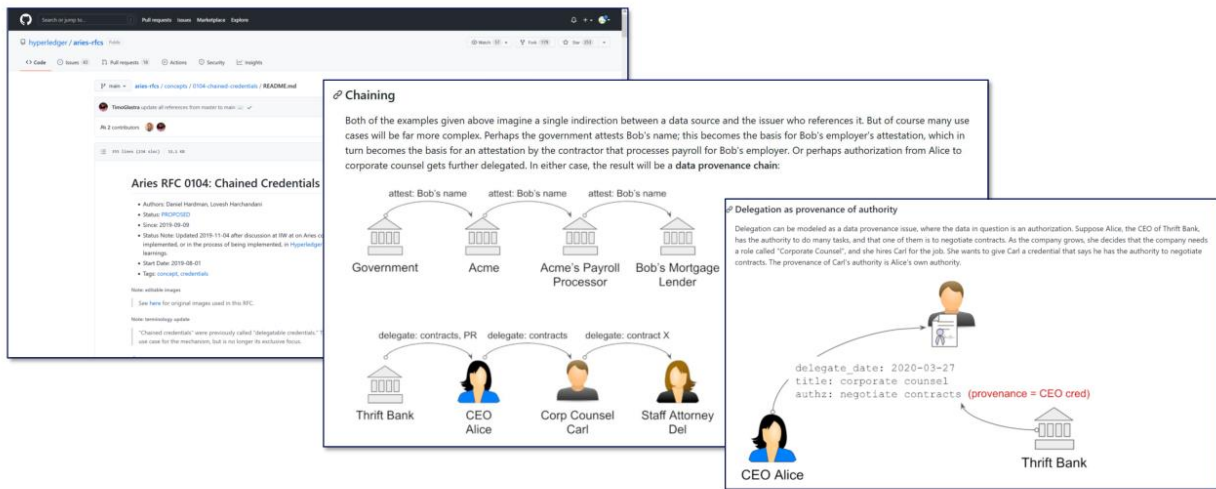


gematik

28.04.2022 Use of chained credentials in vaccination certificates | Berlin

3

## Aries RfC 104: Chained Credentials



Source:

<https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0104-chained-credentials/README.md>

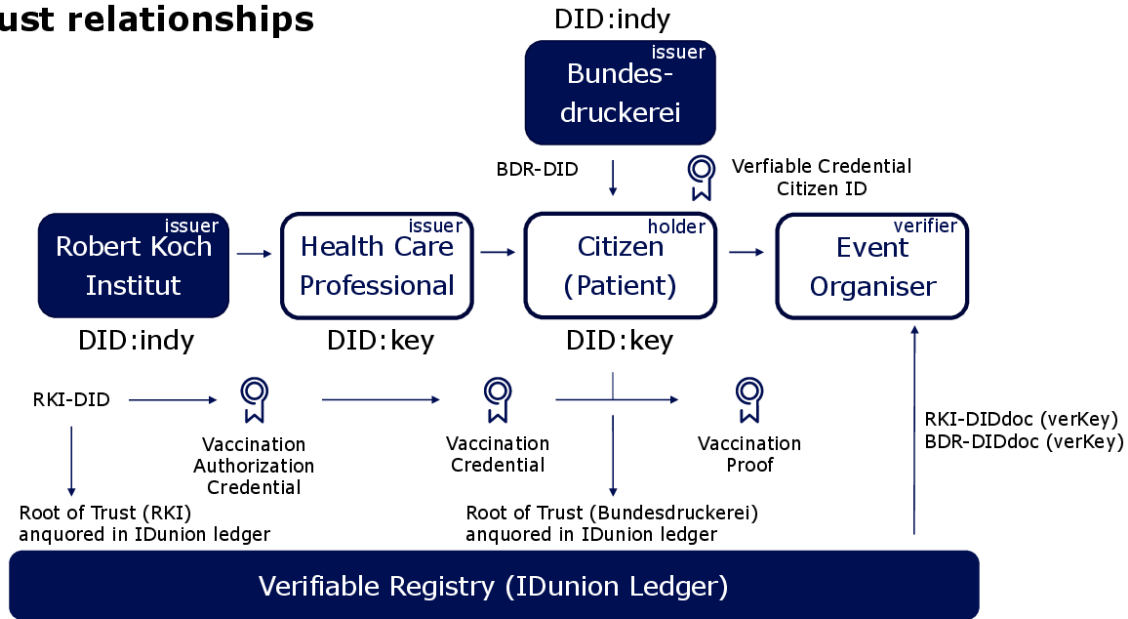
gematik

28.04.2022 Use of chained credentials in vaccination certificates | Berlin

4



## Trust relationships



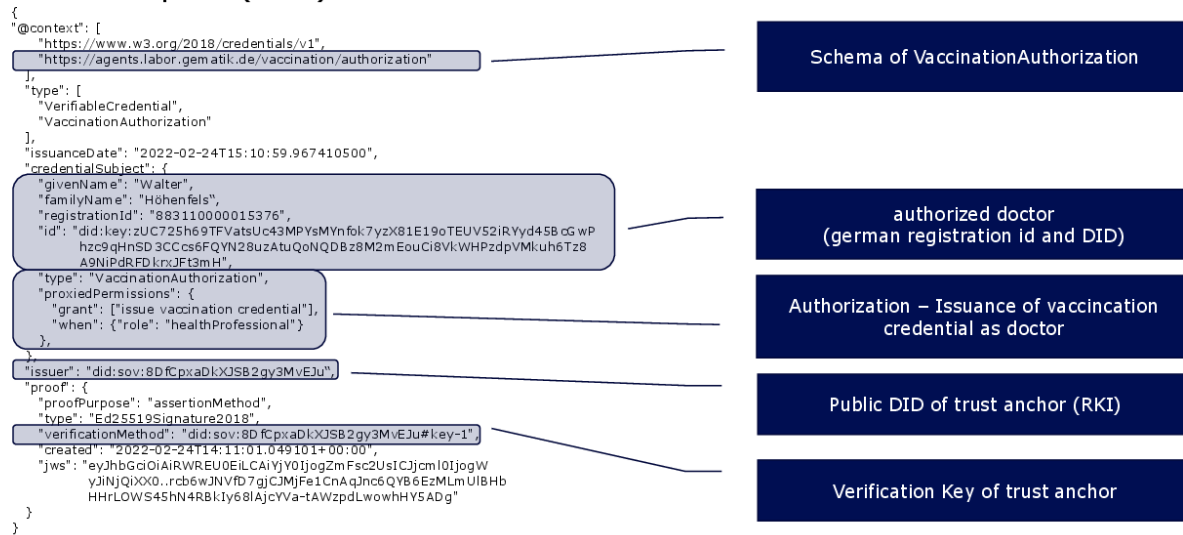
gematik

28.04.2022 Use of chained credentials in vaccination certificates | Berlin

5

## Delegation of Authority

Trust anchor (RKI) authorizes doctor



gematik

28.04.2022 Use of chained credentials in vaccination certificates | Berlin

6

## Vaccination certificate (context + credential subject)

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/vaccination/v1",
    "https://agents.labor.gematik.de/chained/credential",
    "https://agents.labor.gematik.de/vaccination/authorization",
    "https://w3id.org/security/bbs/v1"
  ],
  "type": [
    "VerifiableCredential",
    "VaccinationCertificate",
    "ChainedCredential"
  ],
  "issuanceDate": "2022-02-24T15:56:12.299317500",
  "credentialSubject": {
    "vaccine": {
      "type": "Vaccine",
      "atcCode": "J07B X03",
      "medicinalProductName": "COVID-19 Vaccine Moderna",
      "marketingAuthorizationHolder": "Moderna Biotech"
    },
    "nextVaccinationDate": "2021-08-16T13:40:12Z",
    "countryOfVaccination": "GE",
    "dateOfVaccination": "2021-06-23T13:40:12Z",
    "order": "3/3",
    "recipient": {
      "type": "VaccineRecipient",
      "gender": "Female",
      "birthDate": "1961-08-17",
      "givenName": "Marion",
      "familyName": "Mustermann"
    },
    "id": "did:key:zUC71CtGWGXC2W3KDDHPM7chVse...AcRrUpz8ZtCbh3UiJQDjeNnPRdgYtcte2X",
    "type": "VaccinationEvent",
    "administeringCentre": "Praxis Sommergarten",
    "batchNumber": "1626382736",
    "healthProfessional": "883110000015376"
  }
},
gematik
```

Schema extension for chained credentials  
(provenanceProof)

vaccination event

28.04.2022 Use of chained credentials in vaccination certificates | Berlin

7

## Vaccination certificate (proof)

```
"proof": {
  "proofPurpose": "assertionMethod",
  "type": "Rhs8Signature2020",
  "verificationMethod": "did:key:zUC725h69TFVatsUc43MPYsMYnfok:7yzX81E19oTEUV52IRYyd45BcGwPhzc9qHnSD3CCcs6FQYN28uzAtuQoNQDBz8M2mEouCi8Vl:WHPzdpVMkuh6Tz8A9NiPdRFDkrxJf3mH#zUC725h69TFVatsUc43MPYsMYnfok:7yzX81E19oTEUV52IRYyd45BcGwPhzc9qHnSD3CCcs6FQYN28uzAtuQoNQDBz8M2mEouCi8Vl:WHPzdpVMkuh6Tz8A9NiPdRFDkrxJf3mH",
  "proofValue": "uL5f84Yc6cUJC5B+C7hHHw7ta5wmRi0XaechTo9HcdWN05xL/ewh37RUI7lkL1MGyA3x/L84gTPV87k:/lyGvVjSEvJnCsNwoO34b0B6G+CAVtCa2/d3TKfi8e+t+OaOCULRqVU/Rj7vUxVKoVCxbkA==",
  "created": "2022-02-24T14:56:13.199532+00:00"
},
"issuer": "did:key:zUC725h69TFVatsUc43MPYsMYnfok:7yzX81E19oTEUV52IRYyd45BcGwPhzc9qHnSD3CCcs6FQYN28uzAtuQoNQDBz8M2mEouCi8Vl:WHPzdpVMkuh6Tz8A9NiPdRFDkrxJf3mH",
"provenanceProof": {
  "proof": {
    "verificationMethod": "did:sov:8DfCpXaDlXJSB2gy3MvEJu#key-1",
    ...
  },
  "issuanceDate": "2022-02-24T15:10:59.967410500",
  "credentialSubject": {
    "id": "did:key:zUC725h69TFVatsUc43MPYsMYnfok:7yzX81E19oTEUV52IRYyd45BcGwPhzc9qHnSD3CCcs6FQYN28uzAtuQoNQDBz8M2mEouCi8Vl:WHPzdpVMkuh6Tz8A9NiPdRFDkrxJf3mH",
    "proxiedPermissions": {
      "grant": ["issue vaccination credential"],
      "when": {"role": "healthProfessional"}
    },
    ...
  },
  "issuer": "did:sov:8DfCpXaDlXJSB2gy3MvEJu"
}
}
```

Doctor asserts  
vaccination event

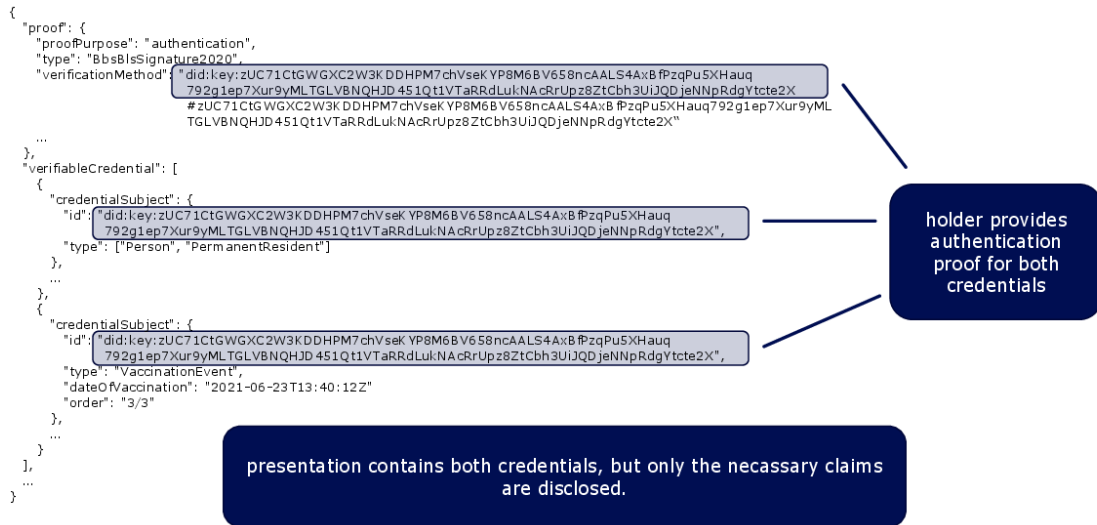
Trust anchor (RKI)  
authorizes doctor

gematik

28.04.2022 Use of chained credentials in vaccination certificates | Berlin

8

## Presentation of both credentials and selective disclosure



gematik

28.04.2022 Use of chained credentials in vaccination certificates | Berlin

9

## Securing API Access with ZKS

Session Convener: Seth Back  
Notes-taker(s): Steve Venema

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

20 attendees

### API Access Threat model

- Tampering with data in transit
- Replay f requests
- Unauthorized access to data
- Exploiting implicit trust
  - (external -> internal / internal -> internal)

### API tokens

- Pros
  - Single token
  - No special computation
- Cons
  - Relies on transport security
  - No request integrity

Public / Secret Token (e.g., AWS token)

- Prosure over specific data
- Without exposing that signature
- In a format that can be publicly verified
  - Secret is actually a secret
  - Request integrity
- Cons
  - Arbitrary connection between tokens
  - Implicit trust / over provisioning access

What do we mean by ZKP in this context (PS Signatures)

- Prove knowledge of a signature

Fixed!

- Sig...

Implementation: Oberon

- <https://github.com/mikelodder7/oberon>
- Rust & Go
- Flexible (use case agnostic)

Trinsic's use

- Login generates "token" tied to the account
- Blinded before returned (2FA / no reliance on transport security)
- Nonce includes timestamp and request hash
- Validation at service level using public key

Ex:

- Oberon ver=1, proof=asdfasdf, data=afafasd, nonce=asdfasdfadf

Q: You mentioned macaroons; can you go into more detail?

A: whitepaper, a way to use hashes on signatures to attenuate authority  
Do a ZKP on the macaroon – seen this used

Q: Combining API keys, access tokens, OAuth2 tokens

Nonce is different each time. Can ...

Biggest value: Never have the API token pass over the wire

C: RFC8749Http structured headers – encouraging use of this in the future

Another version of Oberon coming out

Q: What formats supported

A: You are generating a ZKP of the hash of \*any\* data

## DID URLs

Session Convener: Markus Sabadello

Notes-taker(s): Markus Sabadello

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

DID URLs, DID documents, URIs, <https://www.w3.org/TR/did-core/#did-url-syntax>

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

DID URLs start with a DID, then they can have path, query, fragment.

DID URL syntax components work very similar to HTTP URL syntax components, but sometimes are also DID method-dependent.

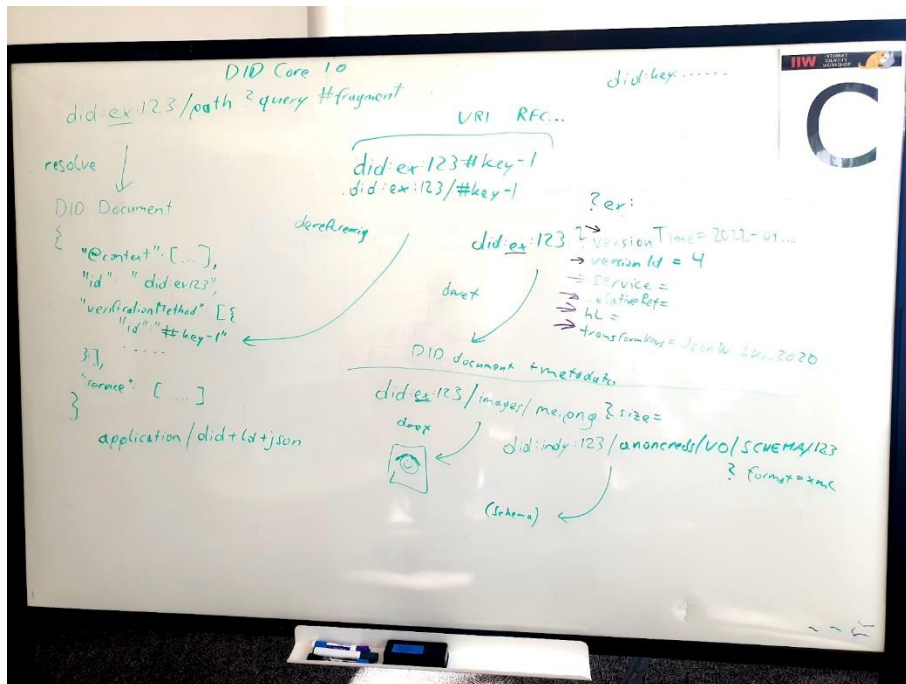
Fragment depends on the media type of the primary resource.

Query parameters defined by DID Core: versionId, versionTime, service, relativeRef, hl

Some examples where DID URLs are used:

- In the did:indy method to reference schemas, credential definitions, and other ledger objects
- By Decentralized Web Nodes (DWN) to reference specific objects inside a DWN.

DID URLs inherit some useful properties of DIDs, e.g. decentralization and persistence.



## Open Trust Claims - Atomic Trust in a Dangerous World - Interactive Hack

Session Convener: Golda Velez

Notes-taker(s):

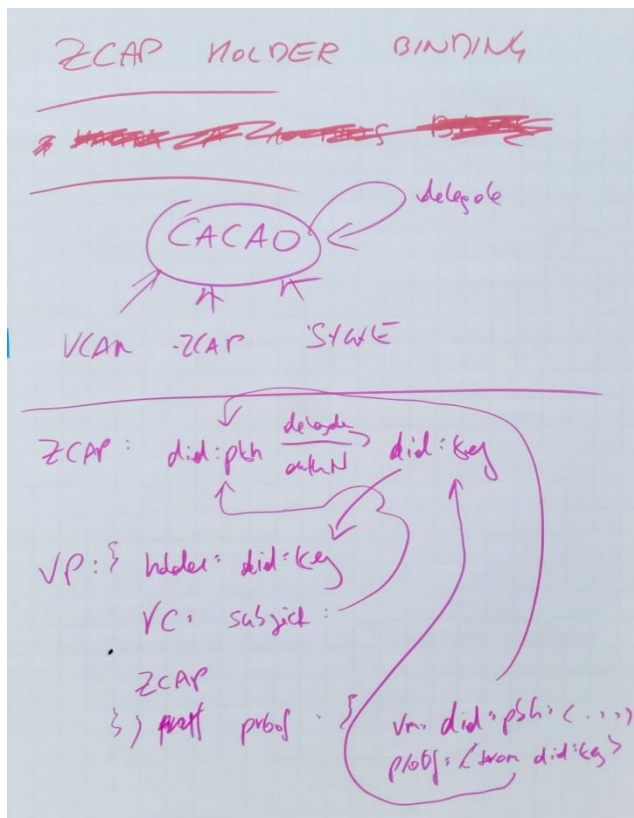
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps: No Notes Submitted

## VP Holder Binding with Session DID through Capability Delegation

Session Convener: Oliver Terbu

Notes-taker(s):

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



## ***DWN Deep Dive - Discussion***

**Session Convener:** Moe Jangda

**Notes-taker(s):**

**Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:** No Notes Submitted

## ***Interchain Identifiers***

**Session Convener:** Joe Andrieu

**Notes-taker(s):** Joe Andrieu

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

[https://legreq.com/pres/DIDs\\_and\\_NFTs.pdf](https://legreq.com/pres/DIDs_and_NFTs.pdf)

<https://w3id.org/earth/Identifiers>

<https://diddirectory.com/cosmos>

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

I shared a presentation on DIDs and NFTs from DID Conference Korea 2022, which describes the motivation and requirements for using DIDs with NFTs, developed for the Cosmos ecosystem, but usable for any on-chain assets, including any and all blockchain-based DID methods.

I also discussed the 14th requirements (not in the slide), versioning. Hardly any DID methods have built in versioning, but for the development of did:cosmos, it was clear that we needed to be able to support breaking changes in the resolution method itself, which required a version.



## ***Credential Formats - What is the Best***

**Session Convener:** Torsten L

**Notes-taker(s):**

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

<https://docs.google.com/spreadsheets/d/1Z4cYfjbbE-rABcfC-xab8miocKLomivYMUFIbOh9BVo/edit#gid=0>

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

- Introduction of ACDC, CSER and CSER Proofs
- Discussion and prioritization of the criteria to compare credential formats
- Discussion criteria by criteria and added information to the sheet
- Agreed to share sheet and continue work on filling in the information

## ***Domains of Identity - Presentation of Kaliya's Book***

**Session Convener:** Kaliya Young

**Notes-taker(s):** Kaliya

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

Kaliya Published a book in 2020 - The Domains of Identity a framework for understanding identity systems in contemporary society.

You can find slides of her presentation at IIW here

[https://docs.google.com/presentation/d/1azVOw2O\\_F4fE50cTs29FGg5w1V1jNUqk/edit#slide=id.p1](https://docs.google.com/presentation/d/1azVOw2O_F4fE50cTs29FGg5w1V1jNUqk/edit#slide=id.p1)

You can find a 4 page summary of the domains here:

<https://identitywoman.net/wp-content/uploads/Domains-of-Identity-Highlights-1.pdf>

You can buy her book here:

<https://www.anthempress.com/the-domains-of-identity-pb>

## Verifiable Web Forms

Session Convener: Shigeya Suzuki

Notes-taker(s):

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

Initial Proposal: <https://shigeya.github.io/verifiable-web-forms/>

**Abstract:** *This document proposes Verifiable Web Forms -- a new way to provide Verifiable Credentials to Web Browser via Clipboard. By using Verifiable Web Forms, users can provide third-party verified data with standard user interfaces without typing. The data is also verifiable on the server-side too.*

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

The above document is just an initial memorandum created by Shigeya. No implementations yet. Plan to implement.

Discussion points:

- Where to incubate this? W3C CCG?
- There are similarities with auto-fill / auto-complete functions, or password managers from the user interface point of view.
- How far it can be implemented without any help from browsers, as polyfills.
  - To see that, implementing the concept is the fastest way.
- We can use similar techniques to verify any form of “input” data.
- We could share the potential of the technique.

Next steps:

- Shigeya will implement it himself or ask somebody to do it. Communicate with other attendees on findings.

## ***Best Way to Work with and Engage Orgs - My Data, MEF, Me2B, Mee...***

**Session Convener: Michael Becker**

**Notes-taker(s): Michael Becker**

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

Example orgs and their upcoming programs:

MyData.org

MyData 2022 <https://2022.mydata.org/>

My Data provided 20% Discount Code to IIW Participants: **MyData2022<3IIW**

Me2B

Mee.foundation

Mobile Ecosystem Forum

MEF CONNECTS Personal Data & Identity

<https://mobileecosystemforum.com/events/mef-connects-personal-data-identity/>

The talk primarily revolved around our need to have “big tent” multi-party discussions that can focus on the not just the tech, the moving of the bits and bytes around, but also:

- The problems being solved
- Value propositions
- The need to understand the flows of money

Suggestions for why business models and commercial models are not being discussed:

1. People have no clue about the answer
2. Those that have a clue, proven answers, don't want to share. They won't share until they've pulled out all the value from their secret sauce.

Interesting observations, we will often ball back to what we know and are comparable with...tech people will ask business questions and fall back to the tech, business people will ask technical questions and then quickly fall back to business ones.

## ***JWT - VC Interop Profile***

**Session Convener:** Daniel M and Kristina Y

**Notes-taker(s):**

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

Daniel presented a profile for VC interop.

The profile was developed in collaboration with Workday Microsoft Mattr Ping Identity and IBM.

The presentation follows on from the interoperability demo session.

In that session the Microsoft Authenticator wallet shared credentials issued from a Microsoft managed identity to a Ping Verifier. The Workday CLI wallet demonstrated the sharing of the credentials issued by a Workday controlled issuer to a Ping verifier and a Microsoft verifier.

The profile is an opinionated description of existing open standards.

It does not create any new IP.

Elements

Identifiers of the entities - DID:ION, .well-known

Agent-to-Agent Protocol - Self-Issued OpenID Connect Provider v2

Credential format - VCs encoded as JSON and signed as JWT

VC Transportation - OpenID Connect for Verifiable Presentations

Query Language - Presentation Exchange v1

Revocation - Status List 2021

Issuer/Verifier Trust - Well-Known DIDs

## ***Interoperability Part 2***

**Session Convener:** Riley Hughes & Telegram Sam

**Notes-taker(s):** Mike Ebert

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

Related questions (mostly) posed by Riley Hughes:

Without interoperability, does SSI have marginal value when compared to standard database/API/other existing methods?

Why don't we have very good interoperability?

Why aren't there really any successful implementations at scale?

Some potential answers shared by a big circle of people (such as Sam Curren, Timothy Ruff, Mike Ebert)

Yes, there are marginal values to SSI even without full interoperability. Simplified implementations, value of privacy preservation and verified data within limited ecosystems.

The SSI market is very similar to the early Internet-walled gardens, poor interoperability, lots of competing standards, experimentation, etc.

We don't have a lot of implementations at scale, but they are likely coming. For example, the RFP from the EU for age verification in 50+ nations.

Everyone concluded it was very good for us to examine our assumptions and understanding to make sure we aren't misleading ourselves and are focused on the most important steps to achieving success.



**Mike Jones** @selfissued · Apr 27

This is the best [#IIW](#) in many years! The level of people's engagement and the degree of collaboration achieved among experts who otherwise would have never even known to talk with one another is outstanding. IIW is irreplaceable! 🐶💻



**Internet ID Workshop** @idworkshop · Apr 27

Many Thanks to @selfissued for continuing the tradition started by Kim Cameron and the very first #IIW of Sponsoring the Conference Dinner! We appreciate you ~

MEET OUR SPONSOR

[#IIW](#)



Microsoft



**IIWXXXIV**  
APRIL 26-28, 2022

2

5

34



## Notes Day 3 / Thursday April 28 / Sessions 11 - 15

### SESSION #11

#### *CESR Proof Signatures*

**Session Convener:** Phil Fearheller

**Notes-taker(s):** Phil Fearheller

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

LINK to SLIDES: [CESR Proof Signatures: Partial Digital Signatures with KERI and ACDC](#)

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

#### *How to Govern All Your Personal Data in One Place?*

**Session Convener:** Johannes Ernst

**Notes-taker(s):** (Johannes Ernst)

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

Did an abbreviated demo compared to previous sessions, as nobody in the room had seen the demo yet.

Discussed some of the dangers if too much personal data is in the hands of the wrong people. Even initially well-meaning orgs can go “evil”.

Discussed multi-chamber governance ideas: assembly of businesses, assembly of consumers, assembly of experts. It was suggested that the regulators should be included from the beginning (but of which country?)

Discussion on DAOs. Mentioned work with the Ostrom workshop.

## ***What to Expect with DIDcomm V2 (Sam Curren) and Auto-Generating Language Wrappers for SSI Rust Libraries (Steve McCown)***

**Session Convener:** Sam Curren & Steve McCown

**Notes-taker(s):**

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

What's new in DIDComm V2 - <https://github.com/decentralized-identity/didcomm.org/blob/main/site/content/book/v2/whatsnew.md>

DIDComm Book: <https://didcomm.org/book/v2/>

-----  
Auto-Generating Language-Specific Wrappers for Rust Libraries

[https://www.dropbox.com/s/tykk9yybojhs1l/McCown Uniffi DIDComm RS Presentation II W%20 4 2022.pdf?dl=0](https://www.dropbox.com/s/tykk9yybojhs1l/McCown%20Uniffi%20DIDComm%20RS%20Presentation%20II%204%202022.pdf?dl=0)

## ***Identity Conspiracy Theories***

**Session Convener:** Kaliya Young

**Notes-taker(s):** Charles E. Lehner, Chris

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

Reason for attending

- Concerning articles
- Anti age verification
- EFF/ACLU shared concerns
- Sounds like fun
- No one believes Google
- Why is WEF seen as evil?
- My family is concerned; open to talking
- Explores confusion
- When I tell people - it's bad
  - GlobalID
- \_\_\_ is evil.
- Biometrics

Books about conspiracy theories in identity

- Thinking that Adhar and Social credit score are “what’s next”

People posted conspiracy theory videos about people in this community - were removed



Someone from ID2020 getting death threats

Impacts to personal safety of people in this community

The kernel/seeds of truth in the theories

#### Examples of Conspiracy Theories

- Any new tech for buying and selling -> Book of revelation number of the beast
- Encryption backdoored. Seed of truth: clipper chip - some encryption does have backdoors.
- Age verification
  - Honey pot for attackers
  - Access data of minors
  - Have to buy into the system otherwise be treated as a child online
- Hard to imagine corporations doing the right thing
- Enhanced tracking
- Tracking is happening
- Fake sites abuse trust
- Any ID system -> confiscate guns and money; concentration camp. Slippery slope argument.
  - Seed of truth: WW2; more Jews were rounded up in Holland because they had better records
- Monitor and limit purchases
- Lack of trust with authority / governments
- Bill Gates chip. Seed of truth: he loves Adhar. (Adhar: centralized phone-home database of all Indians)
- Government-funded tech from MIT, military money, shaping credentialing of education. AI -> train robots to replace people's jobs.
- Decentralized identity just a skill to (de)legitimize crypto/NFTs
- Digital ID -> Central bank digital currencies -> Control
- One World Order
- Naive scientists, not asking if "should"
- Startup with good intentions
- Funding from DHS
- Solution looking for problem

Fact: some aspects of the technology has inherent dangers

Combination of digitization and standardization -> surveillance.

People feel anonymous even though tracking effectively creates identity without a name.

Logic against conspiracy theories in general: organizing is really hard.

Congress - can't get anything done. Really hard to organize people to do anything.

Hard to keep secrets.

Research: how people's minds change.

Flood of with conflicting information

Present with facts: doesn't change minds.

Ask to explain. Simple questions, and don't oppose.

Treat people with compassion and respect. Your mind may change, and so may theirs.

"What are you concerned about?" What is your fear? I'm concerned about that too. We work on this and want to hear what you think.

"I'm so glad to hear people are working not hat stuff"

"How does that work exactly?"

Book: "Never split the difference" - hostage negotiation  
who/what/where/when/why  
Convince: only use "when" and "how". - key questions.  
Other questions... defensive.

Cognitive bias: What we see is what we think is true.  
Allay fears  
Own experience -> what we think tru

Debate on whether should respond at all, vs how to respond.  
When you do respond, don't make it worse.

Astroturfing: getting parties to support; backfires  
Streisand effect: trying to ban it spreads it

Feelings are true: experience of system causing harm

Meet the public where they are at.

Humility. Real problems are not "out of scope"

Response must be credible. "We wouldn't do that, because it would cost us money".

Build in genuine opportunities for recourse.  
Can't just say no choice for life.

Harms are more than just money lost. Mental, physical, multi-dimensional harms.

Learning about the past to understand how we got to now.  
We have digital identities already even we don't log into anything, because we interact with institutions that host our data in database records.  
No databases with names -> institutions melt down to nothingness.

Book: "Records, computers and the rights of citizens". Has clear language about computer records.  
Language after that got obfuscated and corporate-speakified.

Humanize our community. Share our stories.

Open and model radical transparency.  
Listen to CCG call recordings.

Tone down hyperbolic revolutionary language. We're just building tools. Demonizing traditional identity doesn't create credibility.

The feeling of truthiness. Confirmation bias. Useful to make people feel seen and heard.  
Invite people to be part of the solution.

Disinformation uses anger to get engagement. More interesting to be outraged. Modifying people's behavior to be afraid and angry. Why?

Mainstream gets details right. Hold people accountable.

Save-the-world "one solution" is not the way. What is the unique value you are adding?

What incentives drive conspiracies?

Short-term, long-term reward.

Identify and shift incentives to not promote ignorance, fear, anger.

Who are our allies and leaders?

Getting excited about adoption... Covid credentials -> tells people "If you sign up for our tech, you can do the things you could already do before, otherwise you can't"

Same with age verification.

Compare to alternatives... giant public database of names of vaccinated.

Outrage and scandal structurally rewarded by platforms.

Transparency with business models.

Possible to make money doing things the wrong way.

We're planning to do things the good way; if we lose your trust we don't make money.

Need to rewrite terms of service to be clear.

Fund strategic communications. The work to communicate clearly. How to fund and amplify...  
Documentary?

Otherification. Outrage at the problem "over there".

The Social Dilemma. Can't combat that with a spec and GitHub repo.

Meaningful public participation and engagement.

- Articles Concerning
- Anti Age Verification
- EFF / ACLU share <sup>concern</sup>
- Sounds like for
- @google no one blames

Why WEF seen as Evil  
 my family is concerned & uncomfortable  
 - explore confusion out  
 - when I tell ppl. - its BAD  
 global ID  
 - is evil  
 Biometrics

- Not sharing our stories <sup>(humanizing)</sup>
- Model Radical Transparency
- Tone down "revolutionizing language"
- building tools
- ↳ Also <sup>vitalizing</sup> about the OG systems

Feeling of truth iness

invite part solution

The point of <sup>travel in SM.</sup> disinformation <sup>(human circuitry)</sup> engagement  
makes angry  
 why make angry & afraid "OTHER"

Mainstream get Details Right  
 HOLD ppl Accountable

Own Experience  $\Rightarrow$  what think true  
 Debate should respond  
 vs how to respond  
 Response  $\Rightarrow$  Needs not to make worse  
 $\Rightarrow$  Needs credible response  
 Feelings true System experiencing  
IS Harming them  
 Meet Public where at.  
 We also should be humble  
 Buied In genuine opportunity reverse  
 Harm is not only \$\$\$  
 Understanding History

- clipperchip <sup>Seeds of trust</sup>  
 $\rightarrow$  tracking is happening  
 - Fake sites out there about trust  
 "germany"  
 Lack of Trust  
 particularly  
 Immigrant & religious  
 minorities  
 Canadians did this to +  
 $\rightarrow$  He loves Aadhaar  
 Digitization has  
 standardization risk  
 and impact  
 People don't

Conspiracy theories (?)  
 Edu micro credentialing  $\rightarrow$  AI  
 Decentralized ID is a ruse  
 & support legitimize NFTS  
 Crypto  
 Digital ID - CBDC  $\rightarrow$  control  
 All established to create New World  
 Order  
 We are scientist never asked if should  
 n/w so cool  
 Blockchains 4 ID 4 AI

Seeds of Truth 2

Startup w/ good intentions  
bought

some of  
our work is funded by DT

Kalya - a YGL w/ WEF

soulution looking for problem

You can't get things done

negative Example  
Congress  
can't get things  
done

Research: How ppl's minds change?

• expose to facts multiple sources

Flood of conflicting info & question who believe

We need evangelist

Ask ppl to explain it to you

How do you know it's true

How does it work? what are your fears

mutual  
openness

Book: Never Split the Difference  
on Hostage Negotiation

When  
How

Key Que

People have legit concerns  
we should acknowledge



Meaningful Public Engagement  
 Save world "one solution" <sup>about</sup>  
 not way tech

What existing thing add value

What are incentives drive conspiracy story telling  
 ↳ shift

Who are our allies  
 who are our leaders

Don't focus on covid credential adoption  
 Don't be gate keepers

How compare different choices

We need to be transparent on  
 our business models

TOs so understand  
 Find good communication  
 "documentary" → like Social Dilemma

<sup>Conspiracy theory (1)</sup>  
 All encryption has back doors

Age verification ⇒ about tracking  
 behavior online

- honey pot hackers  
 process all data
- Access Data of minors in way
- Everyone Buy into tracking  
~~have~~ unless treat 12 y old

~~Fact~~

\*Any ID System - confiscate guns money  
 → concentration camps

~~Unproven~~ ID System - monitor

Bill Gates putting chip in every

Digitization makes  
 New Tech Buying selling Book Re

Belief they are "anonymous"



**Notes: Chris** 28th Thurs Session 1 F Conspiracy theories - Kaliya Young 9:30-10:30

Concerning articles  
Anti-age verification  
EFF/ACLU Objections  
suspicion of the WEF  
Concerns in personal circles  
explore confusion  
talk about BAD Global ID  
Biometrics concerns

Theories:  
ID2020  
Named people from the Identity community - Pam, Sam Jones  
Dakota Grüner - death threats  
Potential danger to personal safety

List the theory - drill down to the seed of truth that keeps it alive

1. New tech - buying and selling - book of revelations, marking tracking  
Anchoring barcodes with 6...6...6... GS1 - OOPS

2. All encryption has backdoors - for government?  
ClipperChips  
Some encryption does have backdoors/holes

3. Age verification  
Just a way to track behaviour  
Honeypot for hackers  
Phishing  
Locking adults out of society if you don't buy into the system  
New way to access protected data of Minors

Corporations have normalised tracking, lack of trust in them/the system  
There are actual bad actors out there looking to exploit and manipulate  
No mutual authentication

4. Confiscation of guns, money, concentration camps are next  
Slippery slope argument

5. Distrust of institution  
We lack compelling narratives to talk about the real guarantees of the tech

6. Gov with total control, forbid behaviour, or create disadvantage  
Value judgements of behaviour  
Canadians  
China social credit system

7. Digitization and standardization both together potentiate harm  
actual inherent dangers

8. Mistaken belief that people are anonymous on the internet -status quo  
Fear of this changing for the worse  
Media panic about blockchain

9. Mom from Boston  
concern in Education space  
Resist standardized testing  
Proving educational attributes - work history  
learning economy - refusing  
Alison

10. Decentralized ID a ruse to support or destabilize NFTs crypto

11. route to new world order

12. assumption the community has lack of governance, naïve

Startup gets bought out and repurposed

Funding from DHS  
Kaliya is a YGL

solution looking for a problem? Shoehorning it in where it is unsuitable

One bit of logic against consp theories  
US congress for example  
Don't assume malice when it can simply be ignorance/negligence

Studies on how people change their minds  
Exposure to multiple sources can help change their mind  
Overwhelmed by conflicting info  
Intentionally overload with info to muddy the water  
Ask people to explain it and watch their arguments unravel  
Ask how not why?  
Making people feel seen/heard/ show thoughtful work  
Never split the difference - book - hostage negotiator

People have legitimate concerns - engage with them

Our emotional brains are the strongest  
Confirmation bias

Debate on how/if to respond  
When you do respond - do not make the situation worse  
Needs a credible response  
Many of these theories contain a grain of truth  
TRUTHINESS  
Meet public where they are at

Build-in genuine mechanisms of recourse

New types of agency  
Multi-dimensional harms  
Learning about the past - how we got to now

We are already in systems without active choice  
We have interacted with institutions  
1973 records, computers and the rights of citizens  
Best information practices

Solutions?  
Telling our own stories  
Humanizing our community  
As a community  
Model radical transparency  
Temperate language  
Do not demonize existing structures

Engagement incentivization - outrage travels furthest and is rewarded by the platforms

Don't assume that general public or specific subsets hold such extreme views

Pitfalls of rushed-out global Covid tech  
What existing things add value

Who is incentivizing these theories and why?

Who are our allies and who are our leaders?  
Covid as example use-case - be careful

Don't want to be seen as gatekeeping liberties (like covid)

Be honest about for-profit business models

Fund strategic comms

Revisit presentation/format of ToS for greater transparency/

### **Topics That People Are Concerned About**

- Anti-age verification
- Sounds like fun
- No one believes Google is focusing on privacy.
- Why MEF Seen as Evil
- Video conspiracy theories ID2020 (Dakota Bruner was getting death threats)
- My family is concerned and wants to explain it to them.

#What are the conspiracy theories?

|CONSPIRACY|SEED OF TRUTH|

|Book of revelation, we are being numbered by the beast | Gs1 anchored barcodes with 666 |

|All encryption has a back door | Some encryption does have a backdoor, clipper chip|

|Age verification, tracking behavior online, a honeypot for hackers, phishing exercise, access the data of minors, an attempt that everyone has to buy-in for tracking, otherwise eternally a child|1. tracking has become normal, is happening 2. there are fake sites that are abusing trust, 3. don't have mutual authentication|

|Any ID system censorship, concentration camp, shut off money |slippery slope argument, "Germany," ww2 holland had recorded over everyone|

|Bill Gates is putting a chip|Gates fan of Aadhaar, centralized phone home ID of all Indians|

|New tech buying and selling|Mom, Boston, concerned about standardized testing...micro-credentials for explaining skills, train robots to do everyone's job, Alison ???|

|Dehumanizing people| |

|Consiricity to make money, controlled by central bank digital currencies||

|All about creating the one world order||

|Digital ID-CBDC-Control| |

|Science is naive about what they're making||

|you can't get things done|U.S. Congress|

### **Seeds of Truth**

- There is vulnerability
- Fake sites are out there stealing data
- Germany history WW2
- Lack of trust
- Cambridge Analytica
- Tracking is happening
- Startup with good intentions gets bought by evil
- Kaliya is a YGL w/MEF
- Solution looking for a problem
- Some of the work is funded by DHS
- Congress (you can't get anything done)
- People are overwhelmed with conflicting information.
- Reality
- Digitalization has real ramifications, risks, threats, and dangers.
- Solutions
- Evangelism
- Education
- Expose people to facts from multiple sources
- Ask conspiracy theories to explain the conspiracy, ask "How" not "Why"
- Try to understand people's fear, what are they worried about
- Acknowledge concerns

- Determine should we respond vs. how to respond; if you do respond, have a credible response, e.g. “I do this because of XYZ business model.”
- Meet the public where they’re at
- Be more humble; there is a lot that we may not want
- Building legitimate opportunities for recourse, addressing the issue of multi-dimensional harms (harms is not just about money)
- Share the history/Understand the history (we have a digital ID already, your data is in the database)
- Tell more success stories.
- Tone down the hyperbolic language; just say “we’re building tools.”
- Get the basics right.
- HOLD groups accountable, e.g. Equifax contract.
- Understand the incentives that drive the conspiracy, what are they getting out of it
- Identify allies and leaders.
- Need to be transparent about business models, how are we going to make money with your data
- Write terms of service and policies that people understand.
- Fund strategic communications so that we can communicate clearly about this stuff? How to fund and amplify good work in this space.
- Crowdfund an “anti-social dilemma” movie, a movie that shows the good we are doing
- Find meaningful public engagement behind these schemes

## Blockers

- Standards are not a selling point for the average person.
- Inability to convey and explain any sort of real guarantee
- Referenced Resources/Examples
- Learning Education Foundation (???), Kaliya reference
- Book: [Never Split the Difference](#) by Criss Voss - the only two words you should use are “When” and “How” the other question phrases put people on defense.
- Frequency effect, what we see with think is true.
- [Streisand effect](#) - “a phenomenon that occurs when an attempt to hide, remove or censor information has the unintended consequence of increasing awareness of that information, often via the Internet.”
- Book: Records, Computers, And the Rights of Citizens (PDF); Records, Computers, And the Rights of Citizens R2 (PDF)
- Movie: [Social Dilemma](#)

## ***MARKET ADOPTION STRATEGY for Global Standardization (How to get Budget!!)***

**Session Convener:** Tom Sato

**Notes-taker(s):** Mike Ebert

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

Understand the ecosystem and network

Draw a network diagram

Examine the components

Build a tool set for these groups:

For business team members - Presentation, white paper, use case, video

For developers - Specs, documentation, tutorial

Help interested parties understand how your solution provides maximum benefits for minimum work

Use “carrots and sticks” to “persuade your donkeys to move.”

If your “donkey” won’t move, find a “thoroughbred” (an organization that is willing to take action)

When you communicate, use simple language

With enough work, you can get to a tipping point–market consensus

## ***Teaching SSI with Caucus Credentialing***

**Session Convener:** Kent Bull

**Notes-taker(s):** Kent Bull

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

See the evolving syllabus at / This is the first draft we created during the session.

<https://kentbull.com/2022/04/28/caucus-ssi>

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

### **Goal**

Create SSI solution creation capability in engineers and architects through 3 day workshop.

Audience

Senior and principal engineers and architects

## Syllabus

- Verifiable Credential Ceremonies
  - Present
  - Issue
  - Verify
  - Revoke
- Issuance Technology
  - Hyperledger Indy
- Agents
  - Agent Setup
  - Agent Communication
  - Agent Credential Exchange
- Communication with DIDComm
- Dynamic Witness Selection
  - KERI
  - Trust Selection of Issuers
- Login (auth) with DIDs and VCs
  - DIDAuth
- Credential Types
- Common SDKs
- Key Rotation
- Make your own DID method
- Evaluate your DID method against the DID rubric
- Predicate Proof
- Storing linked documents in IPFS or external data stores
- Perform a graduated disclosure ceremony

## SESSION #12

### *How SSI Will be Adopted (my P.O.V.)*

**Session Convener:** Timothy Ruff

**Notes-taker(s):** Alan Davies

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

Video of presentation on YouTube:

[https://youtu.be/kLSLA8\\_VDFw](https://youtu.be/kLSLA8_VDFw)



## User-Centric Request Model

Session Convener: Adrian Gropper

Notes-taker(s): Adrian Gropper

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

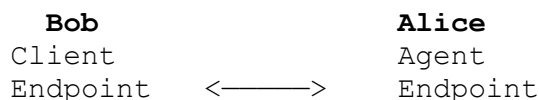
Alice, Bob, Wallet, Agent

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

### User-Centric Request Model

Alice to Bob is the default use-case

- Alice and Bob **each** have a crypto wallet or authenticator
- Alice delegates request **evaluation** to an agent
- Bob delegates request **presentation** to a client
- Request evaluation results in a capability that Bob's client presents to the storage resource.
- Microsoft Authenticator is now holding VCs (is an anti pattern because it combines wallet and agent)
- What's requested?
  - Vaccination status (as registered)
  - Red / Green Infection risk (contextual)
- Protocol Foundation for IETF / W3C / EIP / ISO
- Clarify: Agent
  - is potentially automated
  - Alice needs expert representation
  - Bob's client (agent) is mandated by their employer
- The requested resource is referenced as a URL (addressable and accessible)



- Bootstrapping (out of scope)
  - Who's who
  - Directory (AS first vs. RS first)
- Also consider:
  - 3 Dimensions for interoperability
    - Vocabulary
    - State Transitions
    - Policy Calculus
- Graduated Disclosure (allow)
- Resource Abstraction Layer (include)
- Client knows **How**, Resource Server knows **What**
- Notary or Bond + Auditor = Consequences



## ***NEVER say WebAuthN is hardware-protected - unless you check attestations***

Session Convener: Kosuke Koiwai

Notes-taker(s): Kosuke Koiwai

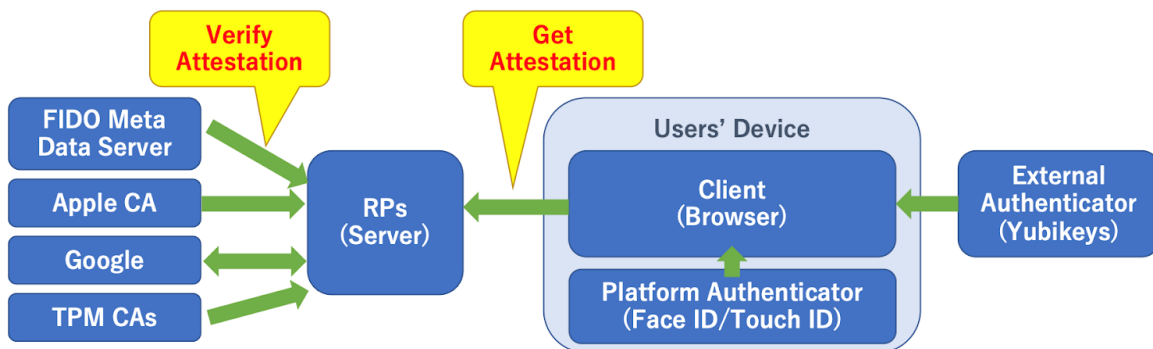
Tags / links to resources / technology discussed, related to this session:

WebAuthN, attestation, FIDO2, CTAP2, wallet, verified credentials, TPM, passkeys,

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

## Attestations

- To make sure a user is using a authenticator that you expect
- RPs can ask for it at the registration, then verify it



The discussion started with a little introduction to the attestation of WebAuthN spec, which is barely implemented by Relying Parties due to its complex nature.

Then many experts explained all the details of how attestation works in WebAuthN.

And in near future, Platform Vendors will introduce multi-device credentials, which is private key sharing among your devices. Users can choose whether s/he wants to use multi-device key or single-device key, but RP may NOT.

We also discussed the Device Public Key (DPK) extension, which attaches extra data signed by a device-bound key. DPK will be an OPTIONAL feature of WebAuthN, so RPs can't always get it, and it is also up to platform vendors to give RPs an option to choose multi-device credentials for single device one.

An action was called to give feedback to platform vendors so that RPs can have an option to ask for a device-bound key.

## ***KEPLER Design Overview: Shallow or Deep Dive***

**Session Convener:** Charles Cunningham

**Notes-taker(s):**

**Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:** No Notes Submitted

## ***Kim Cameron & The Seven Laws of Identity***

**Session Convener:** Doc Searls **Notes-taker(s):**

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

[Kim Cameron's Identity Weblog](#) Digital Identity, Privacy, and the Internet's Missing Identity Layer <https://www.identityblog.com/?p=352>

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

From 2005-July-23 Slashdot story: "Something strange is a brewin' at Microsoft these days. Check out this video interview with Kim Cameron, Microsoft's Architect of Identity, about Kim's Laws of Identity." From the post: "We have undertaken a project to develop a formal understanding of the dynamics causing digital identity systems to succeed or fail in various contexts, expressed as the Laws of Identity. Taken together, these laws define a unifying identity metasytem that can offer the Internet the identity layer it so obviously requires. They also provide a way for people new to the identity discussion to understand its central issues. This lets them actively join in, rather than everyone having to restart the whole discussion from scratch."

<http://yro.slashdot.org/article.pl?sid=05/07/23/2118251>

<http://www.identityblog.com/stories/2004/12/09/thelaws.html>

The Seven Laws of Identity

(<http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.html>)

1. User Control and Consent: Digital identity systems must only reveal information identifying a user with the user's consent.
2. Limited Disclosure for Limited Use: The solution which discloses the least identifying information and best limits its use is the most stable, long-term solution.
3. The Law of Fewest Parties: Digital identity systems must limit disclosure of identifying information to parties having a necessary and justifiable place in a given identity relationship.
4. Directed Identity: A universal identity metasytem must support both "omnidirectional" identifiers for use by public entities and "unidirectional" identifiers for private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.
5. Pluralism of Operators and Technologies: A universal identity metasytem must channel and enable the interworking of multiple identity technologies run by multiple identity providers.

6. Human Integration: A unifying identity metasystem must define the human user as a component integrated through protected and unambiguous human-machine communications.

7. Consistent Experience Across Contexts: A unifying identity metasystem must provide a simple consistent experience while enabling separation of contexts through multiple operators and technologies.

## ***Can we solve the Bring Your Own Wallet Problem?***

**Session Convener:** Snow

**Notes-taker(s):** [Peter Langenkamp](#)

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

The problem:

You're a user, you click the 'issue' button, what will happen?

Issue

- Multi w selector
- DIDCOM
- OpenID connect
- CHAPI polyfill
  - o BrowserAPI

Nascar problem (The NASCAR problem is when there is a jumble of branding icons in a user interface, like 3rd party sign-in/login options or sharing buttons on websites, that is visually busy and often noisy, distracting, and overwhelming.)

Discovery handshake

A wallet doesn't have to be an app, it can be in the browser too

Problem getting wallets to adopt the same schema

Challenge for iOS, it simply picks the last installed app that's compatible with the link (Android gives you the choice)

- No options in settings to switch it
- Can there be some kind of protocol that all wallet providers implement? You communicate to the issue button which profile (e.g. DIDCOM om OpenID) you support
- Is this something that DIF should have a working group for?
- A multi w selector could be discriminating
- The DIF interop group might be a good place to start?
- That's where we're coming from already
- EU has mandated that all countries should have an identity wallet
- Hopes that those wallet providers will want to support more beyond what is mandated so we can build this out

Q: Suppose I was a new company, would I have to work with Matter?

A: No you just have to support this (OpenID) protocol

What GAPI exposes is limited (only GET and CREATE and create?)

Generally the challenge is that we don't want the issuer and verifier to have to name one or more specific wallets, just to present the 'issue' button

Problem, interop generally isn't high on peoples agenda. (it doesn't create business, it removes business)

iOS is a problem issue with browsers, you will automatically be redirected to safari so you can't finish a session in another browser

Can we solve this problem?

- You have to solve it with another intermediary
  - o Who will host that?

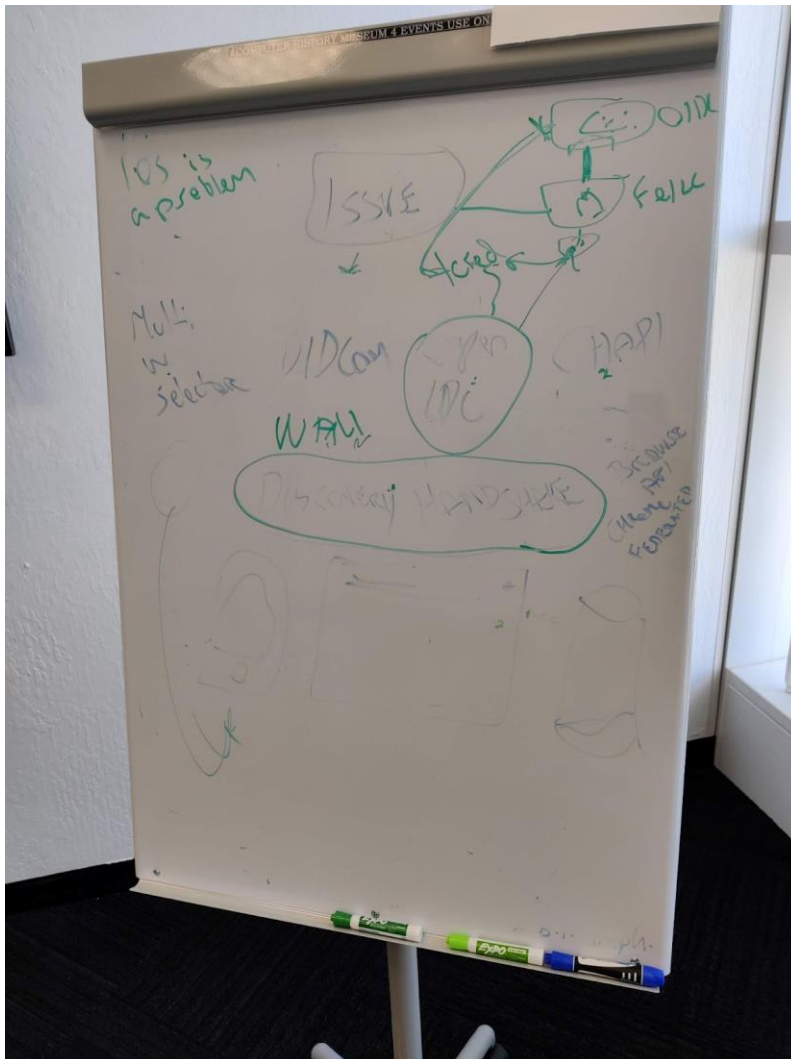
What would the five profiles be? (this is about format compatibility)

- What type of VC are you going to offer?
- What DID?
- What type of encryption?

There's also going to be a UX problem

To stay apprised or involved: [Follow the interop working list](#), if not [join DIF](#) and contact [Snow](#) on Slack.

Picture of whiteboard notes



## ***IdentiTEA for you & Me - The Trust Triangle, Triple Entry Accounting + the New New World***

**Session Convener:** Nicholas Racz, <https://www.cheqd.io/>

**Notes-taker(s):** Michael J. Becker

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

**Facilitator:** Nicholas Racz, <https://www.cheqd.io/>

**Note taker:** Michael Becker, Identity Praxis, Inc.

### **Three Eras of Accounting**

How society, account, and social evolution gave rise to the inevitability of triple-entry accounting/Trust Triangle.

#### **Single Entry (early Egypt) ... tracks matter/mass**

- Thoth - Thoth, (Greek), Egyptian Djhuty, in Egyptian religion, a god of the moon, of reckoning, of learning, and of writing. . He was held to be the inventor of writing, the creator of languages, the scribe, interpreter, and adviser of the gods, and the representative of the sun god,
- Establishment of the state
- Establishment of citizenship (differentiate citizens from the enslaved)
- Monolithic societies
- Made possible by writing and mathematics
- Modern thinking is that numbers came first, and writing followed to give numbers context.
- get quantity and “qualia.”
- led to the creation of money (starts off as collectibles)
- Religious, Economic, Law all in one One (DAO, Sharia); Sharia law dictates it all (vestigial proof that society came as one amalgam)

The sophistication of trade has driven things.

Initially, accounting for grain and tax on how much a field can endure.

“The temple of [Juno Moneta](#) is the etymological root of money” - religious template, the center of trade, and center of coinage. Christ got killed because he disturbed the money train during Passover.

#### **Double Entry Accounting (formally introduced by [Luca Pacioli](#) in 1492) - tracks movements, velocity.**

- Inflows (+1) and outflows (-1) from the account (accounted for number and quality of item)
- First sophisticated form for accounting events, not just taxing land, but now taxing trade of goods.
- Started forming joint-stock and organizations Gold is heavy...deposits in the bank..get IoU for the gold, trade the certificates. The first modern central bank with Amsterdam



Dutch East Indies Trading company had shared, so successful; not possible without mutually assured records.

Joint stock organizations Central banking Colonizations

Unit of identity expands: you are now not just a citizen, but a "Shareholder" - you can now claim a piece of the profit. There is ideological good...best way to support your metabolism is to support a company that brings in revenues

- Decreased fraud
- Increased trust

Religion and states started to divorce themselves by introducing double entry of account. Similar to human development...by necessity specific element of society start to specialize through necessity For society to scale need utility specific assets to specialize and separate from each other.

John Nash, Buckminster Fuller, Henry Ford, Friedrich August von Hayek - all foretold the coming age that money will be abstracted from the state, just as the church was abstracted from the states.

visa is like an intermediary for the triple entry process

Has an implicit notion of the third party - Luca suggested that you were ultimately accountable to god, the moral rule. An implicit part of the double-entry account.

**Triple Entry Accounting (TEA) - tracking momentum (momentum is a change of change).**

Relates to the trust triangle.

The wisdom of the crowd

"Why assume malice when incompetence will do"

You have something. You record the exchange (mutual accountability). You record the momentum (change in the exchange)

**Example 1:** Momentum based accounting ([YUJI IJIRI](#)) |y1|y2|y3| |100|200|300|  
|0|100%|50|%

More complex. If the company's momentum decreases in time, then the auditor damps the company's evaluation.

**Example 2:** Trust triangle emerging - use a trustworthy mediator to coordinate activities. [Ian Grigg](#); [Episode 13 : Ian Grigg on the Evolution of Trust, Triple Entry Accounting and a New Way of Audit](#)

Three Parties: first-party, second-party, coordinative entity. Automation will inherit drifting into the coordination role due to the complexity of the account.

Not possible without \* Computers \* TCP/IP \* Routers \* Cryptography \* Digital ledger technologies (DLT)/KERI

All this will lead to... \* Implicit DAO - no clear governance framework \* Explicitly - has clear governance framework \* Utility Tokens

**Random Discussion**

Does governance framework mean that you'll be moral?

Remove money from nation state you'll create virtualized communities (they will align to utilitarian purposes as opposed to genetic, cultural, geographic, religious—traditional tribal bidding)

Complex civilization society arises because of the ability to seize grains. Cryptography may simplify movements as we know it, or it may change the

Create new means to interact without others - enable us to go to mars, etc., the next big ocean...untold resources out in the galaxy. China: Rare resources, people to get it, and industrial population

Commodification and tradability of energy.

Triple entry accounting is the way out of the bureaucracy problem we find ourselves in today.

Need accumulated utility bills to derive trust

- Triple entry method does not place the actors at the center but the transaction at the center (is anonymous and self-monitoring; an amalgamation of trust)
- Double Entry puts the actors at the center (is bureaucratic and needs oversight)
- Single entry accounting puts the item at the center

### ***Identity Crisis? - Identity in the Age of AI***

**Session Convener:** Wenjing Chu

**Notes-taker(s):** Wenjing Chu, Shannon Wells

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

- Is Digital Identity - as defined by structured trusted data - the Wrong Question?
- What is Identity in social science and humanistic sense?
- Digital Identity is trying to capture a partial representation of that - it's always a partial representation. All models are wrong.
- AI can build a similar partial representation through deep learning for example, unstructured model but a model that can be very accurate/effective - it is therefore also an Identity
- Which kinds of identity is "better"
- Which kinds of identity is more effective in addressing the problems we face (e.g. principles of SSI etc.)
- Case studies
  - Biometric authentication
  - AI bots
  - Social media intermediated by AI
  - Bots on social media
  - Metaverse
  - Who is learning? You or the Machine.
  - A language between human and AI
- If you are interested in continuing this conversation, join me in a new ToIP Task Force for AI and Trust that is coming soon. Ping me on ToIP (Trust over IP Foundation) slack channel. Or Email: chu.wenjing AT gmail D O T com.

Thanks for all of your questions and interests.

## Notes from Shannon Wells:

In one of the first slides, was shown that there are two ways to conceive of an identity. One is to build a descriptive structure, for example, a list of observable features, test results, facts about someone, etc. However these things can all change.

The second is to take everything observable about the person and put it into an AI that will create a “learned structure”.

Keeping a descriptive structure up to date is very hard. People age, they gain and lose weight, they change their hair, maybe they are injured, they change jobs and have children, etc. But we humans continue to recognize someone who has been through these things and an AI may learn even better.

“Rather than digitizing the human world for machines, machines should learn to live in the human world”

In the cases of determining whether someone’s face matches their ID card, or whether someone is over 21, AIs using facial recognition and being trained to comprehend these things outperform people. In both cases there is no need to store anything in a database, so someone’s privacy can be preserved better, rather than storing a bunch of “descriptive” data in a database, even encrypted is less secure and less private than a well-trained robot who performs a single task and then forgets about it afterward. Next there is no “disclosure” to agree to, the person simply walks in the door, or presents an ID card.

These and similar tasks are suited to AIs and can be implemented in ways that not only preserve a level of privacy, and accomplish goals of verifying attributes with high accuracy, but when there are errors they can be addressed immediately instead of being stuck in a database and the person is unable to correct the errors or has tremendous difficulty getting the errors corrected.

In the realm of identity verification, one attendee remarked that smartphone sensors have been shown to be able to produce a profile that can determine whether a phone’s owner is holding the phone based on how it’s oriented, how their hands move, how tall they are, etc.

## SESSION #13

### *Poly: The Game of Community Governance*

Session Convener: Joyce and Doc Searls

Notes-taker(s): [Peter Langenkamp](#)

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

Challenge: Rules for a game for making rules

- Working on the technical aspects, and on the governance aspects
- A way to create a framework, so that any community can create their own governance framework
  - o People don't know how to get started
  - o People need a tool to figure out a way to create their own rules
- There has already been quite a lot of academic thought on this
- This has also been done in for example Minecraft
- Articles:
  - o **"This place does what it was built for": Designing digital institutions for participatory change** <https://dl.acm.org/doi/10.1145/3359134>
  - o **Community Governance for Minecraft** <http://heapcraft.net>
  - o **Modular politics: toward a governance layer for online communities** <https://docs.google.com/document/d/1YA-OJTmpcaUnschbAOF2MAOUrvw19HR55wsGxEo678Y/edit#>
  - o **Emergent Cultural Differences in Online Communities Norms of Fairness** <https://journals.sagepub.com/doi/10.1177/1555412018800650>

**Brainstorm (NOTE: more was discussed, my personal notes were incomplete)**

If we were a community and we were going to set some rules, and were going to do this in a tabletop game format...

"We're doing this locally because we think it's best to make this happen in a physical place" (not dependent on 'apple space', 'google space', ...

You want folks to have fun, and to be able to replay the game, but also to learn something

If people get together just to play the game, they start to become a community already

Trying to start in our little group with 'These are the principles that we think are good ideas'

Creating (new) governance rules is a part of the game eventually

Set up a similar game with professor in Cambridge, show that it actually works in practice

Several years ago, a grant to build a game. Organizing into hierarchy or as flat organization structure.

Like clue. Used the game, afterwards they asked 'how do you feel'? Figuring out what works best (hierarchical vs. flat which allows for self-organizing teams)

- Resulted in papers and talks at conferences

Social media apps could use moderation system that's the result of what a community came up themselves

Communities don't fail on the best path. So most of the community members should be cooperative, but some should be adversarial if you want to create something durable (resistant against non-cooperative subset) using this process

When doing the experiment, many participants tended to ask whether it was a cooperative or competitive exercise. Not allowed to answer this.

The US military so advanced (ahead of adversaries) that they can afford to publish publicly, in fact need to in order to get allies up to the same level.

- Good example in (self-organizing) Ukrainians trained by US going up against the strongly hierarchical Russian military

We need to do stuff for it to stick, simply reading about it isn't enough

Focus here on table-top style game because of the desire to create a *local* community

So what should be in the game?

- Do we want cards?

- ...

Maybe even not give participants a hypothetical problem, but simply the real problem

Does the university have a game design dept? They do, but still need to get in touch

The game is called Poly, because Polycentric is the way governance happens

Having some objective measure (like tokens) that participants can think about, as opposed to just going by how they feel, ... You could design a relatively simple game that starts with things people like, and things people want. Craigslist style selling

Everyone can make a game, but not necessarily a fun game

Christopher Allen runs a game company, has written a book about it

What is the game that will achieve the greater good for this community that we are about to start?

You don't want apathy to take hold and people not to care anymore

## *Tunnel to KERI Island - How can we interoperate with KERI?*

**Session Convener:** Sam Smith + Markus Sabadello

**Notes-taker(s):** Markus Sabadello

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

KERI, OOBIs, DIDs

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

KERI doesn't trust ledgers, resolvers, DID Resolution. But there is a way to bootstrap into the KERI world starting from DIDs and DID Resolution. This uses so-called OOBIs (out-of-band invitations), see: <https://weboftrust.github.io/ietf-oobi/draft-ssmith-oobi.txt>.

An OOBIs is a tuple of a KERI AID and a URL, e.g.:

("http://8.8.5.6:8080/oobi", "EaU6JR2nmwyZ-i0d8JZAoTNZH3ULvYAfSVPzhzS6b5CM")

The OOBIs can also itself be expressed as a URL, e.g.:

<http://8.8.5.6:8080/oobi/EaU6JR2nmwyZ-i0d8JZAoTNZH3ULvYAfSVPzhzS6b5CM>

This can be discovered from a DID using DID Resolution, e.g. try this:

<https://dev.uniresolver.io/#did:web:did-web.godiddy.com:markus7>

<https://dev.uniresolver.io/#did:sov:danube:Xrr91sjfCqLb5tQg4zzqhP>

<https://dev.uniresolver.io/#did:web:did-web.godiddy.com:markus8>

Discussion about did:keri method. The method-specific-id can be an AID, and an "oobi" DID URL parameter could be introduced to supply an OOBIs:

did:keri:EXq5YqaL6L48pf0fu7IUhL0JRaU2\_RxFP0AL43wYn148?oobi=https://...

|----- AID -----|

## ***FIDO / WebAuth for Verifiable Credentials***

**Session Convener:** Torsten Lodderstedt, Paul Bastian

**Notes-taker(s):** Mike Jones, (someone else)

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

Diagram of 1st approach (makeCredential/getAssertion) <https://shorturl.at/efjvQ>

- Group went through the proposal step by step
- Identified a couple of pitfalls
  - Signed response from FIDO authenticator contains more data than just the pure signature of the challenge (e.g. client id of the Wallet with the authenticator)
  - Does not directly fit with existing proof methods for verifiable credentials

We dove deep into what FIDO attestations actually do and surprising things that they do not do and what it would take to use them with a wallet as the FIDO RP.

The surprising thing is that there's no proof of possession of the credential private key in the WebAuthn/FIDO protocols - only of the attestation private key.

John Bradley went into how the HMAC Secret Extension <https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html#sctn-hmac-secret-extension> could be useful in this scenario, barring the limitation that only the platform has access to the HMAC key. He said that a new extension is in the works without that limitation.

## ***VALUE CHAIN How is value spread across***

**Session Convener:** Michael Shea

**Notes-taker(s):** Paul Grehan, Michael Becker

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

Value, Cost and Motivation to adopt a Open Trust Claims (SSI)

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

Explored the true cost and motivation of each actor involved in the SSI chain to adopt.

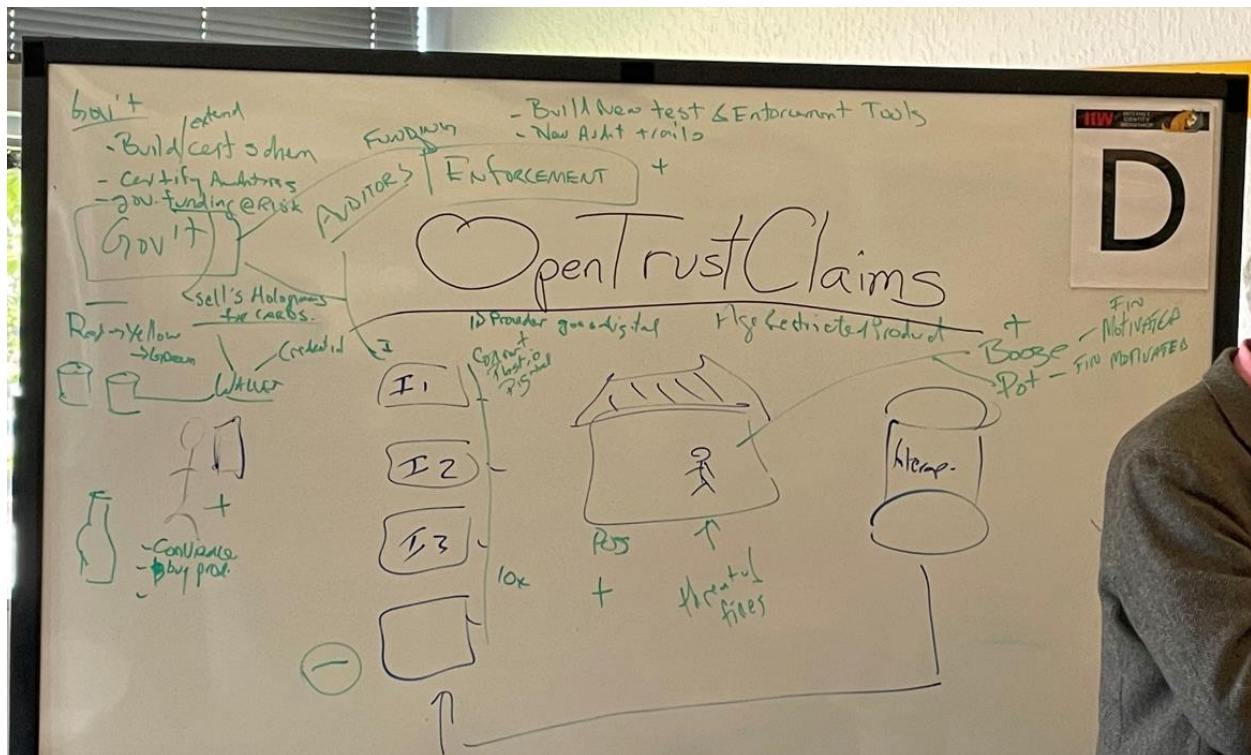
By providing a rollup of value metrics, indicate either a positive incentive to adopt or what barriers exist until a more compelling benefit is realized to adopt and migrate to trusted claims.



Michael walked us through the steps of deconstructed and end-to-end value chain. The key, according to Michael, is to look for the bottleneck. That is to say, to identify the players that are not providing or more importantly getting any value from the process. These will be your points of failure.

You then want to consider exactly how people will engage, especially in the consumer facing environments. Will they have the B2C experiences available to be able to effectively interact with a service. If not, the value chain will fail.

In the end, it all starts with understanding the problem you're solving and for whom, and then to work backward from there.



## How do we make JSON-LD W3C Credentials Suck Less?

Session Convener: Sam Curren

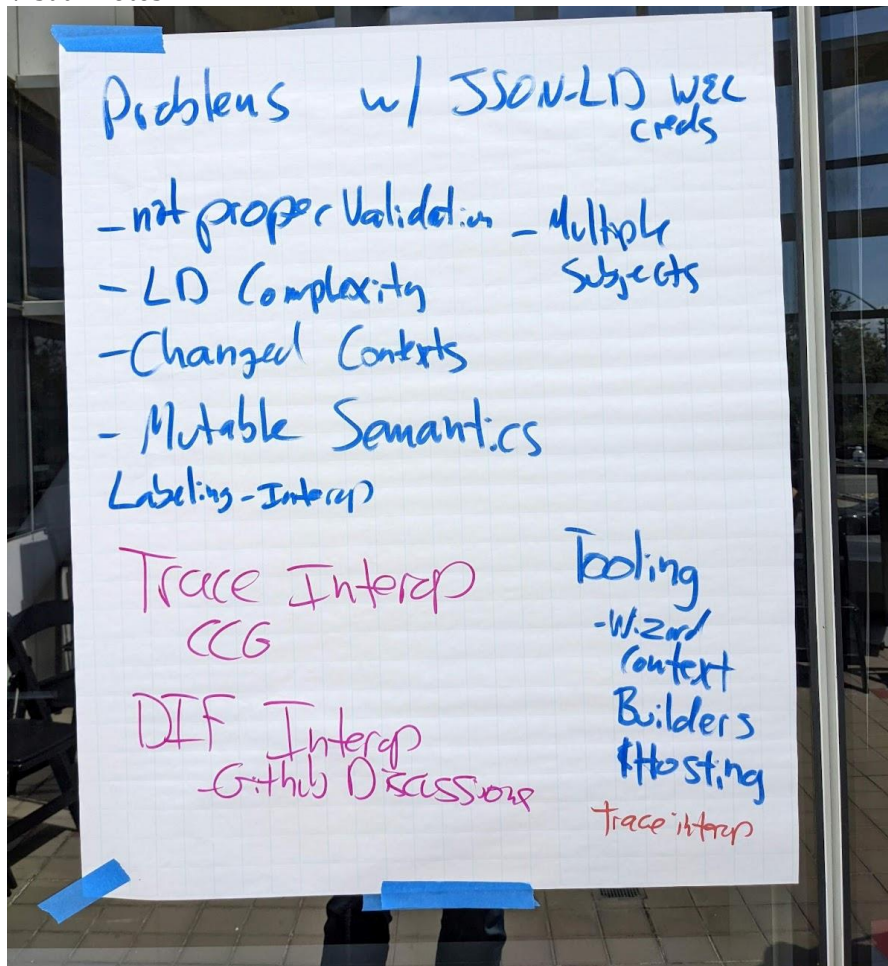
Notes-taker(s): Sam Curren

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

Follow up asynchronous discussion is happening here: <https://github.com/decentralized-identity/interoperability/discussions/63>

Post on Labeling Interoperability: (PDF) [https://indicio.tech/wp-content/uploads/2022/04/Indicio\\_Report\\_TrustVerifiableCredentialsInteroperability\\_040622.pdf](https://indicio.tech/wp-content/uploads/2022/04/Indicio_Report_TrustVerifiableCredentialsInteroperability_040622.pdf)

Visual Notes:



## ***GLOBAL Covid Certificate Network POC Demo***

**Session Convener:** Lucy Yang and John Walker **Notes-taker(s):**

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

Linux Foundation Public Health (LFPH) [launched](#) the Global COVID Certificate Network (GCCN) project in June 2021 to facilitate the safe and free movement of individuals globally during the COVID pandemic. After nine months of dedicated work, LFPH completed the proof-of-concept (POC) of the GCCN Trust Registry Network in partnership with [Fraunhofer Institute for Industrial Engineering \(Fraunhofer IAO\)](#), [Symsoft Solutions](#) and [Finema](#) in March 2022.

Building on the open source [TRAIN Trust Management Infrastructure](#) funded by the European Self-Sovereign Identity Framework (ESSIF) Lab, the GCCN Trust Registry Network allows different COVID certificate ecosystems, which can be a political and economic union (e.g. the EU), a nation state (e.g. India), a jurisdiction (e.g. the State of California), an industry organization (e.g. ICAO) or a company (e.g. a COVID test administrator), to join and find each other on a multi-stakeholder network, and validate each other's COVID certificate policies. This interaction is known as a discovery mechanism. Then based on the discovery, verifiers will decide whose certificates they accept and use the Trust Registry Network to build a customized trust list based on their entry rules and check the source of incoming certificates against their known list to determine if it's from a trusted source. If the certificate is from a trusted source, the verifiers will be able to use the public key to decrypt and decode a COVID certificate.

[GCCN Trust Registry Network POC Demo IIW](#)

## ***They Might Be Squints? (or Distributed Addressable Processes)***

**Session Convener:** Chris Kula (denim.io) **Notes-taker(s):**Chris Kula

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

<https://drive.google.com/file/d/1C4dU0jpfyl85rv9YBQcpIGFT0-QNrTg/view?usp=sharing>

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

Other concepts discussed in addition to slide contents:

- Event sourcing (reconstructing state by replaying an input event sequence)
- The action model
- Rust: Actix
- Accession (new concept introduced by Denim)
- Implications for strong vs. eventual consistency

## *Self Sovereign IoT Decentralizing Sensors w/ Helium, PICOS & DIDComm*

**Session Convener:** Phil Windley **Notes-taker(s):** Phil

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

From [https://www.windley.com/archives/2022/04/easier\\_iot\\_deployments\\_with\\_lorawan\\_and\\_helium.shtml](https://www.windley.com/archives/2022/04/easier_iot_deployments_with_lorawan_and_helium.shtml)

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

I've been [interested in the internet of things \(IoT\)](#) for years, even building and selling a [connected car product called Fuse](#) at one point. One of the hard parts of IoT is connectivity, getting the sensors on some network so they can send data back to wherever it's aggregated, analyzed, or used to take action. [Picos are a good solution](#) for the endpoint—where the data ends up—but the sensor still has to get connected to the internet.

Wifi, Bluetooth, and cellular are the traditional answers. Each has their limitations in IoT.

- Wifi has limited range and, outside the home environment, usually needs a separate device-only network because of different authentication requirements. If you're doing a handful of devices it's fine, but it doesn't easily scale to thousands. Wifi is also power hungry, making it a poor choice for battery-powered applications.
- Bluetooth's range is even more limited, requiring the installation of Bluetooth gateways. Bluetooth is also not very secure. Bluetooth is relatively good with power. I've had temperature sensor on Bluetooth that ran over a year on a 2025 battery. But still, battery replacement can end up being rel maintenance headache.
- Cellular is relatively ubiquitous, but it can be expensive and hard to manage. Batteries for cell phones because people charge them every night. That's not reasonable for many IoT applications, so cellular-based sensors usually need to be powered.

Of course, there are other choices using specialized IoT protocols like ZWave, Zigbee, and Insteon, for example. These all require specialize hubs that must be bought, managed, and maintained. To avoid single points of failure, multiple hubs are needed. For a large industrial deployment this might be worth the cost and effort. Bottom line: Every large IoT project spends a lot of time and money designing and managing the connectivity infrastructure. This friction reduces the appeal of large-scale IoT deployments.

Enter [LoraWAN](#), a long-range (10km), low-power wireless protocol for IoT. [Scott Lemon](#) told me about LoRaWAN recently and I've been playing with it a bit. Specifically, I've been playing with [Helium](#), a decentralized LoRaWAN network.

Helium is a LoRaWAN network built from hotspots run by almost anyone. In one of the most interesting uses of crypto I've seen, Helium [pays people helium tokens for operating hotspots](#). They call the model "proof of coverage". You get paid two ways: (1) providing coverage for a given

geographical area and (2) moving packets from the radio to the internet. This model has provided [amazing coverage](#) with over 700,000 hotspots deployed to date. And Helium expended very little capital to do it, compared with building out the infrastructure on their own.

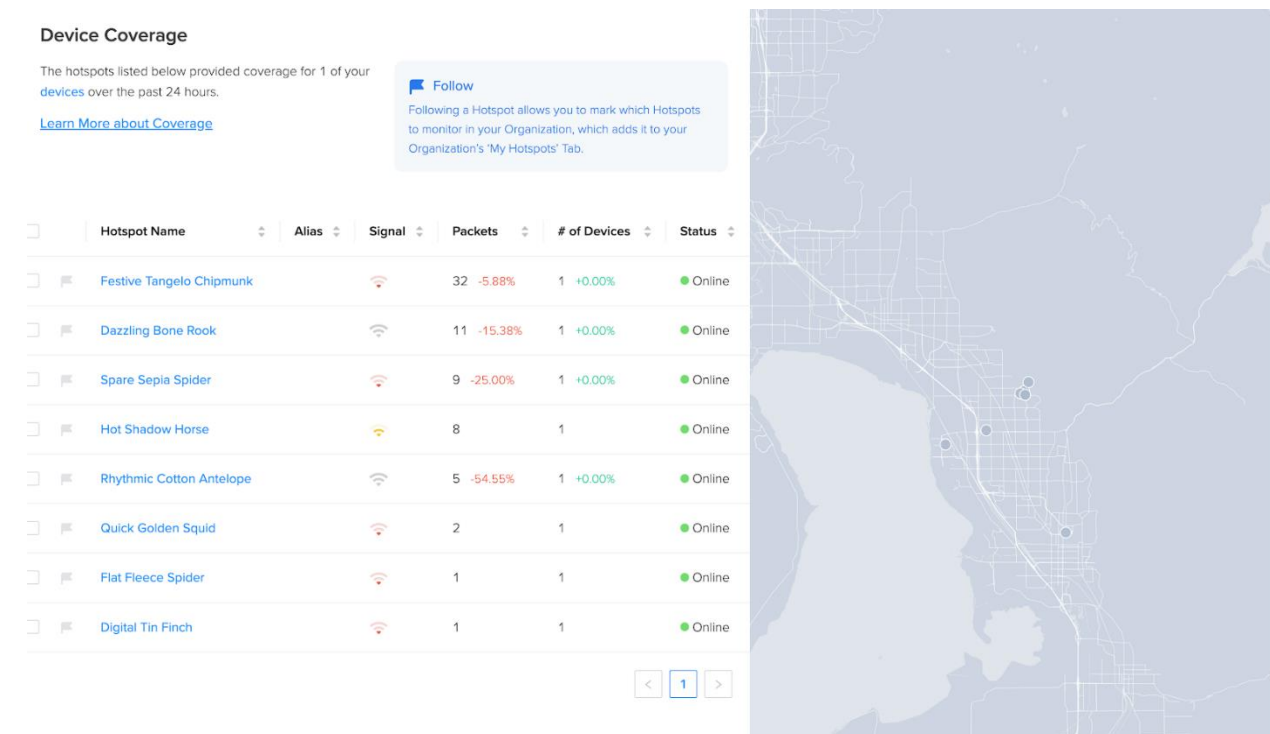
I started with one of these [Dragino LHT65 temperature sensors](#). The fact that I hadn't deployed my own hotspot was immaterial because there's plenty of coverage around me.



LHT65 Temperature Sensor

Unlike a Wifi network, you don't put the network credentials in the device, you put the devices credentials (keys) in the network. Once I'd done that, the sensor started connecting to hotspots near my house and transmitting data. Today I've been driving around with it in my truck and it's roaming onto other hotspots as needed, still reporting temperatures.





Temperature Sensor Coverage on Helium

Transmitting data on the Helium network costs money. You pay for data use with data credits (DC). You buy DC with the Helium token (HNT). Each DC costs a fixed rate of \$0.00001 per 24 bytes of data. That's about \$0.42/Mb, which isn't dirt cheap when compared to your mobile data rate, but you're only only paying for the data you use. For 100 sensors, transmitting 3 packets per hour for a year would cost \$2.92. If each of those sensors needed a SIM card and cellular account, the comparable price would be orders of magnitude higher. So, the model fits IoT sensor deployments well. And the LHT65 has an expected battery life of 10 years (at 3 packets per hour) which is also great for large-scale sensor deployments.

Being able to deploy sensors without having to also worry about building and managing the connection infrastructure is a big deal. I could put 100 sensors up around a campus, a city, a farm, or just about anywhere and begin collecting the data from them without worrying about the infrastructure, the cost, or maintenance. My short term goal is to start using these with Picos and build out some rulesets and the UI for using and managing LoRaWAN sensors. I also have one of these [SenseCAP M1 LoRaWAN gateways](#) that I'm going to deploy in Idaho later (there are already several hotspots near my home in Utah). I'll let you know how all this goes.

## ***Thoughtful Biometrics - A conversation & Workshop in July***

**Session Convener:** Kaliya Young

**Notes-taker(s):** Kaliya Young & Eileen Guo

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

This conversation was convened to go over the upcoming Thoughtful Biometrics Workshop  
[@TB workshop](#)

Biometrics conversation

Test Fraud is high in the developing world and SAT

Background check quality - isn't great right now

Scary to much Verifying

Lying is human - Certain behaviors should not be subject to public scrutiny

Social media system insist on real ID

Bank today different - bank of past - More KYC and Data systems

Security "Boogie Man" agree idealistic way

Push universal - enforced on everyone not good

Digitize something its Record is potential truth

Perfectly Credentialized World

Paper Record in Dossier

Mass Surveillance w/

Not literal anonymity - they don't want scruteningy of every day life

Harassment and Abuse

Issues with facial recognition ⇒ but can w/ surgery / weight

Can't change finger prints - yes injury

How do we regulate the possibility the really bad

Industry is Very uncomfortable with

1:1 AuthN

Attestation use-case

Surveillance huge implications

You using tool to make your life better

Them making a tool to make their life better



## **mDL + FedCM + VC-data-model = ?**

**Session Convener:** ?? Did not include name on Session Post

**Notes-taker(s):** Heather Flanagan (but the notes need fleshing out; tagging [Kristina.Yasuda@microsoft.com](mailto:Kristina.Yasuda@microsoft.com))

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

FedCM = <https://github.com/fedidcg/FedCM>

See also:

- <https://developer.chrome.com/blog/fedcm-origin-trial/>
- <https://developer.chrome.com/docs/privacy-sandbox/fedcm/>
- <https://github.com/privacycg/is-logged-in>
- SIOP = [https://openid.net/specs/openid-connect-self-issued-v2-1\\_0.html](https://openid.net/specs/openid-connect-self-issued-v2-1_0.html)

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

What is FedCM? “The Federated Credential Management API aims to bridge the gap for the federated identity designs which relied on third-party cookies. The API provides the primitives needed to support federated identity when/where it depends on third-party cookies, from sign-in to sign-out and revocation.”

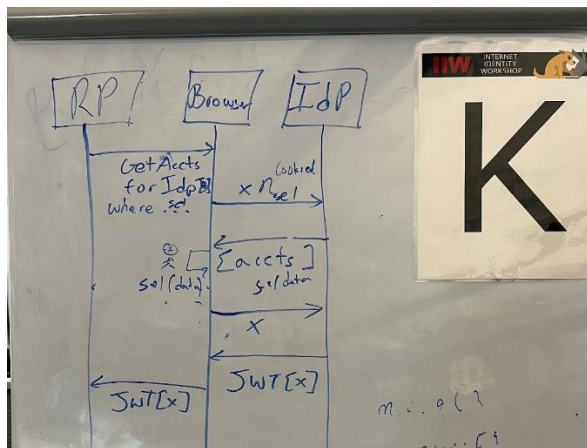
Hope to help fix some of the NASCAR problem.

Data formats? Browser is depending on the IdP to provide the id token. Browser has access to the cookies set by the authentication flow.

Where it might not be satisfying to the VC/mDL model: The RP has to name the IdPs. It's also very OIDC-specific.

There is a separate proposal (isLoggedIn) that might be of interest

Does the IdP have to be involved? This may be where SIOP is of interest. It's an open question as to whether FedCM would even be of use where SIOP is practical. Maybe when mediating when SIOPs?



## SESSION #14

### *Presentation Exchange Over http(s)*

**Session Convener:** Ingo Wolf

**Notes-taker(s):** Ronald Koenig

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

Ingo explained the motivation to connect RP to the SSI eco-system using a simplified protocol.

Starting point was DIDComm stripped down to the capabilities of the RP (JOSE, HTTP).

Persistent connections (DIDComm) are not required for presentation exchange in context of an RP. Connection is closed after presentation exchange.

Relying parties can use existing capabilities to process jwt\_vp and jwt\_vc.

There was some lively discussion around the simplification that is welcome as an approach that might be included in similar ways in DIDcomm v2.

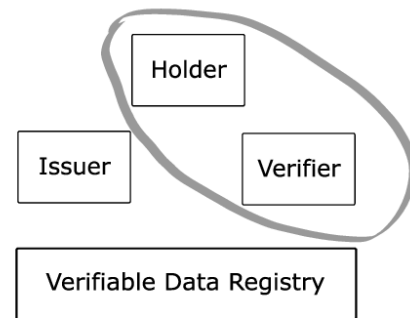
Slides:

presentation exchange  
- over -  
http(s)

simple path for existing OIDC relying parties towards  
verifiable credential/verifiable presentation capability?

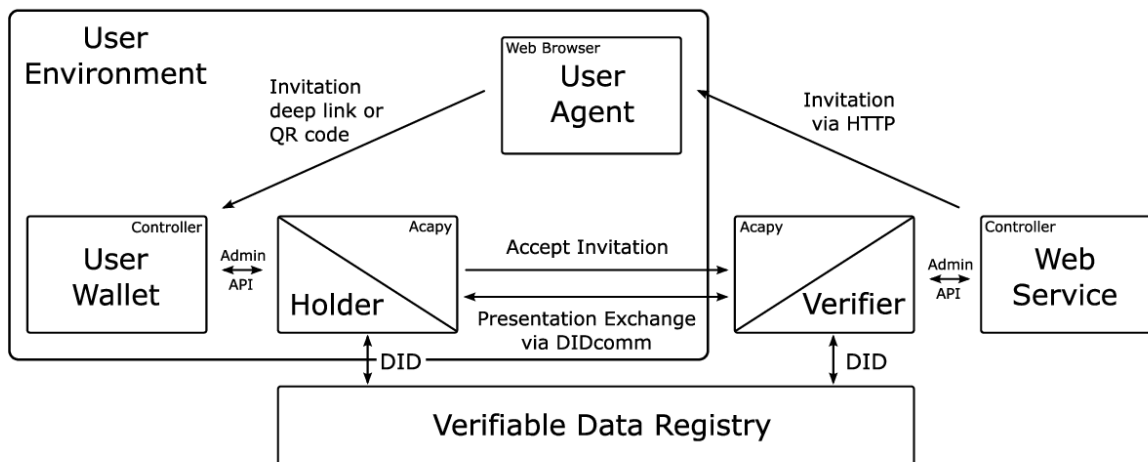
## scope and motivation

- DIDcomm is a great protocol, but brings some implementation complexity for existing (OIDC) relying parties that utilize **Jose/JWT** processing capabilities for IDtoken verification
- Relying Parties / Web Services want to enable resource access for (wallet-) holders based on verifiable credentials and verifiable presentations
- in scenarios where no persistent connection is needed (session based approach)

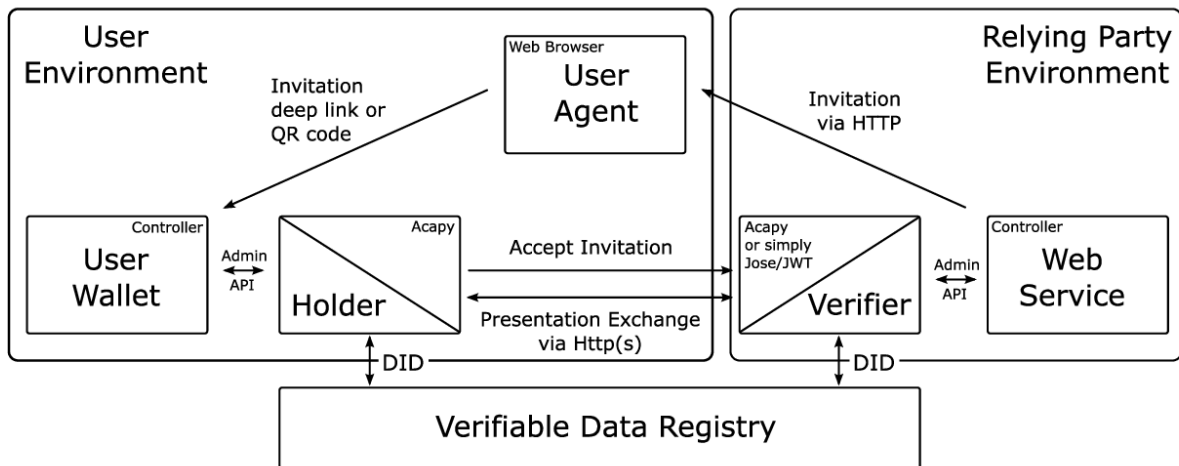


**iD**union

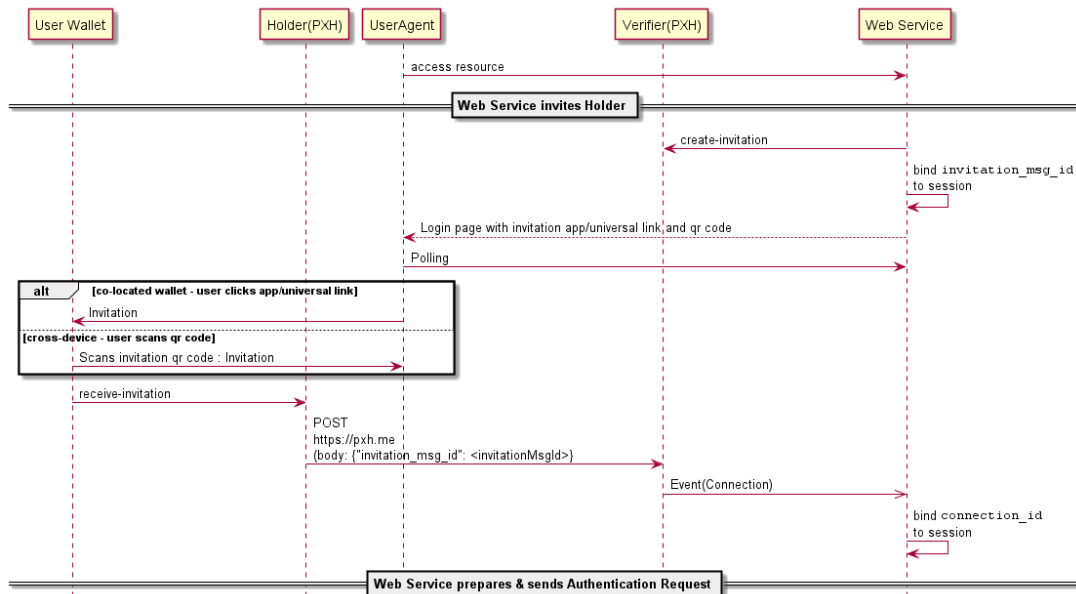
## Starting point: DIDcomm



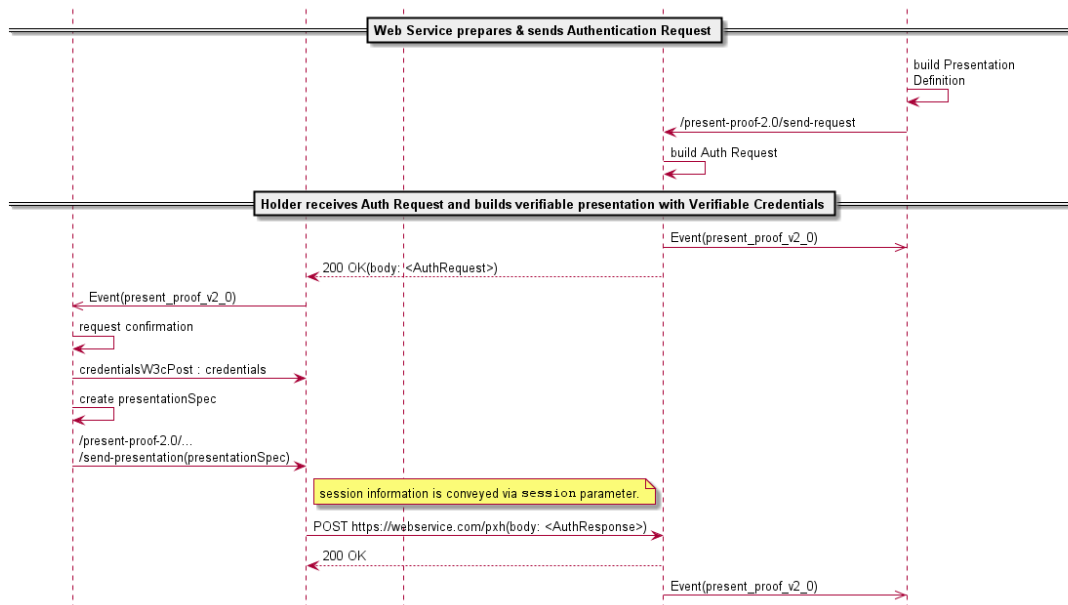
## simplified approach



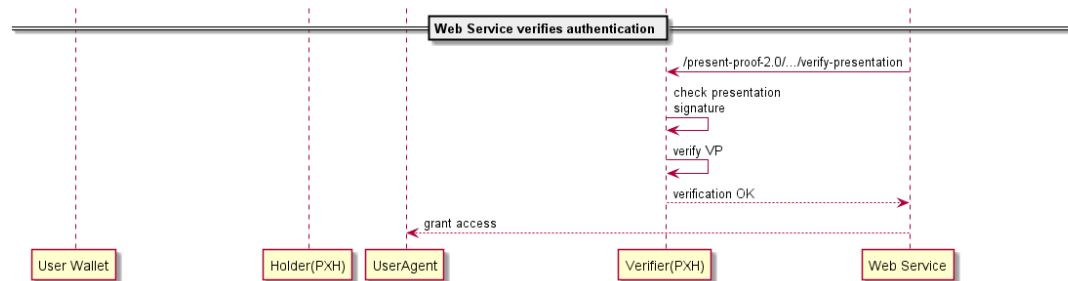
## message flow (1/3)




## message flow (2/3)



## message flow (3/3)



## findings and discussion (1/2)

- approach inspired by aries protocols and SIOPv2
- prototyped in german research project 
- relying parties send an out-of band invitation without any DIDs, verkeys or other DIDComm-related data in the resulting invitation message. Instead, a [service object](#) is used to advertise the verifier's HTTP (verification-) endpoint to the holder.
- similar to SIOPv2 deferred authentication request, but not compatible
- request with presentation definition (jwt\_vp and jwt\_vc)
- credentialSubject is did:key with
  - ldp proof type: ED25519Signature2018
  - Jose alg: EdDSA

## findings and discussion (2/2)

- holder must prove the control of the private key belonging to the holder did when presenting the proof to the verifier
- response with jwt\_vp

## references

- **Aries RFC 0067: DIDComm DID document conventions**

Tobias Looker; Stephen Curran. 10 June 2019. Hyperledger Foundation. <https://github.com/hyperledger/aries-rfcs/tree/main/features/0067-didcomm-diddoc-conventions>

- **Aries RFC 0434: Out-of-Band Protocols**

Ryan West; Daniel Bluhm; Matthew Hailstone; Stephen Curran; Sam Curran; George Aristy. 1 March 2020. Hyperledger Foundation. <https://github.com/hyperledger/aries-rfcs/tree/2da7fc4ee043effa3a9960150e7ba8c9a4628b68/features/0434-outofband>

- **Aries RFC 0454: Present Proof Protocol 2.0**

Nikita Khateev; Stephen Curran. 27 May 2020. Hyperledger Foundation. <https://github.com/hyperledger/aries-rfcs/tree/eace815c3e8598d4a8dd7881d8c731fdb2bcc0aa/features/0454-present-proof-v2>

- **Decentralized Identifiers (DIDs) v1.0**

Manu Sporny; Amy Guy; Markus Sabadello; Drummond Reed. W3C. 3 August 2021. W3C Proposed Recommendation. <https://www.w3.org/TR/did-core/>

- **DID Specification Registries**

Orie Steele; Manu Sporny; Michael Prorock. W3C. 02 November 2021. W3C Working Group Note. <https://www.w3.org/TR/did-spec-registries/>

- **OpenID Connect Core 1.0**

N. Sakimura; J. Bradley; M. Jones; B. de Medeiros; C. Mortimore. The OpenID Foundation. 8 November 2014. Approved Specification. [https://openid.net/specs/openid-connect-core-1\\_0.html](https://openid.net/specs/openid-connect-core-1_0.html)

- **Presentation Exchange v1.0.0**

Daniel Buchner; Brent Zundel; Martin Riedel. DIF. Ratified Specification. <https://identity.foundation/presentation-exchange/spec/v1.0.0/>

- **Self-Issued OpenID Provider v2**

K. Yasuda; M.Jones. 28 January 2022. [https://openid.net/specs/openid-connect-self-issued-v2-1\\_0.html](https://openid.net/specs/openid-connect-self-issued-v2-1_0.html)

- **Verifiable Credentials Data Model v1.1**

Manu Sporny; Grant Noble; Dave Longley; Daniel C. Burnett; Brent Zundel; Kyle Den Hartog. W3C. 3 March 2022. W3C Recommendation. <https://www.w3.org/TR/vc-data-model/>

Thanks for your interest and  
welcome feedback!

## *Let's KERI on Together.*

Session Convener: Phil Fearheller

Notes-taker(s): Phil Fearheller

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

[Practical Introduction to KERI: What Else Can I Do Today](#)

## *@ Address - Fingerprints #Tags a discussion of identifier classes*

Session Convener: Aaron D Goldman

Notes-taker(s):

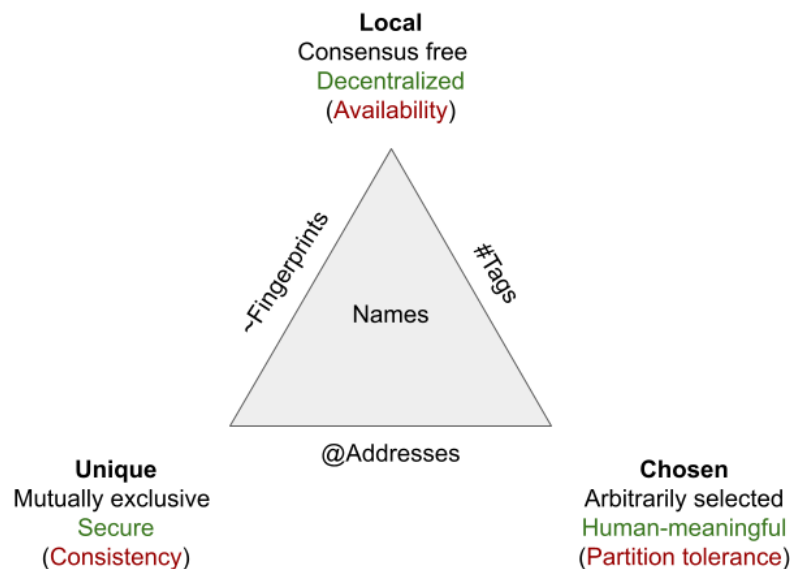
Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

[@Addresses ~Fingerprints #Tags](#)

We started with the discussion of Zooko's triangle AKA the CAP theorem

A name is Local, Unique, or Chosen but you can only pick two.

In order to build the systems we want we need to bind together identifiers from two or more categories.



My name in **bold**

Zooko's name in **Green**

Brewer's CAP theorem in **(Red)**



One might want to bind a public key (~fingerprint) with a verifiable credential(@address) to get an ID that can be generated Locally but that can have its Secure assertions added later.

## ~Fingerprints

### Local Unique (AC)

Issued by random number generation

You don't get to pick the name

- Hash
- Public Key
- Certificate

## @Addresses

### Unique Chosen (CP)

Issued by a consistency preserving authority

You need to get permission to use this name

- Phone Number
- Postal Address
- Email Address
- Social security number
- Twitter handle
- ens.domains

## #Tags

### Chosen Local (AP)

Issued by anybody

Many users may use the same label

- Given name
- Family name
- Attributes
- Hashtags

## pid (Power scaled Identifier )

We also proposed a power scaled identifier pid that would allow a “short” identifier that is both secure and typeable by a human with a low error rate.

We start by generating a certificate with keys and tags as desired.

```
{
  "type": "https://schema.org/pid",
  "public key": public_key,
  "public salt": public_key_salt,
  "name": "Alice",
  "revocation authority": "{pid}",
  "rotation authority": "{pid}",
  "salt": salt,
  "...": "...",
}
```

We also include a salt that is a random number. By varying the salt we can generate many versions of the certificate. We hash each version and keep the one with the lowest hash.

The pid is an encoding of the hash where we run length encode the leading 0s and the next 75 bits of the hash.

e.g.

**~vbazpoyabpjpebvn**

Is a representation of the hash

**2222bazpoyabpjpebvnxrrpq7bv6lls5pubxmpvgoxmr4gwmk  
a72=====**

The four '2's are represented as a single 'v' and the next 15 chars of b32 are quoted to get

## Vbazpoyabpjpebvn

This pID is short enough for a business card and can be read over a phone if needed.

~vbaz**poya**bpjp**ebvn**

Lookup path:

- Know the pID
- Pull the origin cert using the pid as a key
- Use the links in the cert to pull the updates to the pID
- Validate the updates are signed by keys in the origin cert or an already validated update.
- Apply the updates to build the current state of the pID doc.
- Return the pID doc

The group proposed that this might be better served by making a did:pid:vbazpoyabpjpebvn instead of the ~vbazpoyabpjpebvn form and that the doc could be made compatible with the did doc spec to support pID in the existing did ecosystem.

Also a long form could also be supported for items where we expect more than  $2^{40}$  objects to exist.

Vbazpoyabpjpebvn pID-80

Vbazpoyabpjpebvn**xrrpq7bv** pID-120

**Vbazpoyabpjpebvn**

**Vbaz poya bpjp ebvn** on a business card some spacing chunks of four will improve readability

**Vbaz-poya-bpjp-ebvn**

***So I think an Open Space unConference would be good to do for my:  
Organization, Association, Community***

Session Convener: Heidi N Saul & Kaliya Young  
Notes-taker(s): Heidi

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

Feel free to reach out to us! We design, produce and facilitate both in person and online Open Space (unConference) events

Heidi Nobantu Saul - [Heidi@HeidiNobantu.com](mailto:Heidi@HeidiNobantu.com)  
[www.heidinobantu.com](http://www.heidinobantu.com) @nobantu

Kaliya Young - [Kaliya@identitywoman.net](mailto:Kaliya@identitywoman.net) @identitywom

***Life is Global - Living is Local LIL & LOL - Building for Humans without Bull-Dozing their Humanism***

Session Convener: Jeff Orgle Notes-taker(s):

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

**Life is Global - Living is Local**

The first place I was exposed to traffic roundabouts was in a city far from where I live. While the idea of a roundabout made some sense, where I came from, we stopped for such interchange of intentions. Roundabouts were new, challenging, not at all stopping like we did, and therefore a bit hard to simply accept, especially considering the risk space of physical harm. Roundabouts are now somewhat common in my town of St. Louis, and becoming more so.

St. Louis has more stop signs than any city in the US I hear. We are deeply invested in the idea and influence of Stop signs. And...we ourselves have developed a compensatory practice/system in order to ease the friction known as the "St. Louis Stop". Urban Dictionary has this; ***"St.Louis stop - an action where you come up to a stop sign look both ways but never actually make a complete stop."*** It is a rolling stop which is breaking the law... "You Roll It, We Write It" say the signs around town...and you will know it is not just a threat. I think St. Louis is learning to exist with roundabouts and relaxing and breathing easier as they appear.

As it goes, good ideas find their way.

Now let's ponder a locale that has manufactured "Stop" signs for other locales since the birth of stop signs. How do they feel about roundabouts displacing "Stop" signs at intersections? What would change for the people who are making less of those signs? What rituals would change on those streets?

How ancient are those rituals and what value is therein? Think of destinations that are prized for their stasis in time. The old fashion feel. Classic archeology. The paths up to cave drawings. Would displacement by smoother, faster procedures help them...or not? Would St. Louis lose its St. Louis Stop tourism draw - if there were such a thing? Could it begin to change everything - more than anyone needed - or wanted?!

### **Designing For Humans without Displacing (Bull-Dozing) their Humanism.**

As we move to care for our world in our IIW community, we are diligent to consider how to raise all peoples in the range of reach and reach as full a constellation of people as can be cared for by the designs and concepts IIW generates.

Ideally IIW and global spec design is to include all. IIW reaches for that range of functional outcomes by creating "Use Cases". To my sense, Use Cases are highly specific and granular estimations of people living their lives which are very localized to an area, usually, and by some amount of definition, the realms they reside in. Sometimes a local life is far flung into other places with other cultural values, rituals and practices via travel. Sometimes we are in a locale designed for other manners of living and we will need to find our way in THOSE local systems of traditions. These things might be traffic law, cultural deference, currency, language and maybe even attire. Wherever we go, there we are. As we travel by choice or force, living is re-localized more or less.

How can design deliver a managed structure with the value-added quality of self-contouring fit and finish to the environment it will curate? As water fills a vessel to embrace its nature from the inside, can design do that? What portion of a Technocratic Oath-like foundation is that basis? That design/code will be the water. The communities and their nature will be the vessel which will hold such intentions, more or less so.

It has been very apparent that the ability to grasp the "Life is Global" portion of the mission causes immeasurable contemplation and consideration and also is impacted by limited heads and experiences in the room. While we call for more voices, more diversity and more breadth of community at large, at our best we can only gain an approximation of what the people involved in these local lives alongside these systems will experience. Hopefully what IIW generates is aligned with respect of regional/cultural/ethnic way of being. Because Living Is Local, not Global. I would refer to this as what

### ***I call Real People Really Being People.***

How is it that this is going to be so difficult? While not resigning the effort towards this somewhat ethereal goal of considering and designing for all, it seems we must recognize that we will likely never, ever, have all the different voices and ethnicities in the room. It is an unwieldy order. A convention of representatives of phenomenally granular range at a world size round-table may do it. That's a lot of chairs in the room! OK, then what might the "chairs" look like? Online voting, telecom, dunno?! How many would that be? A stadium of 100,000 global, regional, community level representatives? Is that enough? Sort of what I heard in a movie once - we may find out "we need a bigger boat!" The world

will not fit in a boat yet it is the boat we are in. And some don't like oceans and/or water one bit. People are different. Governments are different. Geographies are different. Solutions recognizing that will be different.

"Be Like Water My Friend(s)." - Bruce Lee

How can this be managed more granularly such that we design for a basis that can be amoebic and adaptable and sensitive to the locales the design finds its way into.

***Maybe we can code to Be Like Water.***

As our community moves forward, the idea of a recognizable harmonic of respectful tech design intention may be able to set a tone for those myriad spaces. Harmonics travel through space like water. Sound follows the characteristics of water and vice versa, as they are both fluids. They are both therefore dynamic. Can we create a harmonic code/design philosophy/delivery mechanism that can arrive into a locale as easily as a tribal drum immerses and wraps around the hills and valleys and open spaces of the "locale" that people live in?

As we reach to deliver curating intention, those harmonics which contain respectful values and concepts may be forwarded to the town elders, town square discussions or legislative processes, however ideas and structures are entreéd, considered and welcomed, or rejected in part or total, by the locales of our world. Those things that have been working may not need or even welcome rebuilding and re-jiggering of social aspects. Yet a portion of the design/idea may enhance the considered space and therefore the design/idea is welcomed.

Can there be a framework wherein the delivered structure may be set in place in portions and then receive a later, respectful/gentle inlay of those things which find appreciation in value scaffolding as the community finds benefit in the initial guidance and arc of healthful influence from respectful design? Can that be appended and amended to allow for the next perceived design value steps to be onboarded when wanted or needed? Can we consider not landing a fully inclusive set of services amounting to a contract of adhesion - all or none, all at once as the only option without bulldozing everything in its trajectory arc and implications wake...?

For example, can a current locale's currency of reputation find a relatively regionally accessible design node of a sort which will convert that into a more globally fluid and usable value framework? Could this node be at the locale's point of connection to a bigger faster world while expressing guardianship of forcing or foisting non-essential relationship/identity factors? If so, a community's current tradition and culture, which may have its own handle on the idea of attributing value(s) to an identity, can be left as is. Later a gateway to allow touch to the global systems to expresses governorship of data/value exchange may be put in place until more connection is wanted or needed.

More on this @ IIW.35! As the Cars said let's "Shake It Up!"

—  
***From the JeffO thought Kitchen***

***How to make a Globally Respectful, Non-allergenic Secret Sauce Recipe as possible?***

**Recipe: A + AD = U (Altruism + Agnostic Demeanor = Unassailable Intention)**

Allows for best chance to announce intention which would signal respect of locales. Eases the idea of offering/interjecting awareness and options which may alleviate locally identified challenges being experienced by those locales.

The "Unassailable" matters in the sense that the effort will be seen as doing the best that can be done because **Altruism** is a selfless and respectful thing to signal. **Agnostic Demeanor** (tonality) insists the effort is going forth without preference or limitation as to the recipient(s) of the benefits therefore displaying openly, and holding high, unbiased intention as a core operation and value.

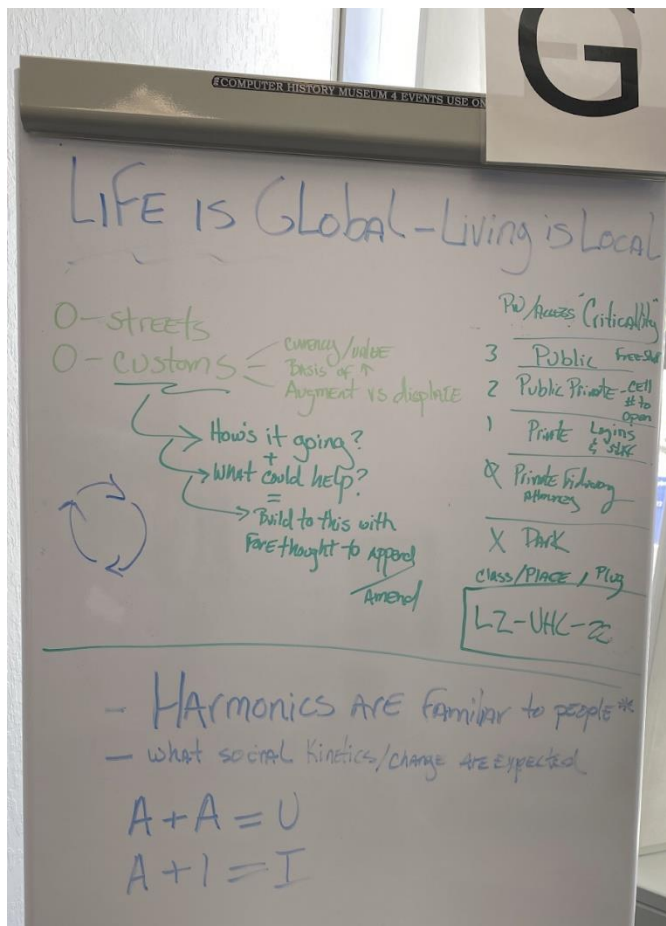
Onboarding > Arriving in Locales of the world and demonstrating uniform consideration of respectful awareness by the efforts to assist/improve/rescue.

### Informing of Opportunity for Wellness / Betterment

Greasing the pan of receptiveness:  $A + (C)I = I$  (Awareness + Intrigue = Information (a call to know more))

"A story is data with a soul." – (roughly) Brené Brown

Ask to hear stories of challenge. Find an  $A + I = I$  story framework and invest the story in the locale's space of concern or betterment wants.



## *Are you telling the story you think? Communication Workshop*

Session Convener: Kimberly Wilson Linson

Notes-taker(s):

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

### Three principles and a Law for Communicating with Humans

1. Dual Coding Theory - Alan Pavio - Our ability to comprehend information is directly correlated with our ability to connect language with mental representation.
2. Humans are thinking FEELING beings...we make decisions on how we FEEL.
3. Human brains are lazy - don't make them work too hard.

LAW: Always start with the big picture/problem. ALWAYS. (And never ask "does anyone here need me to explain...")

### **— DISCUSSION NOTES—**

Must focus on the problem of the customer

Write a fake press release before the product is created

Avoid wiggle words

Developer need INTENTIONAL

Would a Driver's License be trusted at a if I put tape over the unnecessary PII?

New fintech - the problem is: UNBANKED....solving benefits the banks and the user

Watch Dick Hardt - [Identity 2.0 from the 2000s YouTube:](#)



## *The Everything Graph: Building Anything from Identity Primitives*

**Session Convener:** Daniel McGrogan **Notes-taker(s):**

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

Identify and break down the various identity and relationship primitives which exist, from which we can think about the entire space.

The two basic abstractions identified are

- “identities” which are universally unique monikers, the control of which is expressed by control of a private key.
- “relationships” non-repudiable statements made by one identity (issuer) about another (subject)

We can abstract many different relationship models with this. Verifiable credentials which are issued by a DID about a DID can be represented as well as a Bitcoin transaction where one identity (address) makes a transaction to another identity (address), IDPs issues a Identity token about a subject.

Once we have an appropriate abstraction which can be applied to such a wide array of systems we recognise that there is a universal identity graph where the nodes are identities and edges are relationships. Note the graph is not necessarily a completely connected graph but may have clusters. One cluster may be the Bitcoin network, another the Ethereum network, another a collection Decentralized Web Nodes which have credentials referencing each other.

The graph itself is most likely too big to represent but is consistent enough to rationalize about and subsets of the graph may be codified for specific use cases.

What can we do with the graph

- Western Super Apps: there is a noticeable absence of super apps in the west. This may be in part due to the lack of strong identity which can be leveraged by the “applets” on the super app. SSI provides a mechanism for federated identity across the subject entity vs a centralized IDP. This provides an opportunity for a platform to bring together applications and users.
- DAOs & DAPs: Use of governance frameworks to describe process across identities can enable the DAPs which describe actions across different sub graphs e.g. a ethereum smart contract issues a VC to a DID subject holder who can then use it to share with a verifier at the door to a concert.
- The Metavers: if one considers the ability to tokenise any entirety physical abstract identity and we can represent any relationship between identity then we can create a meta layer of information on reality. This meta identity layer can provide endless possibilities of interaction, not just with other people in virtual meeting rooms but with anything in the physical world.

Constructive feedback: we are lacking the terminology or clarification required to discuss concepts in the abstract and implementations.

## SSI & IoT (identity powered renewable energy)

Session Convener: Michael Shea & Paul Grehan

Notes-taker(s): Paul Grehan

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

IoT SSI Renewable Energy

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

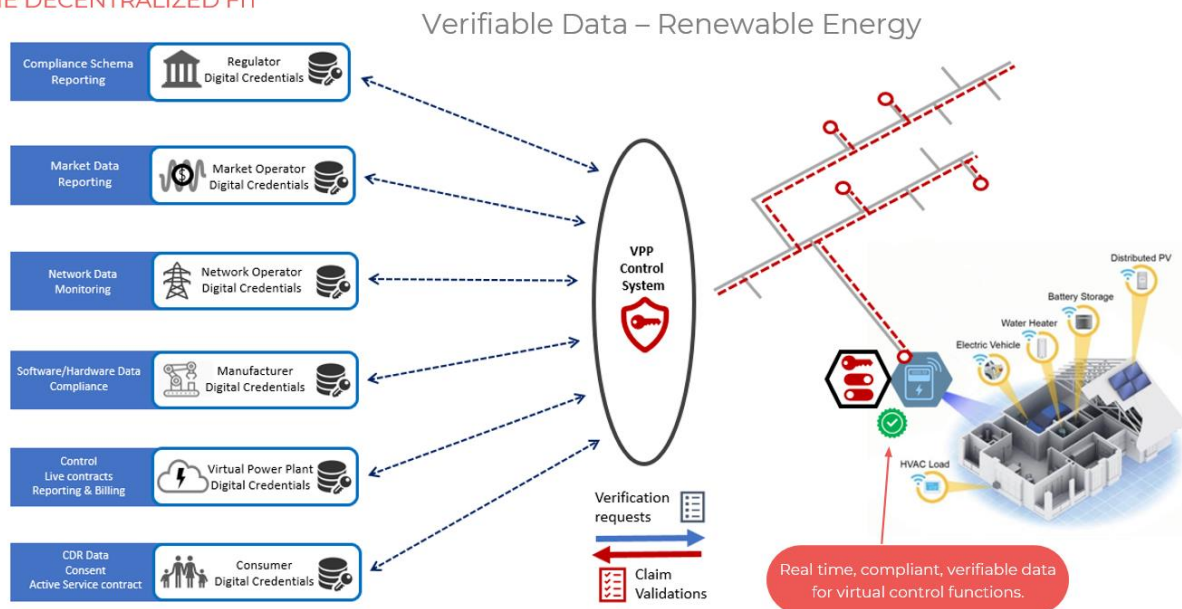
Discussion on how SSI can be applied to Renewable energy assets as a part of the grid.

The reliance on leveraging individual's renewable assets (Solar and Electric Vehicles) is increasing as we move away from traditional fossil fuels based power generation. In this talk we discussed how leveraging Identity for delegated control of assets, along with balancing privacy issues and grid requirements to help progress to a renewable future.

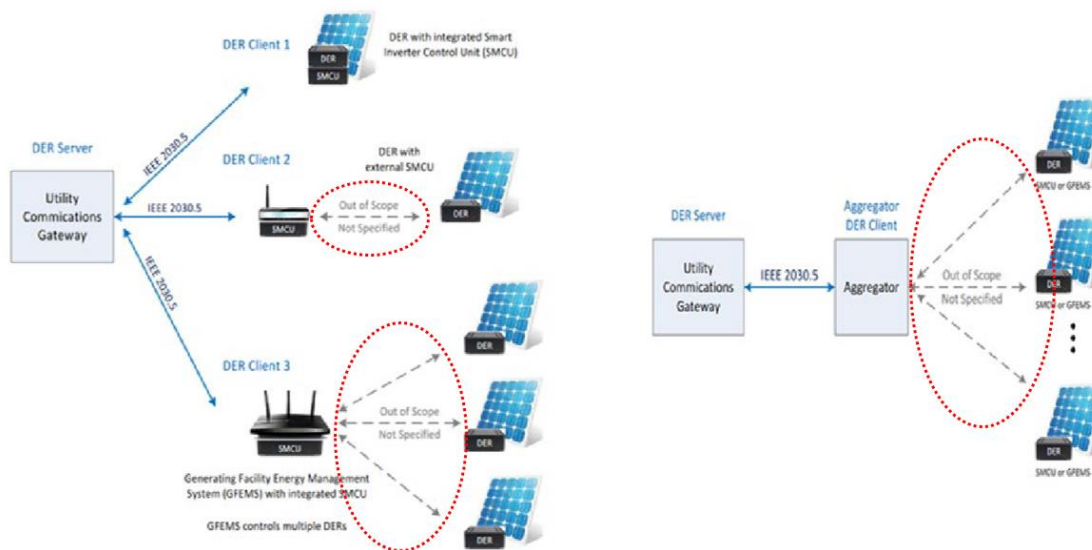
SSI elements included deployment of delegated (ZCAP) control to assets owned by the individual and how verifiable credentials can be used to help provide a level of security and trust required to participate in a critical infrastructure environment.

We covered opportunities and issues faced in providing a level of privacy whilst providing financial benefit and options that might be needed moving forward.

### THE DECENTRALIZED FIT



Dynamic Envelope – areas of concern (untrusted areas participating in a trusted environment)



## GDPR: Does the G stand for Glitter Nails? A shared Vocabulary

Session Convener: Chris Kelly (DIF)

Notes-taker(s): Chris, Peter

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

IDPro intro to GDPR (v2) <https://bok.idpro.org/article/id/11/>

ToIP Terms Wiki <https://wiki.trustoverip.org/display/HOME/Terms+Wikis>

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

Starting with a goofy title to catch attention, highlight confusion around acronyms and the need for clear, concise communication.

Acronyms get confusing fast, even for those in the community.

Best practice is to expand the term the first time it appears and link to further info is possible ([Terms wiki- ToIP etc.](#))

Material often goes out-of-date quickly

- Needs to be reviewed periodically
- Clearly marked with publish date (and edit date if needed)

Important to speak to various audiences and remember to meet people where they are at

Co-opting and leveraging existing concepts, use cases and terminology can be helpful

One Example is **GDPR**

- Came into force in the entire EU May 2018
- Applies even to businesses operating outside the EU with EU citizen data
- Legal obligation and regulatory oversight
- This forced most businesses to examine how they handled data
- Also introduced them to identity concepts
- Lots of localized explainer material
- Many service providers offering middleware/compliance services/audits

Specific mention goes to terms used/defined:

- **Personal Data**
- **Special Category (sensitive) Data**
- **Processing**
- **Data Controller**
- **Data Processor**

GDPR includes and is underpinned by specific concepts:

1. **Lawfulness, Fairness, Transparency:**
2. **Purpose Limitation**
3. **Data Minimisation**
4. **Accuracy**
5. **Storage [time] Limitation**
6. **Integrity and Confidentiality**
7. **Accountability**

A number of these (eg Data minimisation - selective disclosure) maps onto some SSI tech and concepts. These terms and principles can be used to further the conversation with partners about potential benefits and goals of SSI

**BONUS:** Lots of material explaining these at a variety of levels is available in a variety of languages (not just EU!)

The current wave of 'passwordless' promotion and rollout can be another useful starting point for constructive conversations about data privacy and SSI, as well as concerns about data leaks and hacks.

The communications around SSI and decentralized ID need to be

1. **Accessible & Easy to understand**
2. **Tailored to the audience**

3. **Aligned across the community/orgs**
4. **Accurate**
5. **Current (and marked with publication dates!)**

Community resource creation is an excellent way to provide resources  
These can serve B2C and B2B businesses in the space and help them have conversations with investors, customers, policymakers etc.

Examples of resources that can serve this purpose:

- Lexicon of SSI terms
- Dictionary of Acronyms
- Simple Primers
- Explainer articles about specific key technologies or elements
- Example pitch decks
- Highlight Use Cases and real-world examples
- Sample talking points for speaking opportunities
- Road Maps
- Best Practice guides

### **Next steps**

Assemble a modular toolkit for community members looking to have conversations about SSI  
A selection of material for a specific level and audience  
Refine, iterate and update these materials

## ***Cards Against Identity***

Session Convener: Justin R

Notes-taker(s):

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

<https://bspk.io/games/cards/>

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

## SESSION #15

### *AR - ACDC Reputation - How to build a distributed auto resourcing Algo using ACDC*

**Session Convener:** Sam Smith **Notes-taker(s):**

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

[https://github.com/SmithSamuelM/Papers/blob/master/presentations/AR ACDC Rep.web.pdf](https://github.com/SmithSamuelM/Papers/blob/master/presentations/AR%20ACDC%20Rep.web.pdf)

### *Going to DWeb Camp Aug 24 - 28 Community Planning*

**Session Convener:** Kaliya and Friends **Notes-taker(s):**

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

[DWeb Camp](#) is happening August 24-28th in Northern California - about 3 hours north of San Francisco.

They are inviting people and communities to submit ideas for topics and projects.  
So Kaliya called a session to explore ideas for what the community might share at the event.  
Some suggestions were made without people from those projects present.

Here is the list

- DIDs for DAOs
- Why BlueSky Likes DIDs
- How Verifiable Credentials play a role in KYC
- DISCO is the grovy tool for Web3 ID
- How are DIDs being used by a range of projects
- Introduction to Standards and a Map of the Organizations and Working Groups

## Discussion: Best Practice & Architecture for Cloud Enterprise Wallet

Session Convener: Azeem Ahamed

Notes-taker(s): Markus Sabadello

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

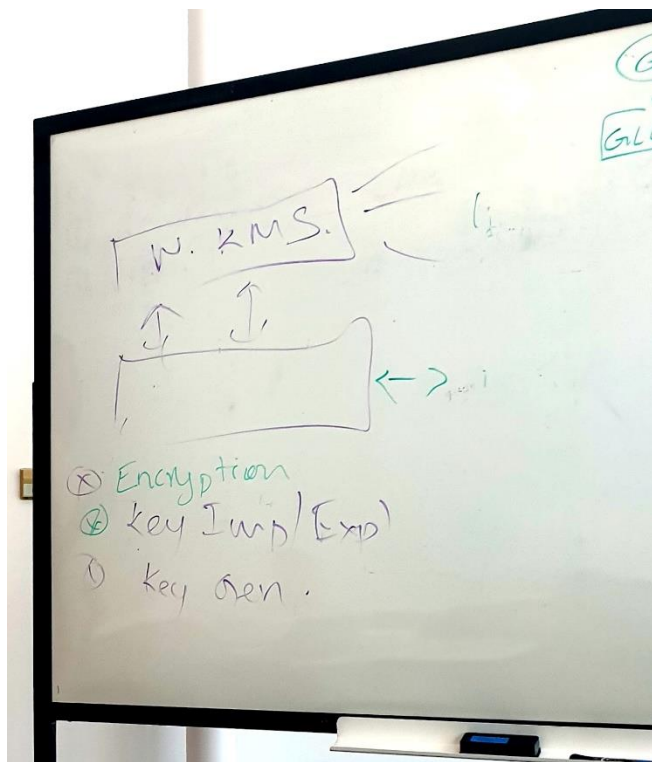
Cloud Wallet, Enterprise Wallet, Security

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

How can cloud wallets be secured, that store users' private keys?

Topics:

- Private keys could be encrypted twice - once with a key the server holds, and with a key the client holds
- Maybe a signature generated by FIDO/WebAuthn could serve as a seed for a client key that gets re-generated every time on the server
- Where/how do keys get generated and stored?
- How can keys be imported/exported?
- Use of key derivation functions
- Hierarchical deterministic keys (HD keys).. Keys can be less privileged than master keys



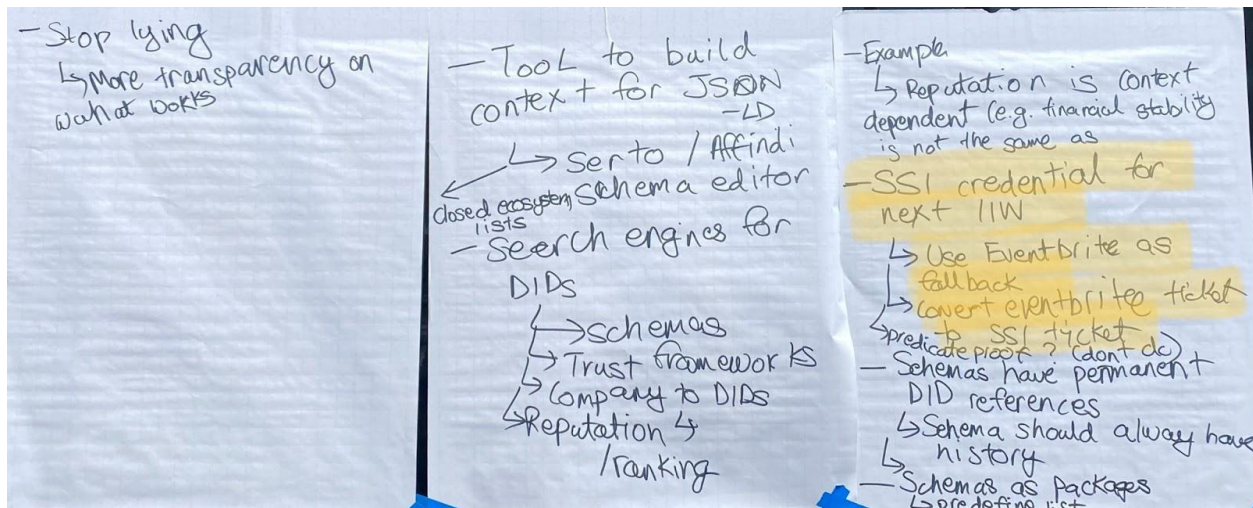


## Moonshot ideas to GET DONE by NEXT IIW

Session Convener: [Ankur Banerjee](#)

Notes-taker(s): Ankur Banerjee

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



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

### Main takeaway/idea

Let's all come together to have **SSI credentials as the tickets for next IIW!** We spend so much time competing with each other, that we sometimes forget to play nice 🤝 ([Twitter thread about this.](#))

- Yes, we know this was done once in the past (3-4 years ago). However, the SSI/digital identity industry has moved on vastly since then and the technology has evolved too. This could even be a recurring thing.
- We don't need to solve the whole stack of event signup and management: that can still be on Eventbrite or similar platform, since it offers payments, email communications etc.
- After someone registers on Eventbrite, the QR code/PDF/email/wallet files could be turned into an SSI credential by any wallet. All it needs to do is to allow people to

## ***DIDLANG Language for DID identifiers, documents, clustered DID agents, and DID Objects***

**Session Convener:** Michael Herman **Notes-taker(s):** Michael Herman

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

- Twitter: <https://twitter.com/hashtag/didlang>
- Github: <https://github.com/mwherman2000/BlueToqueTools>

didlang is a new interpreted, command line language for working with DID Method Namespaces, DID Identifiers, DID Documents, DID Agent Service Endpoints, DID Agent Servers, DID Agent Clusters, and DID Objects (the 7 DIDs).

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

From today's discussion, two primary use cases were identified:

1. Interactive exploration of a DID Identifier's DID Document, DID Agent implementations as well as the value of the object identified by the DID Identifier.
2. Simple, elegant query language for DID Method Namespaces, DID Identifiers, DID Documents, DID Agent Service Endpoints, DID Agent Servers, DID Agent Clusters, and DID Objects ...supporting all CRUDV operations against each of the above. A value property of a didlang query is that it can be remoted through multiple hops (multiple DID agents).

## ***DID Method Rubric***

**Session Convener:** Joe Andrieu

**Notes-taker(s):** Peter Conerly

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

The DID Method rubric came out of the discussion out of "what was a decentralized identifier". We couldn't agree on a common definition that was suitable for everyone.

"DID as a format that combines both issuer and identifier. Method is kind of issuer, or the domain in which this credential is unique. There's value in that structure regardless of whether it's decentralized. There's potentially a lot of value here even if they're not decentralized, and we'd like to let them still use the `did:` prefix." - George

DIDs have 3 columns:

- Sovereign system:

- Ethereum
  - Bitcoin
  - Mastercard
  - “We will manage our data how we want to!!!”
- Apps: can use decentralized identifiers to verify actions taken on sovereign systems
  - Banks
  - Messengers
- Resolvers
  - Can verify a DID and retrieve DID documents. Ideally resolvers are run by apps and are open-source
- 

Running it on PREM is most trustworthy than AWS?

Sometimes you care about reliability, sometimes you care about anti-censorship

Criteria rubric for DID systems

<https://www.w3.org/TR/did-rubric/#the-criteria>

Evaluators need to disclose how they evaluate dids

How is the did-rubric updated?

It's now an informal registry. As a registry, there is a registration process and it will explain how to make a pull request.

In evaluations, there needs to be a use case specified to understand the use case specification.

Implementations are ignored for the case of evaluations. Internet has a lot of vulnerabilities

Who are the users of the did method evaluations?

- It's organizations that need to evaluate these did method implementors
- But also customers who are going to use these did methods and wants to choose a method.

## ***MOBILE CREDENTIALS - wish lists, changes to standards org, how to help each other***

Session Convener: [Andrew Hughes](#) andrewhughes@pingidentity.com

Notes-taker(s): Andrew Hughes

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

- The group brainstormed things that we want to request from other groups or organizations. There are some action items for follow up that each of us will pick up and tack back into our standards bodies.
- Wish list – to device manufacturers
  - 3<sup>rd</sup> party vendors can implement all listed functions from 18013-5 spec – e.g. NFC engagement is not possible for 3<sup>rd</sup> party apps on iOS
  - Secure Area / Enclave access – functions and data access is limited
  - Access (read or create) to multiple biometric template profiles (e.g. apps can only see that a biometric check passed/failed) – this limits information needed for authorization/decisions by the app
    - E.g. apps have to add in-app authentication functions to get unique identification of human
- Wish list – for operation systems
  - User choice of invoked wallet (e.g. Custom URL scheme / Universal links) – to support wallet choosers (this is a dubious request)
    - E.g. scan QR with native camera app – behavior is to send user to platform wallet
- Wish list – for standards work groups
  - eCommerce presentment of mobile DL data
  - What are the requirements for this?
  - Liaison agreements
  - Active sharing of concepts and information
  - Individuals who can participate in WGs in different standards bodies
  - Regular Communication inwards/outwards
  - Awareness sessions / listening sessions
  - Common issuance/provisioning protocol standards that can handle any credential type
  - Consider abstracting the standards to accommodate non-platform software/hardware solutions
  - Recommended guidelines for hardware minimums – e.g. for different assurance levels
  - Open test suites & interoperability harnesses
  - Address terminal authentication – opens the user to risks if terminals cannot be authenticated (it is optional in 18013-5 today)
  - Could there be a “CBOR serialization” of VC?
  - Recognize existing well-exercised standards and technologies in own standards e.g. crypto suite selection, layering, etc.
  - Push generalizable topics to more-suitable standards WGs e.g. the mechanisms for crypto agility should be pushed to IETF; the concept of Secure Area should be exposed to the wider industry

- Education sessions on implementation complexity and heavy lift of standards choices e.g. “Developers really don’t like working with CBOR” – so teach standards writers why this is true
- Secure Area / key attestation formats are exploding – this needs standardization or coordination
- Look into an ISO IWA workshop to jointly develop <something>
- Support import/export operations e.g. move credential to another wallet
- Wish list – for regulators/legislator
  - Harmonization of regulations across jurisdictional authorities
  - Avoid closing down usage / presentation purpose – e.g. limitation for DL usage only is not great
  - Citizen protections – robust recourse pathways
  - Budget allocation to support technical implementation and marketing and public perception
- Wish list – for Industry
  - Standards for Measurement for enrolment mechanisms – degree of binding strength between person-DMV record
  - Kantara Initiative has an active WG “Privacy Enhancing Mobile Credentials” – defining requirements on Verifiers, Issuers and software vendors for protection of information

## ***Popper’s Paradox of Tolerance***

**Session Convener:** Justin Richer

**Notes-taker(s):** Justin

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

[https://en.m.wikipedia.org/wiki/Paradox\\_of\\_tolerance](https://en.m.wikipedia.org/wiki/Paradox_of_tolerance)

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

The session was attended by six white men. Anything discussed would be purely theoretical and not applicable to the lived experience of society at large.

## ***Digital Identity as a Response to Climate Change***

**Session Convener:** Shannon E. Wells of Unfinished Labs

**Notes-taker(s):** Same

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

Prompted by this article in Discover Magazine

(<https://www.discovermagazine.com/environment/can-the-blockchain-give-this-island-nation-threatened-by-climate-change-a>)

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

Wanted to discuss this particular response by the Tuvaluans to their situation; they are at risk of going completely under water. Points of discussion:

- Is their plan (digital identity, digitizing currency, governance as well as cultural assets such as literature, lore and music) the best plan?
- How did the main driver of this plan, George Sosi Samuels, arrive at these particular solutions, and would they have been different if he were aware of this organization beforehand?
- Does this suggest other threatened nations, groups or municipalities to reach out to?

Using digital verifiable credentials was also mentioned by Patrick M. as a way of tracking and providing accountability in carbon trading programs, however, he unfortunately had to leave the session. We would like to return to this topic in the future.

Shannon began the discussion by summarizing the article, saying that this was a response to the threat of losing a national identity, government infrastructure and access to wealth due to rising sea levels. More citizens are working and living abroad and sending money home to family. The need was seen for following the model of e-Estonia.

Shannon also referenced the Rohingya Project as another example of people responding to crisis with technological solutions (<https://rohingyaproject.com/>)

Chris Kelly observed that Tuvalu is small enough that there are a lot fewer trust barriers to overcome when instituting such a plan. Everyone more or less knows each other and so consensus and communication are easier. Also there is no need for an elaborate structure to prevent corruption and to increase trust.

Most agreed that the situation is special enough to not be able to draw very many widely applicable ideas from it.

Another thought from Samuel Gbota was that digitizing everyone's identity isn't very helpful without designed interoperability. If there is a diaspora of the nation's citizens it won't help them much if the IDs are not recognized by other nations.

Robert Reddick said that there are three situations to consider when deciding whether SSI and other digitization is an option. In "normal life" where you have generally enough resources for an effort, but

the risk of loss is low (making it harder to approach someone with the possibility). Next, where a group is aware of a crisis and its risks, and preparing for it, or considering how to prepare for it. Finally is crisis mode in which case people are generally worried about meeting basic needs.

It seems that rarely are people willing to find solutions to problems that haven't started surfacing yet and that people will be most receptive to possible solutions when they've recognized they are at risk and wanting to prepare. RR added that preparing for a crisis is largely a matter of organization. Then "how can organizing rest on top of identity," he asked, saying adopting SSI can be hard because it's a mitigation instead of prevention. He also recognized that a lot of people would be left out of an SSI/digital solution because they simply don't have the technology and infrastructure, and asked why telecoms don't just give away phones.

Anmol Sekhri replied that giving everyone a smart phone will not really work for people who don't have electricity and while technically not under "crisis" meaning famine, war or natural disaster, still have problems meeting basic needs. Secondly there is the language barrier as many people don't speak languages that are generally supported by smartphones.

Also there is the issue of education; if people don't have electricity they will generally not be in a position to know how to use smart phones. Furthermore there is a risk of digital colonialism.

This does not seem to be an issue with the two projects above as these were started by members of those communities.

The discussion also sparked a memory for Samuel about how two young children came up with a solution to poaching in their region by installing microphones around the area, and training an AI on the sounds of human footsteps and cars, so that the sounds, if detected, would be triangulated and authorities could go check out the source. He said that these were two young children who came up with this solution, so it's clear that people are in a position to help themselves in ways they need help, if given the knowledge and opportunity.

***"The Scout Mindset" Why some people see things clearly, and others do not.***

**Session Convener:** Timothy Ruff **Notes-taker(s):**

**Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:** No Notes Submitted

Notes in this book can also be found online at  
[https://iiw.idcommons.net/IIW\\_34\\_Session\\_Notes](https://iiw.idcommons.net/IIW_34_Session_Notes)

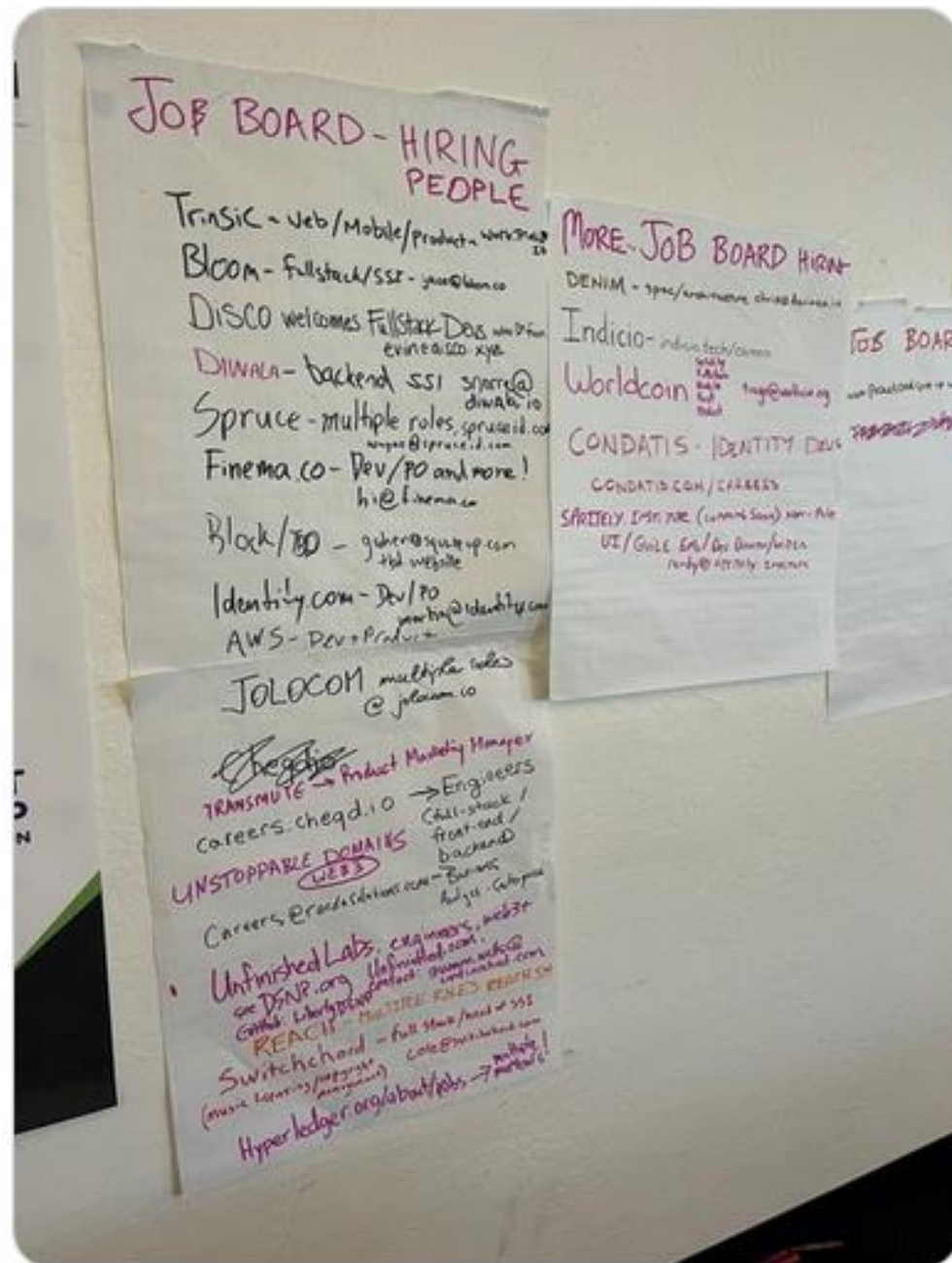




Hannah Sutor @hhsutor · Apr 27

Replying to @codenamedmitri

Well, the list only got longer...#IIW



# Thanks to our Demo Hour Sponsor!



**SPEED DEMO HOUR**  
SPONSORED BY

**DANUBE**  
TECH GMBH

## DEMO Table #

1. **GoDiddy.com - Universal DID Services:** Markus Sabadello - Danube Tech  
URLs: <https://godiddy.com/> GoDiddy.com is a hosted platform that makes it easy for SSI developers and solution providers to work with DIDs. Based on open-source projects Universal Resolver & Universal Registrar.
2. **UBOS Mesh** - what if you had all your personal data in a single place that you control?:  
Johannes Ernst, Indie Computing Corp URL: <https://indiecomputing.com/products/> Sometimes it seems that everybody has our data, except for us! (That's because it's true!) But under recent privacy legislation, we have the right to get everything they have about us, too. UBOS Mesh takes that data, parses it, and integrates it into a single MeshBase from where you can browse, search, and build bots and applications on it. What could you do with that in your own life? What could you do in the life of your customers?
3. **Global Legal Entity Identifier Foundation (GLEIF) The Keep** - KERI and ACDC Powered Enterprise Agent and Wallet for the vLEI Ecosystem: Kevin Griffin & Phil Fearheller  
URLS: <https://github.com/WebOfTrust/keri>, <https://github.com/WebOfTrust/keripy>, <https://github.com/WebOfTrust/keep> The Keep is an Electron desktop application with a task based user interface and embedded cloud agent and wallet deployed with tasks for all participants in the vLEI ecosystem for creating identifiers, making connections and issuing, holding and verifying vLEI credentials.
4. **HTTP Signatures and GNAP Interoperability Testing:** Justin Richer  
URL: <https://httpsig.org/> <https://gnap-c.herokuapp.com/> HTTP Message Signatures and the Grant Negotiation and Authorization Protocol (GNAP) are two new security efforts currently being worked on in the IETF to provide practical and functional security improvements on systems. We'll be demonstrating the playground for HTTP Message Signatures, where you can sign and verify arbitrary HTTP messages, as well as the XYZ implementation of GNAP, available as a hosted service for interoperability testing.
5. **Pravici PocketCred:** Mahesh Balan  
URL: <https://www.pocketcred.com/> Pravici PocketCred is a platform that allows for easy creation, issuance and verification of Verifiable Credentials. These credentials can be used in multiple contexts such as education transcripts, health records (such as proof of vaccinations). Pravici PocketCred is integrated with Salesforce HealthCloud.
6. **BOTLabs GmbH presenting DIDSign:** Antonio Antonino, blockchain engineer, [antonio@kilt.io](mailto:antonio@kilt.io)  
URL: DIDSign available at <https://didsign.io/>. <https://medium.com/kilt-protocol/announcing-didsign-a-new-application-built-on-kilt-e4896ffffb44>. DIDSign provides a browser-based digital signature suite for any digital files-PDFs, audio, video, software, etc., using Decentralised Identifiers. The resulting signature can be downloaded and shared with interested parties.

7. **Global Assured Identity Network (GAIN) Proof of Concept:** Torsten Lodderstedt/ Daniel Fett  
URL: <https://openid.net/gainpoc/> The GAIN PoC is pulling together a test bed where key technical hypotheses of GAIN can be tested over the course of 2022. We will show that relying parties can obtain assured identity claims from identity information providers from different jurisdictions (SE, IT, DE) and built based on different architectural approaches (central, distributed, SSI) via the same interoperable interface.
8. **NFID Internet Identity Labs:** Dan Ostrovsky  
URL: <https://NFID.one> NFID is a single sign-on protocol designed to guarantee anonymity across the accounts created with it, and secures the identity holder against all impersonation attempts
9. **humanID Anonymous SSO Solution:** Tim Hradil  
URL: [human-id.org](https://human-id.org), <https://web-login.human-id.org/demo/> humanID has developed a one-click, anonymous authentication solution that provides a safer online experience through the guarantee of user privacy and the prevention of bot, duplicate, and spam accounts.
10. **TrustSphere** - A Clinical and Research Application of User Managed Access: Alec Laws  
URL: <https://www.bcchr.ca/TrustSphere> TrustSphere is a consortium project between four Canadian companies. We will demonstrate a childhood Type-1 diabetes management platform, including shared control of a health record, an ethical digital consent process, and data sharing with researchers.
11. **Mysilio Garden:** Ian Davis  
URL: <https://mysilio.com/> Mysilio Garden is a Bi-directionally linked headless CMS that uses personal datastores, decentralized identity, and Web Monetization to support creating, publishing, and monetizing Digital Gardens easily.
12. **TheDew - The Planet Earth Society:** Blaine Garst  
URL: <https://fosdem.org/2022/schedule/event/bgarst/> We solve Identity out of the gate on a new decentralized software platform called TheDew (in Alpha). Coded in a multicore Actor typesafe language with no strings, loops, or locks, it offers a Xanadu-esque collaboration sharing at its core. Coders own their code, always.
13. **The DID Directory:** Joe Andrieu  
URL: <http://diddirectory.com> The DID Directory is the easiest way to search, review, and learn about existing DID Methods. It combines the DID Methods registered in the W3C DID Spec Registries with simple landing pages, directly under control of the same party that controls the W3C Spec Registry Entry.
14. **cheqd:** Ankur Banerjee, CTO/co-founder at cheqd  
URL: not live yet, will be closer to the date / Check out issuance and holding of verifiable credentials on cheqd's DID network, combined with decentralized public-permissionless governance
15. **Hello:** Dick Hardt  
URL: <https://hello.coop> & <https://hello.dev> Hellō gives users control over their identity and choice of providers, while simplifying user registration and login for app developers, providing all the choices users may want in hours instead of days or weeks. Hellō is an OpenID Connect provider that operates between developers and existing IdPs.
16. **Interoperable presentation of VCs between Ping Identity, Microsoft and Workday:** Gabriel Bauman, Jeremie Miller, Daniel McGrogan, Kristina Yasuda  
URL: **coming soon** Come and see how users can choose wallets provided by Microsoft or Workday to present Verifiable Credentials to a verifier provided by Ping Identity, Microsoft or Workday!

17. Indicio - Cardea: Mike Ebert

URL: <https://cardea.app/> Cardea uses verifiable credentials and machine-readable governance to offer health and travel workflows. Come and see a demo based on SITA's trial in Aruba and the Cardea open-source code base. Digital COVID-19 test results are vital for safe global air travel.

18. Worldcoin: "W"

URL: <https://worldcoin.org/> Worldcoin Proof of Personhood SDK

19. Umazi: Cindy van Niekerk

URL: [umazi.io](https://umazi.io) Umazi is an enterprise digital identity platform enabling all businesses to share verified corporate identity data securely using self-sovereign identity (SSI) technology.



**Mahesh Balan** @maheshbalan · Apr 27

Had great fun at the demo hour in #IIW at the @ComputerHistory museum today! Thanks for the turnout folks.

- <https://github.com/WebOfTrust/keri>, <https://github.com/WebOfTrust/keripy>, <https://github.com/WebOfTrust/keep> The Keep is an Electron desktop application with a interface and embedded cloud agent and wallet deployed with tasks for all participants in ecosystem for creating identifiers, making connections and issuing, holding and verifying
4. **HTTP Signatures and GNAP Interoperability Testing:** Justin Richer  
URL: <https://httpsig.org/> <https://gnap-c.herokuapp.com/> HTTP Message Grant Negotiation and Authorization Protocol (GNAP) are two new security efforts currently in the IETF to provide practical and functional security improvements on systems. We're the playground for HTTP Message Signatures, where you can sign and verify arbitrary as the XYZ implementation of GNAP, available as a hosted service for interoperability
  5. **Pravici PocketCred:** Mahesh Balan  
URL: <https://www.pocketcred.com/> Pravici PocketCred is a platform that allows issuance and verification of Verifiable Credentials. These credentials can be used in as education transcripts, health records (such as proof of vaccinations). Pravici Po Salesforce HealthCloud.
  6. **BOTLabs GmbH presenting DIDSign:** Antonio Antonino, blockchain engineer  
URL: DIDSign available at <https://didsign.io/>. <https://medium.com/kilt-didsign-a-new-application-built-on-kilt-e4896fffb44> DIDSign provides a br

linkedin.com

Mahesh Balan on LinkedIn: #SSI #verifiablecredentials #IIW

Had great fun showcasing PocketCred #SSI and #verifiablecredentials capabilities at #IIW (internet identity workshop) in the Computer ...



## Diversity and Inclusion Scholarships



**DIVERSITY & INCLUSION**  
SPONSORED BY



### Thank You to Our Diversity & Inclusion Scholarship Sponsor [SpruceID](#)

Through this sponsorship we offered both complimentary tickets and travel reimbursement to 8 new attendees to IIW.

From our sponsor:

*We care about increasing support for women, black, and other starkly underrepresented technologists in our ecosystem. We can't build identity for everyone when demographics are homogeneous.*

*We are also interested in increasing participation from people that represent developing economies, as a counterpoint to the sweeping claims some SSI companies make about the technology's potential while their actual connections to those communities are limited.*

We would also like to thank [Women in Identity](#) @WomeninID who helped get the word out and increased our reach in terms of possible recipients.





## Kim Cameron - The 7 Laws of Identity



Gary Rowe @garyrowe · Apr 26

Thanks to Doc Searls @windley and @IdentityWoman for including this tribute to Kim Cameron at #IIW. Not forgotten.



linkedin.com

Gary Rowe on LinkedIn: #IIW

Thanks to Doc Searls Phil Windley and Kaliya IdentityWoman Young for including this tribute to Kim Cameron at #IIW. Not forgotten....



Leah Houston MD @LeahHoustonMD · Apr 28

@dsearls & @drummondreed sharing the 7 Laws of Identity in memory of the late & great @Kim\_Cameron a founding participant of #IIW and founding contributor to the standards and protocols that currently govern internet identity #InternetIdentity #DecentralizedIdentity



## Stay Connected with the Community Over Time - Blog Posts from Community Members

### New Community Resource

Each week Kaliya, Identity Woman and Informiner publish a round of the week's news from the industry. It is called **Identosphere - Sovereign Identity Updates (weekly newsletter)**

You can find it here: <https://newsletter.identosphere.net/>

As a follow up to the session 'Let's Bring Blogging Back' an IIW Blog aggregator has been created here: <https://identosphere.net>

If you want your blog to be included please email Kaliya: [kaliya@identitywoman.net](mailto:kaliya@identitywoman.net)

A BlogPod was created at IIW - Link to IIW Slack -

<https://iiw.slack.com/archives/C013KKU7ZA4>

If you have trouble getting in, email [Kaliya@identitywoman.net](mailto:kaliya@identitywoman.net) with BlogPod in the Subject.

**Planet Identity Revived** ~ @identitywoman & @InfoMiner cleared out & updated Planet Identity (see links below) you can support the work here:

<https://www.patreon.com/user?u=35769676>

IIW Community Personal Blog's shared via: <https://identosphere.net/blogcatcher/>

IIW Community dot.org's in the IIW Space: <https://identosphere.net/blogcatcher/orgsfeed/>



Hope to See you November 15, 16 and 17, 2022

## IIWXXXV / The 35<sup>th</sup> Internet Identity Workshop

### REGISTRATION OPEN



Internet ID Workshop @idworkshop · Apr 28

Many thanks to all the Sponsors of #IIW34 IIWXXXIV We appreciate you!  
#IIW



Heidi Nobantu Saul 🐛🦋 @nobantu · Apr 28

And it's a wrap!! First in person #IIW in over 2 years ~ a lot of work and so much fun. Hope to see everyone again in November for IIWXXXV ~



[www.InternetIdentityWorkshop.com](http://www.InternetIdentityWorkshop.com)