



BOOK OF PROCEEDINGS



#DICEurope
June 18 - 20, 2024
Zurich Switzerland

www.diceurope.org

Thank You to our Documentation Center/Book of Proceedings Sponsors: esatus and Validated ID

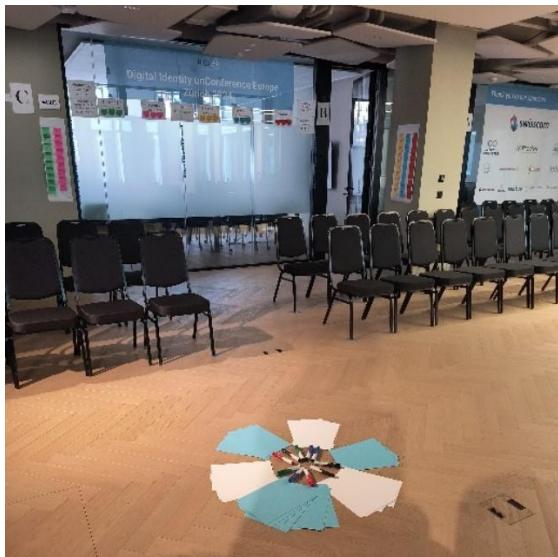


Contents

Thank You to our Documentation Center/Book of Proceedings Sponsors: esatus and Validated ID	1
About the Digital Identity OpenSpace unConference Europe	4
Thank You to our Sponsors!.....	6
Daily Schedule	7
DICE Pre-unConference Day 0 Schedule w/links to Presentations	9
Agenda Creation = Sessions Called and Hosted by Attendees.....	10
Wednesday June 19, 2024 ~ Day 1 / Sessions 1 - 5.....	10
Thursday June 20, 2024 ~ Day 2 / Sessions 6 - 10	12
Session Notes Day 1 / Wednesday June 19/ Sessions 1 - 5	15
SESSION #1	15
Designing Self-sustaining B2B identity ecosystem	15
Payment Rails in Open Ecosystems - How Verifiers pay Issuers	17
Swiss E-ID Tech Roadmap	18
KERI Fundamental Introduction	19
SSI Love AI agents	21
Trust DID Web - A new web-based DID Method	23
Education → Learning	28
ZKPs - From BBS To X.509	30
QWACS @ CH (Qualified Web Authentication certificates of the EU Eidas).....	31
SESSION #2	32
Decentralized Storage	32
Organisational Identity	33
eIDAS + Swiss E-ID Public Sector Cross Pollination.....	36
Multi Stacks & Multi Formats on Wallets.....	37
SSI-based B2B ecosystem.....	37
German eIDAS Wallet Consultation Project	39
Decentralized Interoperable Trust Registries	41
Paper Based Credentials - Do we need them? Why? How? For how long	45
SESSION #3	46
Ethereum Attestation Services (EAS)	46
VC Appearance e-ID with OCA	47

Health SSI.....	48
Security Issues Architecture Zero-Trust ARF 1.4 EUID + KERI - Security Models based on Root-of-Trust Type	49
Tell me about your identifier! Identification Traits.....	52
NAO - Now Networked Adaptive Organisms.....	53
OpenID4VC Updates, AMA	55
SESSION #4	56
User Centric - What does it mean?.....	56
From Identity to Reputation	57
Pros & Cons of UNIQUE IDENTIFIERS	59
Join the TolP Fun.....	61
Open Wallet Foundation - SIG's, Intention, SDK's, Wallets, Profiles	62
Thinking Outside the Wallet - A blueprint for Universal Zero Trust	62
Birth Certificates 2.0 aka Foundational Identity.....	63
IETF Token Status List	71
The Missing Principle of SSI: “Trust must be earned”	72
SESSION #5	74
Zooko and Houdini - a parable and why it matters to all of us	74
Session Title: The User Acceptance of the European digital Identity Wallet	75
Accessibility - How to Design for All	78
Joint session: Company Passport & Small Scale Pilots / What if websites were verifiable?..	79
vLEI KERI eIDAS 2.0 European Banking Authority (EBA)	80
Collating Requirements for a VCaaS (Picking your provider or frame your offering).....	81
Revocations / Status Comparison	82
Credential Schema & Layout Standards.....	84
Session Notes Day 2 / Thursday June 20 / Sessions 6 - 10	87
SESSION #6	87
Ask Me Anything about U.S. Department of Homeland Security (DHS) Digital Credential Infrastructure	87
Sovereign Data beyond VC	91
Wallet Attestations in context of eIDAS 2	93
Verifiable Government	94
LexDAO x DeSci = JoLE -> Journal of Legal Engineering - feat. decentralized peer review - > call for papers on identity & privacy	95
Legal identity, proof of identity and responsibility to protect	96
Creating B2B ecosystem (Open Discussion)	103
SESSION #7	105
Looking for Issuers Verifiers on ‘Swiss’ trust Infrastructure	105
Challenges in Designing Alonecasting Ecosystem	107
Duplicity Evident	107
The role of Qualified Trust Service Providers under eIDAS 2.0 - EU Regulation 2024/1183	108
Privacy and Unlinkability with and without ZKPs.....	110
Dreams and Nightmares: Real Talk combined with Beyond Statist ID	110
OPEN ID Federation	114
SESSION #8	115
Self-Sovereign did:web	115
Trust Statement Standardisation.....	115
ge-Scale KERI Network Design	116
Consensus Building	117

AMA - Holochain = a free, open-source framework for building peer-to-peer applications. / Matthew Schutte	118
VC-Catalog for non-public vc	118
OID4VC - Advanced Topics	119
Discussion on Binding Users, Holders, Subjects	119
Identity, Social Media & Democracy	121
SESSION #9	123
Funding Community Organizations & Community Work/Leadership, a discussion about what is working & challenges	123
Build your decentralized identity use case in less than 1 hour!	128
Legal Person (wallets) what makes them different & lessons learned.	129
Beyond the Issuer-Holder-Verifier-Model - Collecting use cases	129
Permissioned Smart Contracts.....	131
Use cases vs Business Cases.....	132
Potential Interop OiD4VCi (track 2)	133
SD-JWT VCDM	133
Let's make something fun with / about SSI - in sports, inbusiness, in family	134
SESSION #10	136
Go To Market Strategies for Wallet Ecosystems	136
ZKP Growth 16 Alternatives to BBS Signatures / Dima.....	139
How can we harmonize the user experience of consent and what is needed there?	139
Credhub - a cloud wallet at open wallet foundation.....	141
But Should We?	141
Identity for Universal Private Compute	142
What is missing? Looking forward from ARF 1.4	143
Attendee Posts about #DICEurope 2024.....	144
Link to Photo Library from DICE 2024	154
Digital Identity unConfernce Europe #DICEurope 2025	154
Follow DICE and Trust Square on LinkedIn.....	154
DICE 2025.....	154
Upcoming IIW and IIW Inspired Events	155



About the Digital Identity OpenSpace unConference Europe

The goal of the event is to foster collaboration on Digital Identity between governments, citizens, and companies across Europe.

OpenSpace unConferences are particularly generative, with a facilitator we will co-create the agenda live each day of the event. There are no keynotes or panels, it's all about exploring the topic with professional peers from a range of identity areas.

Digital Identity is a keystone for a digital society and economy.

- Who are the people?
- What are the Organizations?
- Where are the things (products, commodities, shipping pallets) and where did they come from?

There are many reasons that secure identity systems are needed for connecting to others, tracking trade, supporting labor markets, crossing borders. Significant investments have been made into the development of interoperable standards, protocols, systems application layers, conceptual use cases, and more.

Who is this Event for?

This event is for individuals, practitioners, researchers, regulators, implementers, government leaders, technologists, and digital and privacy rights activists. A neutral event where people from a range of different standards, efforts, and businesses can come together, learn from each other, build connections and move the work forward.

- Anyone who is implementing digital identity technologies, in government, enterprise, and civil society.
- Startups working on emerging digital and decentralized identity technology
- Enterprises that are exploring digital and decentralized identity technology
- Ecosystems of interoperability are a key emerging topic and companies cultivating networks of interoperability are encouraged to attend.
- Government leaders who are regulating digital identity and seeking to understand digital identity technology choices
- Those new to the concepts of Decentralized Identity and want to learn what it is all about
- Consumers of Self-Sovereign Identity (SSI) products and services

Event Background

The Digital Identity unConference Europe is Inspired by IIW™ the Internet Identity Workshop. The two facilitators and producer of IIW, Kaliya Young, Identity Woman and Heidi Nobantu Saul partnered with Danny Gasteiger & Andreas Freitag and collaborated with local Zurich partner Trust Square (Mark Degan and his fabulous Team) to host and produce the event.

The time is right to host an event for the European region with the same OpenSpace unConference format that the Internet Identity Workshop uses. DICE will bring together

business decision-makers, innovative startups, bold large companies, and governments, who are exploring the value of digital identity, building products, and developing services using emerging digital identity technologies. One of the goals of the event is to foster a more connected ecosystem of companies working in European Countries.

How an Open Space unConference Works

This is a participatory event and we will co-create the agenda together live each day of the event. There are no keynotes or panels, it's all about exploring the agenda topics with professional peers from a range of identity areas. All sessions are breakouts, and the topics are chosen and led by participants.

Through dozens of sessions, lunches & welcome reception and evening meal **Provided by our Generous Sponsors** (all included in the ticket) participants have plenty of chances to exchange ideas and make new professional connections. The OpenSpace unConference format is perfect for a rapidly moving field where the organizing team cannot predetermine what needs to be discussed.

We do know great people who will be there and it is the attendees and their passion for learning and contributing to the field of Digital and Decentralized Identity that all combine creating a successful event.

Read about [how to prepare for an unConference here](#).

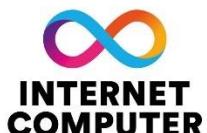
Read more [about Open Space here](#).



Thank You to our Sponsors!

The second iteration of Digital Identity unConference Europe would not be possible without the Sponsors who stepped up to make this gathering feasible.

Thank you to our sponsors



Validated ID @ValidatedID · Jun 21

This week, our colleagues Albert and Bernat from our #VIDentity team represented Validated ID at the #DigitalIdentity unConference Europe #DICE2024 in #Zurich! 🎉

...



Daily Schedule

DICE 3 Day Schedule

Tuesday June 18 / Pre unConference Day Brought to You by swisscom!

Start and Welcome to the DICE Pre-Conference Day at **9:00**
Trust Square ~ Bahnhofstrasse 75, 8001 Zurich / 3rd Floor

Registration / Coffee Official Welcome & Welcome by Swiss Government - Beat Jans Panel/ Digital Identity and Switzerland's Road to the Digital Economy Speaker/ Digital Identity - Why it is so important for a trusted digital society to close this last mile.	8:00- 9:15 9:15- 9:40 9:40- 10:15 10:15- 10:35	From ARF to Large Scale Pilots: Understanding the Full Scope of eIDAS 2.0 DHS Decentralized Identity Requirements - Choices Made & Work to be Done SSI Business Models	13:30- 14:00 14:00 - 14:30 14:30 - 15:00
COFFEE BREAK Journey in the EU Digital Identity Wallet Landscape: Pioneering Digital Travel Credentials The global protocol challenge and the art of timing Verifiable Credentials, Meet Smart Contracts LUNCH BREAK - Lunch Provided!	10:35 - 11:00 11:00 - 11:20 11:20 - 11:40 11:40 - 12:00 12:00 - 13:30	COFFEE BREAK Trust in a digital world Government Panel Closing Pre-Conference Day / Transition to Day 2	15:00 - 15:30 15:30 - 16:00 16:00 - 17:00 17:00 - 17:15

DICE Welcome Reception - 17:30 til late @ Bärengasse 16 (5min Walk)
Sponsored by - swisscom

Open Space unConference Day 1 - Wednesday June 19 / Doors Open at 8:00 Coffee/Tea & Breakfast Snacks			
Welcome & Introductions	9:00 - 9:30	Session 3	13:30 - 14:30
Opening Circle / Agenda Creation	9:30 - 10:30	Session 4	14:30 - 15:30

Session 1	10:30 - 11:30		Session 5	15:30 - 16:30
Session 2	11:30 - 12:30		Closing Circle	16:30 - 17:30
Lunch Sponsored by - SICPA	12:30 - 13:30		Conference Dinner	18:00 - 20:30
DICE Conference Dinner for all Attendees Sponsored by DFINITY @ Bärengasse 16 (5min Walk)				

Open Space unConference Day 2 - Thursday June 20 / Doors Open at 8:00 Coffee/Tea & Breakfast Snacks			
Women's Breakfast Sponsored by KOSMA CONNECT	8:00 - 9:00	Lunch Sponsored by SICPA	12:30 - 13:30
Opening Circle / Agenda Creation	9:00 - 9:30	Session 9	13:30 - 14:30
Session 6	9:30 -10:30	Session 10	14:30 - 15:30
Session 7	10:30 - 11:30	Closing Circle	15:30 - 16:30
Session 8	11:30 - 12:30		
No Host Post Event Gathering / Suggested Location to be Announced			



DICE Pre-unConference Day 0 Schedule w/links to Presentations

Registration 8:00 - 9:15 Trust Square ~ Bahnhofstrasse 75, 8001 Zurich / 3rd Floor			
09:15	09:25	Welcome to DICE	
09:25	09:40	Welcome by Federal Councillor Beat Jans Link to Speech Text Head of the Suisse Federal Department of Justice and Police FDJP	
09:40	10:15	PANEL / Digital Identity & Switzerland's Road to the Digital Economy Moderator: Daniel Saeuberli	Collaboration between DoJ / DIDAS and Swisscom Chief Digital Officer (Isa)
10:15	10:35	Digital identity - Why it is so important for a trusted digital society to close this last mile	Andreas Tölke Link to Presentation Deck Head of Fintech & Digital Trust at Swisscom
10:35	11:00	Coffee Break	
11:00	11:20	Journey in the EU Digital Identity Wallet Landscape: Pioneering Digital Travel Credentials	Xavier Vila / Technical Product Lead SICPA Matteo Marangoni / Senior Software Engineer SICPA Link to Presentation Deck
11:20	11:40	The global protocol challenge and the art of timing	Andreas Freitag / Co-CEO Procivis Link to Presentation Deck
11:40	12:00	Verifiable Credentials, Meet Smart Contracts	Jan Camenisch / CTO & Cryptographer DFINITY Link to Presentation Deck
12:00	13:30	Lunch Break / 1.5 Hours A Light Lunch is Provided	
13:30	14:00	From ARF to Large Scale Pilots: Understanding the Full Scope of eIDAS 2.0	Franziska Granc / Nimbus Technologie Beratung Link to Presentation Deck
14:00	14:30	DHS Decentralized Identity Requirements - Choices Made & Work to be Done	Anil John / Department of Homeland Security Link to Presentation Deck
14:30	15:00	CONVERSATION / SSI Business Models Moderator: Tim Weingärtner Link to Presentation Deck	Franziska Füglstaler / Cardossier Thomas Wüthrich / Biznet
15:00	15:30	Coffee Break	
15:30	16:00	Trust in a Digital World	Roman Zoun / Swisscom Link to Presentation Deck
16:00	17:00	Government Panel Moderator: Tim Weingärtner	Alexandra Hacklin / Finland Rolf Rauschenbach / Switzerland Paolo de Rosa / European Commission Anil John / USA - Dept. of Homeland Security
17:00		Closing Pre-Conference Day Transition to Day 2	Daniel Saeuberli Kaliya (IdentityWoman) Young & Heidi Nobantu Saul
DICE Welcome Reception 17:30 til late @ Bärengasse 16 (5min Walk) Sponsored by - swisscom			

Agenda Creation = Sessions Called and Hosted by Attendees



80 distinct sessions were called and held over 2 Days.

We received notes, slide decks, links to presentations and photos of whiteboard work 70 of these sessions.

Wednesday June 19, 2024 - Day 1 / Sessions 1 - 5

Session 1

- 1A/ Designing Self-Sustaining B2B Identity Ecosystem (innopay) / Beau
- 1B/ Payment Rails for Open Ecosystem of IDP / Sebastian + Dyma
- 1C/ Swiss E-ID Tech - Roadmap / Andreas
- 1D/ KERI Fundamental Introduction / Henk Van Cann
- 1E/ SSI + AI Agents / Volodymyr Parlyshym
- 1F/ Trust DID Web - A new web-based DID Method / Stephen Curran
- 1G/ Education - How to educate the public on SSI - dig. Identity / Tim W
- 1H/ ZKPs - From BBS To X.509 / Johannes Sedlineir
- 1I/ QWACS @ CH (Qualified Web Authentication certificates of the EU Eidas) / Imad Aad
- 1J/ NO SESSION

Session 2

- 2A/ Data & Metadata Storage Concerns P2P Privacy / Dr. MAFA Vero Estrada Galinanes
- 2B/ NO SESSION
- 2C/ NO SESSION
- 2D/ Organizational Identity (KERI) / Timothy Ruff
- 2E/ eIDAS + Swiss E-ID Public Sector Cross Pollination / Kai Wagner & Jan Carlos Janke

- 2F/ Multi Stacks & Multi Formats on Wallets / Bryan
2G/ SSI / Wallets in Business Identity (B2B) / Jeroen (Innopay)
2H/ German eIDAS Wallet Project * Funke Wallet Challenge *Discussion on Signed Data and Reputation / Paul + Torsten L
2I/ Decentralized Interoperable Trust Registries / Isaac Henderson
2J/ Paper Based Credentials - Do we need them? Why? How? For how long? / Hgath Taylor

Session 3

- 3A/ EAS Ethercom Attestation Service / Grace R
3B/ VC Appearance eID with OCA / Michel
3C/ Digital Health with Self Sovereign Identity / Peter
3D/ Security Issues Architecture Zero-Trust ARF 1.4 EUID + KERI - Security Models based on Root-of-Trust Type / Sam Smith
3E/ Tell me about your identifier! Identification Traits / JC - Jan Christoph E
3F/ NAO Now Networked Adaptive Organisms / Charles
3G/ NO SESSION
3H/ Open Discussion on the Missing Pieces of OIDGVC / Merul - Auvo Digital
3I/ NO SESSION
3J/ NO SESSION

Session 4

- 4A/ USER - CENTRIC What does it mean? / Dr.MFA Vero Estrada G
4C/ From ID to Reputation / Ekhard S
4D/ Pros & Cons of UNIQUE IDENTIFIERS / Laurant
4E/ Trust over IP Foundation (ToIP) Introduction & Update / Judith Fleenor
4F/ Open Wallet Foundation - SIG's, Intention, SDK's, Wallets, Profiles / Mirko
4G/ Thinking Outside the Wallet - Blueprint for Universal ZEROTrust Interoperability / Manu Fountaine
4H/ Birth Registration 2.0 aka Foundational Identity / Stephan
4I/ OAuth Token Status List / Christian + Paul
4J/ The Missing Principle of SSI: Trust Must be Earned! / Mike
4K/ NO SESSION

Session 5

- 5A/ NO SESSION
5B/ Zooko and Houdini - a parable and why it matters to all of us / Daniel Hardman
5C/ User Acceptance of the European Identity Wallet / Adrian Doerk
5D/ Accessibility - How to design for All / Luana V & Raman Z
5E/ What if websites were verifiable? Linked-up spec / Jan Christoph E
5F/ vLEI KERI eIDAS 2.0 European Banking Authority (EBA) / Christoph Schneider (Gleif)
5G/ Collate Requirements for a VCaas - How to pick your service or frame your offer / Dominik Geller,
5H/ Revocations / Status Comparison / Mirke
5I/ Cred. Schema & Layout Standards / Sven
5J/ NO SESSION

Thursday June 20. 2024 ~ Day 2 / Sessions 6 - 10

Session 6

- 6A/ DHS (US) Decent ID Tech Requests - AMA / Anil John
- 6B/ Sovereign Data beyond VC / Volodymyr P
- 6C/ Wallet Attestations / Paul B
- 6D/ Verifiable Government - A new model for Digital Government that's inclusive, secure, and privacy preserving / Timothy Ruff
- 6E/ LEXDAU x DESEIER = JoLE Journal of Legal Engineering Decentralized Peer Review / Charlie
- 6F/ Legal Identity - Proof of Identity - digital ID - Blockchain for Human Rights / Gabriela
- 6G/ Creating B2B Ecosystem / Beau & Douwe
- 6H/ NO SESSION
- 6I/ NO SESSION
- 6J/ NO SESSION

Session 7

- 7A/ Looking for Issuers Verifiers on 'Swiss' trust Infra. / Rolf R
- 7B/ Challenges in Designing Alonecasting Ecosystem / Stefan T.
- 7C/ NO SESSION
- 7D/ KERI: Duplicity Evident Data: How verifiers are protected from impostaers w/o blockchain or Trusted Third Parties / Sam Smith
- 7E/ The role of Qualified trust service providers in eldAS2 / Jorg + Adrian + Stephan Privacy and un Linkability with and without ZKP's / Stephen Curran BC Gov
- 7F/ Beyond "statist" ID = Exploring how SSI & related tech can be leveraged for change at community & a better planetary future & Dreams and Nightmares Real Talk / Kaliya and Matthew Schutte
- 7G/ OPEN ID Federation / Marten en Timo
- 7H/ NO SESSION
- 7I/ NO SESSION

Session 8

- 8A/ Self - Sovereign did:web / Jan Christian
- 8B/ Trust Statement Standardization / Michel
- 8C/ NO SESSION
- 8D/ Large-Scale KERI Network Design / Martin B
- 8E/ ToIP Main Glossary + Spec-Up / Drummond Reed & Hank Van Cann
- 8F/ AMA - Holochain = a free, open-source framework for building peer-to-peer applications. / Matthew Schutte
- 8G/ VC Catalog for NON-PUBLIC Credentials / Piet and Roman
- 8H/ OID4VC - Advanced Topics / Oliver T and Paul and Christian
- 8I/ Discussion on Binding Users, Holders, Subjects / Peter Langenkamp
- 8J/ Identity, Social Media & Democracy / Yuting

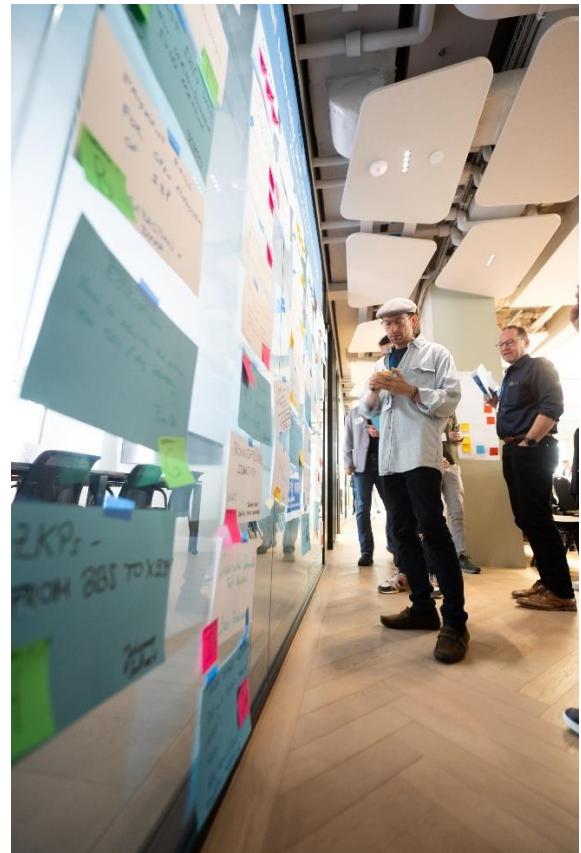
Session 9

- 9A/ Finding Community Organizations & Community Work/Leadership - a discussion about what is working and challenges / Kaliya
- 9B/ Build you decentralized identity use case in less than 1 hour! / Kai, Marco and Robin
- 9C/ Legal Person (wallets) what makes them different & lessons learned. / Maarten

- 9D/ Beyond the I-H-V model! (collecting use cases) / Sebastian Z
- 9E/ Permissioned Smart Contracts / Titus (civic)
- 9F/ Finding the right tools, use cases vs business cases / Marul
- 9G/ Potential Interop OiD4VCi (track 2) / JH & Linas (meeco)
- 9H/ SD-JWT VCDM / Oliver
- 9I/ Let's make something fun with / about SSI - in sports, in business, in family / Thomas W
- 9J/ NO SESSION

Session 10

- 10A/ Go to Market Strategies for Wallet Ecosystems / Adrian
- 10B/ ZKP Growth 16 Alternatives to BBS Signatures / Dima
- 10C/ How can we harmonize the user experience of consent - (to Tos, privacy policy, etc...)? / Kai + Marko
- 10D/ Cred hub cloud wallet by Open wallet Foundation / Mirco
- 10E/ But Should We....? Grace R
- 10F/ Identity for Universal Private Compute when Private Data Meets Verified Code / Manu F
- 10G/ NO SESSION
- 10H/ What are we still missing? Looking forward from ARF 1.6 / Christian
- 10I/ NO SESSION
- 10J/ NO SESSION



OpenSpace unConference

Session Notes/ Documenting Your Discussions

We collect Notes from all of the sessions convened to be shared openly and importantly with other attendees who were unable to attend the session because they were participating in a different session happening at the same time. After the unConference Notes are compiled into a Book of Proceedings that includes all Session Notes, photos and information about the event. It is made available to everyone several weeks after the workshop.

Please follow the process below

Session Convener:

- Before you begin, please identify 1 -2 people to take notes for the session.
- OR write up a brief summary of your session after the session is complete

In Qiyo Online Collaboration Space
(Use the private link you were emailed to access the platform)

Session Note Taker(s): (Anyone in the session is welcome to add notes)

1. Go to the Day 1 or 2 Agenda Button or Tab you will see the Agenda Wall Grid for that Day
2. Scroll down to find your Session # (1-5 or 6-10) and the Breakout Space you are in (A - G) The Session Title may or may not be filled in yet on the Grid.
3. Click on the 'Access Notes Form' link that corresponds to the Session # (1-5 or 6-10) and your Breakout Space (A-G) for which you are taking notes. It will take you to a GoogleDoc specifically set for this session # and Breakout Space.
4. In the GoogleDoc Form Fill-in:
 - Session Title
 - Name of Convener(s)
 - Name of Notetaker(s)
 - Optional - Names of Attendees
 - Type notes directly into the form or if you've taken hand written notes transcribe them later. Include links to slide decks or resources, photos of whiteboard work etc...

Session Notes Day 1 / Wednesday June 19/ Sessions 1 - 5

SESSION #1

Designing Self-sustaining B2B identity ecosystem

Session Convener: Beau Schellekens (INNOPAY), Jeroen van der Hoeven (INNOPAY)

Session Notes Taker: Jeroen van der Hoeven (INNOPAY)

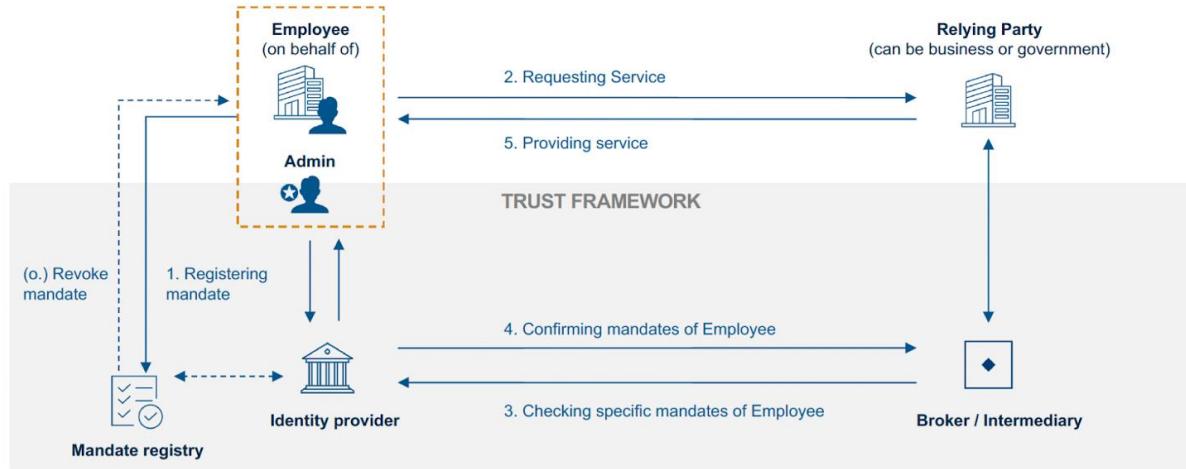
Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Session summary:

- Businesses are striving for trust and operational efficiency with B2B services. A considerable potential lies in solutions that facilitate authorised transactions of individuals on behalf of a company. Digital identity and how (natural) persons digitally identify and authenticate has gained substantial traction with the revision of the eIDAS regulation. How businesses and individuals acting on behalf of a business identify themselves in external interactions (B2B, B2G) is little explored.
- An eID solution for organisations (often referred to the organisational wallet under eIDAS 2.0) with mandate management functionality results in an efficient and standardised process. This process enables us to identify a person and to check what the person is allowed to do on behalf of the organisation.
- Both sides of the transaction benefit through time and cost reduction as well as risk mitigation.
- Established implementations of this, such as eHerkenning in the Netherlands, have been operational for several years.

Established mandate management systems are based on mandate registries as (de-)central place to store and check attributes

EXAMPLE FLOW SETTING UP AND CHECKING MANDATES WITH MANDATE REGISTRIES



NOTE: This is an indicative overview. There are several ways to depict the B2B digital identity ecosystem. Roles can be multiple and interoperable

DICE 2024 – Business Identity. June 2024 © INNOPAY BV. All rights reserved.

INNOPAY
A business of Oliver Wyman

Step-by-step workings of eHerkenning (sustainable business identity ecosystem):

1. The admin of a Business registers the business in the Trust Framework using a unique identifier, e.g. Chamber of Commerce number. The admin then receives admin credentials linked to the company.
2. Using the admin credentials, the admin grants specific rights (or authorisations) through mandates to employees, documenting these mandates in a Mandate Registry. The Mandate Registry functions as a comprehensive list of authorised services within the Trust Framework, detailing who is authorised to access which services on behalf of a given business. There can be multiple, decentralised Mandate Registries within a Trust Framework
3. After the employee of the business was successfully assigned a mandate in the mandate registry, the employee requests a service from the Relying Party, identifying with personal credentials
4. Based on the identification credentials of the employee, the Relying Party initiates the system's verification process to confirm whether the employee is authorised to act on behalf of the business for the requested services
5. The system returns if the individual to which the credential belongs, is authorised by the business to perform the specific service requested (on behalf of the business)
6. The Relying Party grants or denies access to the requested services, according to the obtained reply

Payment Rails in Open Ecosystems - How Verifiers pay Issuers

Session Convener: [Sebastian Rodriguez Cabrera](#) and [Dmytro Sukhiy](#)

Session Notes Taker: [Sebastian Rodriguez Cabrera](#)

(optional) List of Session Attendees:

David Z - Privado.id

Sebastian Rodriguez - Privado.id

Dymtro Sukhiy - Privado.id

Tania - W3 Trust Capital

Sebastian - Lissi

Kaliya - Identity Woman

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Discussion

Verifier sponsorship User verification - has challenge

90% cases user is paying - we should be talking about it.

Web3 space user is paying.

Mint NFT - generate SBTs

BigCo's (MetaApple etc) have taught users not to pay

90% of verifier is paying - subscriber is paying per batch.

Business model

Doctors in the US. Have an extreme using

In the UK Truu, Condatas

SSI is not the “business model” it is how we handle data - not a technical solution.

Cheqd - Revocation List charging

Velocity - viewing keys on credentials.

Swiss E-ID Tech Roadmap

Session Convener: Jonas Niestroj, Michel Sahli, Andreas F

Session Notes Taker: Lara Schwab

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Presentation & discussion of the [Swiss E-ID Tech Roadmap](#).

Identifiers

- central managed identifiers within the ecosystem by the gov → identifiers are a specification also others use
- are used for the issuer as a start, did:tdw is used (integrity is ensured)

Status Mechanisms

- Status list, which is well described, same which is used in the EU and currently also works for eLFA would be a solution to use → there is the challenge of linkability
- To ensure unlinkability the FOITT is also considering accumulators to try it out and get some experience there. The challenge is that it is not deeply described adequately and the DEV teams needs to run some POCs

Trust Protocol

- Ensures that the identifier is the identifier it claims to be (initially on issuer side, could be also enhanced to verifiers later on)
- Trust protocol will be selected based on the requirements which is currently minimal (what's written in the law)

Communication Protocol

- FOITT would like to go with the standard protocol. bad internet connection is a challenge which needs to be tackled (e.g. with asynchronous communication) we accumulate use cases, relevance, requirements about it

Payload Encryption

- Specs from the specification are used for an E2E encryption of the VC

VC Format/Signature Scheme Combination

- Scenario A: EU direction → SD-JWT, ECDSA/EdDSA → implemented already for the eLFA pilot
- Scenario B: Unlinkable direction → JSON-LD, BBS+ → incl. data integrity (since there is a hardware holder binding)

Holder Binding Scheme

- currently it is open it will be implemented
- LOA 3 (equivalent to eIDAS level substantial) is selected
- Holder Binding is only for high LOA VCs → VC's aren't backupable

VC appearance

- Session 3, Room B the topic will be tackled

Off Topic Questions / Parking Lot:

- Backup: E-ID is not backupable (holder binding), other VCs can be restored
- Issuing Process
- Verifier Identification → there will be a misuse list where ecosystem participants and citizens can report misuse
- Trust Interactions
- Asynchronous communication
- Federal wallet
 - next to the E-ID there can also be other VC be held
 - holder can also have E-IDs of the kids (delegation)
 - Combined proof (taking attributes from several VCs in one proof) is currently not in discussion for the initial solution

KERI Fundamental Introduction

Session Convener: Henk van Cann

Session Notes Taker: Merul Dhiman

(optional) List of Session Attendees:

Link to slides including presenter notes: [KERI-v2.1.0.pdf](#)

<https://drive.google.com/file/d/1r7LAPORgA3wBCdXQGdOYBD4H6DMHLXVH/view?usp=sharing>

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Notes are in markdown

Objectives of KERI

- Digitally sign things and allow people to verify them
- No shared infrastructure, no CA no Ledger no blockchain
- Enables a method of rotation and recovery, has a persistent identifier instead of having public key as an identifier

[Keri Introduction](<https://keri.one>)

> Session by: Henk van Cann

complex - unpredictable and unbound

complicated - predictable, difficult to grasp but can be bound

What is KERI (Key Event Receipt Infrastructure)

Intends to repair the internet:

- Don't need a middleman to prove who said what
- Internet is broken because we need CAs to tell us who is trust worthy and who is not
- A completely new internet where internet is a new property of communication

What does it look like

- Several key events are put on an event ledger

Why KERI

- Has strong autonomous identifiers
- No total global ordering (you do not need a global ordered ledger)
 - bypass blockchain
- Security First (Privacy comes later, SECURITY comes first)
 - Interoperably security to add semantics to later, if you can't secure the source of the data then you can't trust the data
 - SSI space focuses on the wrong problem, Interop of data instead of Interop of Security
- Scalable (no blockchain, KEL, Key Event Log, Personal Log, Can use agents, supports key delegation)
- Transfer of control is built in

Keri Suite

- KERI: Key Event Receipt Infrastructure
- ACDC: Authentic Chained Data Container
- CESR: Composable Event Streaming
- OOBI: OOB Introductions
- KERIA: KERI Agent in the cloud
- Signify: Web client to sign

Key Delegation

- Keri allows one entity to have as many key delegations as possible allowing for very scalable system where you can have as many keys

Why KERI is what it is

- Blockchain is limiting
- KERI is portable, move from any system to any system, from any blockchain to any blockchain

Use cases

- can use KERI now
- Implementaiton concept: [GLEIF](<https://gleif.org>)
- Healthkeri, company in europe working on cardiology
- Web of trust repo reference impl (in python)

KERI Concepts

- Doesn't need blockchain
- Direct & Indirect verification methods
- Duplicity detection and recovery
- Pre-rotation

Key differences which KERI Makes

Authentication: Who said what

Veracity: Was it true

Questions

[Kerisse](<https://kerisse.org>)

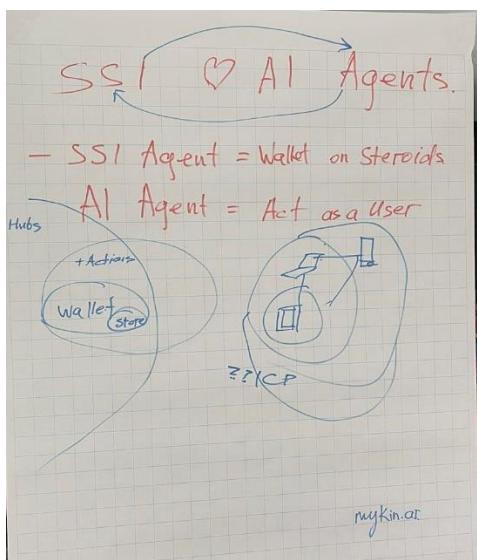
SSI Love AI agents

Session Convener: Volodymyr Pavlyshyn

Session Notes Taker: Volodymyr Pavlyshyn

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Volodymyr Works at mykin.ai privacy first, local first, personal ai empowered by SSI



Summary:

SSI agent = Wallet on steroid with actions available online

AI agents could take action on behalf

AI SSI agent = LLM + SSI agent with rules

<https://www.youtube.com/watch?v=mP9cbOibt5A> This is a full talk about why AI agents need a SSI data and sovereignty

<https://www.youtube.com/watch?v=AsdGc-E0Qns&t=4s> - This is a full talk about AI extended agent and how AI agents transform data

Key Ideas

- AI has a data hunger we need a way to create a space for users to share data with models is a fair way and build data economy relations
- AI looks for personal and soft data that require trust
- SSI systems could be empowered by SLM (small model) to automate credential generation and exchange
- We all need ownership and verifiability of data sources for fair AI model training

Topics

- SSI agent in the empowerment of SLM
- AI agents that use sovereign data
- Sovereign data is not VC and it is non vcfied data
- We need sovereign storage for structured data that allows to run queries
- How ICP could jump to a game
- The challenge of decentralized compute GPUs and AI

More to read : <https://medium.com/stackademic/ai-love-sovereign-data-9acce2141f11>

Data — AI Fuel

- Open data — public data is just a fraction of the data universe that struggles with quality, accuracy, and heavenly bias. Quite often, it is not present in person
- Quality data — quality and curated data sources quite often is out of public space and are in the ownership of closed companies or individuals. Recent research show that even much smaller models show significantly better result on quality and curated data sets
- personal — users are not comfortable sharing sensitive data even in exchange for personalized service
- closed data- the majority of modern data sets are closed by platforms and companies

Data Ownership

- Ownership is a key answer to the problem of closed and personal data. We need to create a secure and open space for user data to which users can access and consent to use their data for the good of all.

- - **web2** — Soviet Union-like state of data ownership. All produced data points and content are owned by the platform. User authorized to have access under control of platform
- **web3** — give ownership back for digital assets, but data stays locked in a network. The user wallet has no data, just keys. All data point is public and recorded in transactions or intelligent contracts
- **web5** — give privacy and selective sharing to ownership

AI use cases of SSI and WEB5

- learning on private data
- Authentic sensors — how to prove nongenerative content
- ZKML — proof of Model use
- data economy
- agents interaction

Personal AI use cases

- proof of personhood
- personalized experiences without risking privacy
- personal AI

Trust DID Web - A new web-based DID Method

Session Convener: [Stephen Curran](#)

Session Notes Taker: Jin Wen (copied and updated from IIW 38 proceedings)

(optional) List of Session Attendees: So many!!

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Summary: A new DID Method that builds on did:web that adds access to a verifiable history of the DID as the DIDDoc evolves, authorised keys for updating a DID, and the DID includes a self-certifying identifier (SCID) that enables movement of the DID to other DID locations when required or desired. The DID Method has relatively low complexity dependencies — nothing fancy!! Further, since HTTPS URLs are so easy to use, the DID Method makes it easy to translate DID URLs into HTTPS URLs for retrieving DID-related files. Special callout to <did>/whois, which is a DID Method URL that resolves to a Verifiable Presentation where the DID is the **credentialSubject** in the VCs in the Verifiable Presentation.

We also covered advanced features, such as publishing a parallel did:web DID, key pre-rotation support, what keys are “authorised” to update the DID,, multi-signature authorization handling, witnesses and watchers, the two implementations and more.

Session Presentation: [Trust DID Web - A New Web-Based DID Method](#)

Specification: <https://bcgov.github.io/trustdidweb>

Trust over IP Task Force Page:

<https://wiki.trustoverip.org/display/HOME/Trust+DID+Web+%28did%3Atdw%29+DID+Method+Task+Force>

TypeScript Implementation: <https://github.com/bcgov/trustdidweb-ts/>

Python Implementation: <https://github.com/bcgov/trustdidweb-py>

Rust Implementation: To Be Added

What is did:tdw

- similar to did:web, but with ledgerless, verifiable, authorized history
- instead of/beside did:web's did.json file, there is a did.jsonl file
 - JSON Lines (jsonl) – lines of JSON - jsonlines.org
 - Could publish both **did:tdw** and **did:web** DIDs - although use of only the **did:web** DID reduces the security model.
- Resolvers process and verify the log to retrieve the entire DIDDoc history
- All versions, chained, and signed by the DID controller
- A self-certifying identifier (SCID) enables uniqueness and portability
- Defined DID URL path handling:
 - <did>/path/to/file
 - <did>/whois
- Small/simple implementation with minimal dependencies

Who fund this: BC Gov

- Started with well-defined (but not obviously implemented) requirements
- Result - clear, simple and complete specification and 2 implementations.
- Builds on many years of listening to the challenges.

Mechanics

Each entry is a JSON array of 6 elements:

[entryHash, versionID, versionTime, parameters, DIDDoc, dataIntegrityProof]

parameters - configurations for entry processing

- examples - algorithms in use: did:tdw spec, hash, cryptosuite
- also contains the authorized keys to update the DID (**updateKeys**)
- As well, the hashes of the keys that will later be authorized to update the DID — the pre-rotation keys (**nextKeyHashes**).

Dependencies

- Hash — default to **sha256** but specification can add more schemes
- [Base32 Encoding](#)
- [JSON Canonicalization Scheme](#)
- [JSON-Patch](#) (used to define the transition from one DIDDoc to the next)

- [W3C Data Integrity](#)
- [did:key](#)
- [Multibase/multiformat](#)

Creation, Verification Process

How SCID is generated: from initial DIDDoc log entry (first 5 items of the log entry) with placeholders in place of SCID (literal string `{SCID}`). Calculation to get SCID and the replace the `{SCID}` strings with the generated SCID.

a did:tdw log is shown here

Log Entry: entryHash, versionId, versionTime, parameters, diddoc, proof



```
[{"yza4hoyihukpz5wxcag26clggwqbpsjv26zpp3kqc7gtusokvfpa", 1, "2024-06-18T19:25:55Z",
{"hash": "sha3-256", "prerotation": true, "updateKeys": [{"z82LkqR25TU88tztBEiFydNf4fUPn8oWBANckcmuqgonz9TAbK9a7WGQ5dm7jyqyRMpaRAe"}, {"nextKeyHashes": ["enkkrhe5ccxyc7zghic6qux5inyzthg2tqka4b57kvtrysc3aa"], "method": "did:tdw:1", "scid": "1kq33irvim6iktjkagnw2ee6bgcw"}, {"value": {"@context": [{"https://www.w3.org/ns/did/v1", "https://w3id.org/security/multikey/v1"}], "id": "did:tdw:domain.example:1kq33irvim6iktjkagnw2ee6bgcw"}}, {"type": "DataIntegrityProof", "cryptosuite": "ecdsa-jcs-2019", "verificationMethod": "did:key:z82LkqR25TU88tztBEiFydNf4fUPn8oWBANckcmuqgonz9TAbK9a7WGQ5dm7jyqyRMpaRAe#z82LkqR25TU88tztBEiFydNf4fUPn8oWBANckcmuqgonz9TAbK9a7WGQ5dm7jyqyRMpaRAe", "created": "2024-06-18T19:25:55Z", "proofPurpose": "authentication", "challenge": "yza4hoyihukpz5wxcag26clggwqbpsjv26zpp3kqc7gtusokvfpa", "proofValue": "zUDcd2Yjuzu8XLmZufkYY3Xm8VEZRWgwE9SoKFP83d1ZnKtEwGLf42KCm6nmr8YQVQ6ykusRSSaq8iJjiPa8axNpeTSR2ERjVDiMGf33np9ayVFopZjXYd92g7RYXmGhSSw"}]]
```

Interesting Topics

- parallel publishing with did:web
- publishing a did:tdw — perhaps using [did-web-server](#)
- DID URL Handling: Paths
- Witnesses and Watchers

Use cases

/whois

[Traversing the Web of Trust](#) from 2018 paper — realized!!

Link to [implicit service definitions](#) within the specification.

Key points in the transcript:

1. The goal is for a DID to provide a verifiable presentation linked to the DID subject and signed by the DID itself, accessible via a /whois click.
2. The simplicity of transforming a DID to an HTTP URL is emphasized, as it simplifies usage and is compatible with any DID method.
3. The project is funded by BCGov and achieved significant progress in about a month and a half, including two implementations and a full specification ready for feedback.
4. The implementation is concise, (less than 1600 lines of Python, same for TS), and the mechanics involve a DID to HTTP transformation similar to DID web but with an added 'L'.
5. The system uses a JSON array with six elements for each entry, which includes a version ID, version time, parameters item, and a data container group signed by an authorised user.
6. The parameters allow for the configuration of entry processing, including hash algorithms, crypto suites, and DID spec versions, allowing for evolution and advanced features like DID migration.
7. Dependencies for the system are minimal, including SHA-256, Base32 encoding, a JSON canonicalization scheme, JSON patch, and data integrity proofs.
8. The creation of data process involves inputs like the DID document and preset parameters, with requirements for an ID and an authentication key within the DID document.
9. The system uses a method called "scid" that replaces placeholders in the DID document and ensures data integrity through a chaining mechanism. Note: It does not use KERI directly due to dependency considerations, but it is inspired by KERI
10. The entry structure in the file is an array with a consistent format, and the system allows for changes in parameters to be made mid-stream.
11. There is some discussion about the choice of data structures and the proof mechanism, with a focus on simplicity and minimal dependencies.
12. The possibility of parallel publishing using DID:WEB is discussed, with considerations for verifiability and adoption.
13. The system defines two services, cache files??, and cache news??, which are included in the spec and can be used implicitly or explicitly added to the DID doc.
14. The system does not change how a key within the DID doc is referenced; it uses the same method as the DID core specification.

Additional discussions:

Moving DID's Web Location

- social network porting from A to B
- Bluesky related use case — it hosts DIDs. Wouldn't it be nice if you could decide to move your Bluesky-based DID to another platform, while retaining the entire DIDDoc history.

Next Steps:

- Look into where authorized public keys should be published.
- Move to standard bodies: ToIP and/or W3C.
 - Task Force has been formed at ToIP — join [us there](#).
 - What features being proposed here should be in the DID Core spec.
 - Could this be an evolution of did:web at W3C?
- Polishing the spec. and formally publishing it.
- More implementations beyond Typescript, Python, and Rust.
- Adding to Aries Cloud Agent Python, including for use in rooting AnonCreds VCs.
- A [did-web-server](#) implementation supporting did:tdw.

Education → Learning

Session Convener: Tim Weingaertner

Session Notes Taker: Tim Weingaertner

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

We changed the title to Learning, since Education has a push attitude.

First you have to decide “What people should learn about?”. This could be: benefits, risks, concerns, how to gain trust, why should you trust,

Next decide the “Why” or Vision. Choose the why regarding the user group.

Finally choose the “How”. Best try to get viral (video, discussion, ...) and use the ambassador principle:

- Young people teach their parents.
- Learn together.
- Students could make sessions for elderly people and gain credits or can use this in their CV.
- Facilitate peer learning
- Make info sessions in libraries.
- Build user groups, clubs, associations, ...
- Choose people or organisations you trust (banks, newspaper, tax advisors, teachers (bring it in the teachers curriculum)).

It is important that you address the pain points of the people and build concrete use cases.

These use cases could be:

- Library cards
- Loyalty cards
- Access to medicine (like in pharmacy)
- Access to documents (e.g. for lawyers)
- Give voting rights
- Anonymous social media

We also discussed that identity and SSI should not be used as terms since SSI is very technical and identity has for each person another meaning.

Better use: digital xxxx (something that already exists) like digital library card, digital passport, digital student card,

Notes:

Education learning

- What to educate about?

- Benefits / Concerns / risks
- Trust

Why : Vision

How: Video, Discussion → Viral

Young talk to parents

Link to Use Cases

show-don't tell addresses pain points

Libraries → Info session

ambassadors whom you trust
user groups, clubs, association
learn together

students do sessions for others

newspaper (fashion) bankers, tax advisors, school (P4)
Material: Examples library card, loyalty card
access to health
access to documents (lawyers)
give voting right
anonymous social media

not identity / SSI → digital XYZ

library card

LANDR FLIP-CHART-PAPIER • ART. 100050592

passport



ZKPs - From BBS To X.509

Session Convener: Johannes Sedlineir
Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Two Types of ZKPs available

- Special purpose ZKPs
- General purpose ZKPs
 - Usable to compute an arbitrary algorithm
 - Around 1,000,000 slower, improvement by 10 times a year

raw notes:

Initial discussion about the definition of ZKPs, proving something without revealing information that is not trivially available.

For Schnorr signatures: Mathematical trick that convinces you I have special knowledge.

2 Approaches:

- Special purpose ZKPs: New form where the credential is constructed in a way that allows an easy construction of a proof; Very fast & elegant, but struggle to integrate with legacy infrastructure
- General purpose ZKPs: Proof the correct execution of an algorithm; ZKVMs

Mental model for ZKVMs should be: Consider this an execution trace of the algorithm that decomposes the algorithm to additions and multiplications and allow the verifier to do some spot checks. The verifier often doesn't care about the public key or the signature, but about correctness of them. The game-change is that we can keep using the hardware and credential formats we already have, but we get the guarantee of da minimization by applying a ZKP on top.

Computation could be delegated to an untrusted verifier (blinded via cryptographic randomness).

A ZKP has private and public inputs - usually the public key of the issuer will be known to both, the holder and verifier.

Computation is slower by ~1million, but some factors like GPU support and parallelization can help mitigate. Currently there is a roughly an increase of 10x per year. Improvements are mainly because the algorithms are improving.

Quantum resistance: Best proving time & prove size of 250kb - Ligero / Ligetron -> ZKvm for WebAssembly and Risco are good options.

Proposal from Johannes: Keep using the current formats (x509 chain + sd-jwt or mdoc at the end) and the only thing that changes is the verification process. The ZKP would not change anything for the attributes you are explicitly revealing, but strips other parts of the credential like public key because the verifying happens at the holders side.

Computation penalty could go as low as an overhead of 10000x

LegoSnark as an option to use BBS signatures and are kind of an intermediate solution between general purpose ZKVMs, but they lose the hardware support

QWACS @ CH (Qualified Web Authentication certificates of the EU Eidas)

Session Convener: Imad Aad

Session Notes Taker: Imad Aad

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

(CA = Certificate Authority)

It makes sense that governments (like the EU) introduce their own trust schema, to become independent from the private sector, in terms of Trust.

It's not easy/straightforward to decide whether the private sector or states are more trustworthy, to take the CA role.

It is risky to reinvent the wheel, to replace the current trust schema that evolved during decades.

Nowadays the trust is based on (CAs + Browsers), not on any one separately. It makes sense to think of introducing a similar setup for the governments as well, where trust is not based on a government alone.

It remains unclear what will be the impact on Switzerland: will Swiss simply use browsers made for the EU, while the jurisdiction is different / does not apply, or continue adopting the trust schema of the private sector alone?

SESSION #2

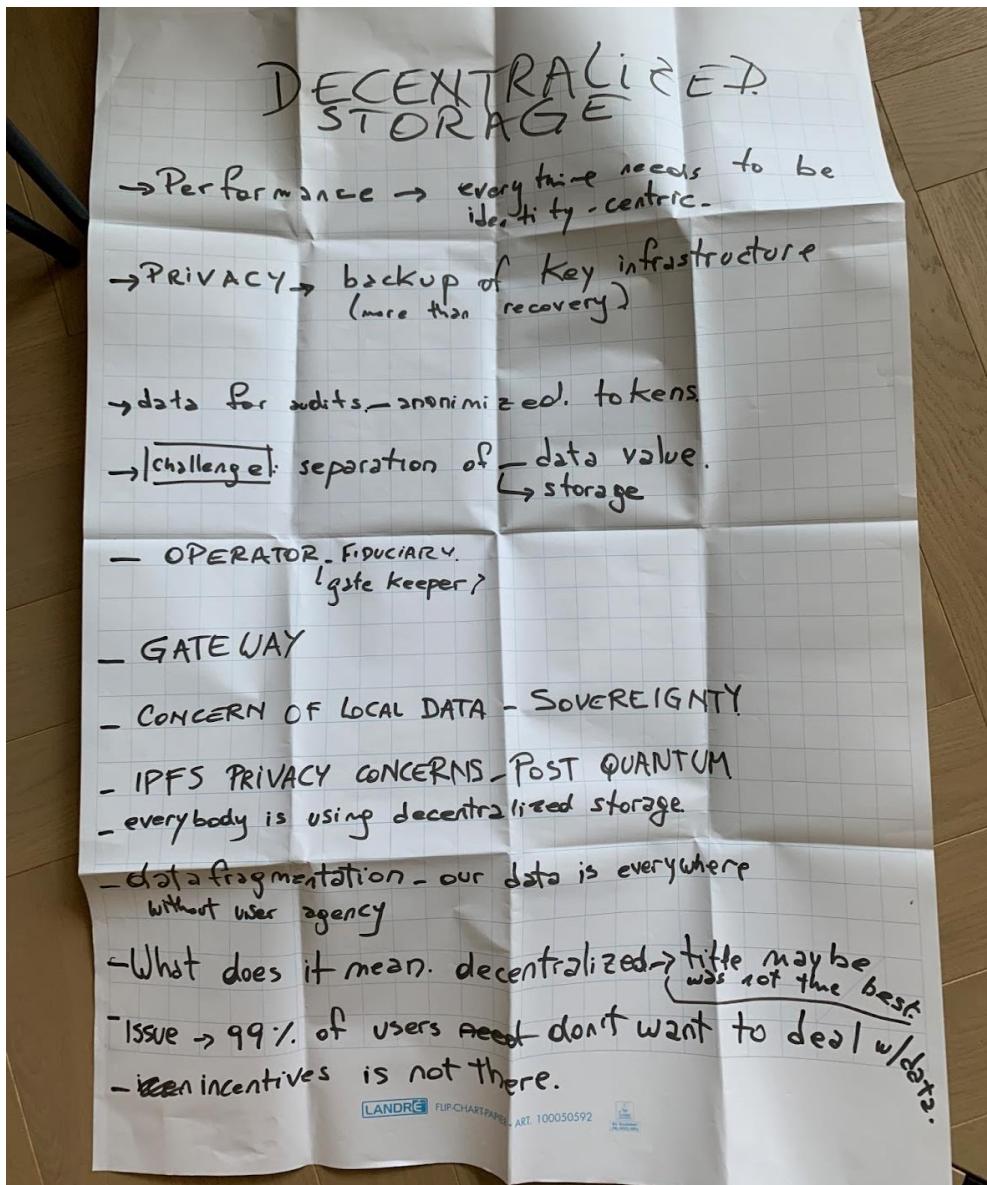
Decentralized Storage

Session Convener: Vero Estrada-Galiñanes

Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

I will write notes later. Meanwhile I include the poster pic (check next page).



Organisational Identity

Session Convener: Timothy Ruff

Session Notes Taker: Merul

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

> Session By: Timothy Ruff

link to presentation

https://docs.google.com/file/d/1aMX0JGptzJW-KLNn-ft51ArUq1uCTZn6/edit?usp=docslist_api&filetype=mspresentation

- There is no B2B ID
- Organizations don't act, people do
- When an org performs an action it's a delegate which does it

Examples

- Police officers prove they are one
- Bank rep proves they are from bank
- Signatures with verifiable authority
- Login based on presented authority instead of identity (pilot can fly a plane because they are rated and no that they are Bob or Joe)

Markets of ID

- IAM: \$15B
- SSI: ~\$100M
- OI: New global market between organizations

What is Organization Identity

- Identity of an organization
- Identity of a representative
- Authority of representative

Example of Organization Identifiers

- LEI (legal identity identifier) -> 20 Char String
- Local, regional and national identifiers
- Legal Name, Doing Business As
- Address

Representatives

- Types:
 - Employees, Members, [Customers], Contractors...
 - loyalty programs can use them
 - devices, bots, APIs

Verifiable Authority

- identifiable rep
- id of organization
- authority

1st gen VCs (for people)

- Portable VCs
- Secure and verifiable
 - who issued by
 - not tampered with
 - issued to who
 - not revoked
- verifiable by anyone
- great for personal things

2nd Generation Credentials (for organizations)

- Verifiable authority
- Delagability
- Non-repudiable signing (so an organization can't just say nuh-uh I wasn't me)
- Instant Revocability
- Broad/Global verifiability
- Use of existing cloud infrastructure
- Persistent Identifiers
- Keys become weak over time

Security

- recovery from compromise
- key rotation
- multi signature
- detectability of compromise
- prevent a thief of private key from using it for using credentials
- Quantum resistant

Autonomy

- no blockchain
- selective disclosure
- contractual disclosure (partial disclosure, step based, graduated)
- contingent disclosure, disclosure is contingent on something else

The first organization credential: vLEI

- bind to human legal entities
- held by top level representatives
- root-of trust for all other Credentials
- roles change, LEI changes hands
- LEI never changes

OI's Future

OI makes this verifiable:

- any person claiming authority
- documents, agreements, filings, any piece of data
- phone calls, texts, messaging any comms
- digital signatures
- bots, AI
- anything digitally produced by an organization

DTVP startus that use OI

- Telecom
- Healthcare
- Supply and Trade

Root of Trust != Authority

- A root of trust is not similar to authority, authorities can punish and come after you if you misbehave

eIDAS + Swiss E-ID Public Sector Cross Pollination

Session Convener: Kai Wagner

Session Notes Taker: Kai Wagner

(optional) List of Session Attendees: ca. 15 people (ranging from public sector ID project context in EU & CH; representatives of ID tech companies and standards people as well as consultants)

Notes:

The core quest of this session was to discuss in an open format about the learnings that can be achieved via cross pollination of the two major regulatory wallet and credential projects in Europe, the Swiss E-ID project and the eIDAS 2.0 regulation.

It was very vibrant discussion and the following take home messages were what we agreed on:

The state should:

- Provide Open Source tooling (planned in EU and CH)
 - (The public and private sectors issuers and verifiers need to be able to access the ecosystem of wallets via low risk tech investment, so key tools should be provided as open source by the ecosystem creator (government))
- Enable early stage piloting to create learning effects while implementing and allow for timely adjustments (done in EU and CH)
- Drive concrete use cases beyond E-ID (PID) issuance (done in EU and CH)
 - It was identified as a key need to ensure that the wallet contains more than just the E-ID from the start to increase everyday relevance and attractiveness.
- Support efforts to ensure semantic interoperability of credentials to harness interop potential and economies of scale when credentials are usable across contexts. (so far not properly pushed for in EU and CH)
- Create a storytelling around the day to day utility of the new tools (wallet, E-ID) and not describe technicalities or technical details)
- Provide support to implementers and wallet users to get feedback about concrete issues und challenges and take responsibility for fixing them, rather than launching the E-ID and then handing it over to some unmotivated managers.
- Motivate public and private sector players to issue credentials into the wallet and make it easy to do so, by helping people to leverage existing trust management or provide guidance on setting up sector or credential specific trust infrastructure

Multi Stacks & Multi Formats on Wallets

Session Convener: Bryan
Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

No Notes Submitted

SSI-based B2B ecosystem

Session Convener: Jeroen van der Hoeven (INNOPAY), Beau Schellekens (INNOPAY)

Session Notes Taker: Beau Schellekens (INNOPAY)

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Session summary:

- Businesses are striving for trust and operational efficiency with B2B services. A considerable potential lies in solutions that facilitate authorised transactions of individuals on behalf of a company. Digital identity and how (natural) persons digitally identify and authenticate has gained substantial traction with the revision of the eIDAS regulation. How businesses and individuals acting on behalf of a business identify themselves in external interactions (B2B, B2G) is little explored.
- An eID solution for organisations (often referred to the organisational wallet under eIDAS 2.0) with mandate management functionality results in an efficient and standardised process. This process enables us to identify a person and to check what the person is allowed to do on behalf of the organisation.
- The general consensus is that the eID wallet, whether following the Swiss E-ID approach or the eIDAS-wallet (Europe), will not effectively support managing ‘mandates’ in the form of VCs, nor will it be adequate for standardizing services and roles across borders and sectors. To establish a self-sustaining ecosystem for business identity (i.e., conducting business on behalf of your employer), this component of governance still needs to be addressed.
- GLEIF has initiated a working protocol for mandate management based on the vLEI (Verifiable Legal Entity Identifier), where the root identifier is the LEI (Legal Entity Identifier). This system provides an effective framework for managing mandates and can

be adopted globally for various use cases, ensuring standardized and secure business identity management.

- Other technical solutions are also feasible; however, the key challenge lies in determining who will govern these systems. Effective governance involves standardizing and managing these solutions to ensure they are widely usable and interoperable within the ecosystem. Without a clear governing body to oversee and enforce these standards, the ecosystem's reliability and efficiency could be compromised.
- eHerkenning serves as an example of a system where a central governance body oversees the management and standardization of the Trust Framework. This semi-public organization was established through a collaboration between private parties and public organizations. The central governance ensures that the network operates smoothly and adheres to consistent standards, facilitating secure and reliable identity verification across different entities.
- To successfully manage a B2B identity ecosystem, decentralized wallet-infrastructure is well-suited to provide the technical basis for sharing credentials in a B2B ecosystem. However, a governing trust framework is required to establish the right standardization of e.g., roles and services that dictate and control the mandates. This could be established on an industry level, but preferably on a national or even supra-national/European/global level, to facilitate interoperability across sectors and countries.

German eIDAS Wallet Consultation Project

Session Convener: Torsten, Paul
Session Notes Taker: Christian

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Link to slides: <https://www.kuppingercole.com/get/1430 - 1450 paul bastian torsten lodderstedt german wallet project v2.8.pdf>

Assumption is: Wallets are already here; What we see is a transition of physical cards to Credentials in the smartphone. eIDAS2 regulation will in the end ensure that whatever happens with wallets is done in a way that users are protected. Interoperability is really important to make sure things work across different countries.

eIDAS regulation can be seen as a blueprint for the rollout of the overall ecosystem and explains what kinds of systems should be opened up for this.

Every member-state has the responsibility to find out how that works for their country, the governance etc. The German project is collecting use-cases from the society. It is important to figure out what is provided by the government and what can be left to the market.

13000 municipalities in Germany and a federated state that makes things hard to be implemented at scale. Maintaining Interoperability with the rest of the EU and beyond is important. Key Requirements are security, privacy, usability, and user reach.

Short presentation on the organisational setup in Germany: Consultation Process, Wallet Architecture proposal, Funke (innovation challenge), Evolution Solution.

Consultation Process: Open participation for everyone - also reaching out to certain communities to get feedback. New working group starting soon on the operating/business model in July.

Wallet Architecture Proposal: Initial concept for PID; More PID options and (Q)EAA design; Focus on additional features (e.g., QES), operating model etc. The architecture also has to take into account the current german eID solution.

Short presentation on the 6 options for PIDs that are currently considered. Question on the adoption of the german eID card: Requires 6 digit PIN and not too many services are connected. Torsten comments that the time of plastic cards is over and we should focus on an onboarding process for the PID that has no obstacles.

Where should cryptographic keys be stored?

- 1: german eID as WSCD (Option B and C")
- 2: Secure Element as local WSCD (Option C and D)
- 3: Cloud HSM as remote WSCD (Option B' and C')

3rd Option (Cloud HSM) will be the choice for the first implementation to enable a bigger reach. HSM only contains the keys, but no PII data. Some discussion about the amount of keys that would result in HSMs and that everyone agrees that in the long run we want the keys to live in the smartphone but need something for the transitional phase.

Question on regulation: Is it only allowed to use the Cloud HSM for a transition phase? Torsten answers that there are no obligations from the current regulation.

Question on experience from the different consultation processes throughout europe: What option is most likely to get adopted and which other country is following a similar approach as germany. Torsten explains that other countries like Netherlands are following a similar approach to C' and the authenticated channel is a special proposal from germany.

Short presentation on "normal" signed credentials and that the keys live in the WSCD from the wallet. This option does not offer repudiation: It can be presented towards a third party and the third party can validate that this is also valid. There are concerns that this possibility of third party verification with government issued data is dangerous. If the relying party is acting malicious or gets hacked, the data is supposedly worth more. Torsten adds that RPs usually do not store signed data and not ID_tokens or similar. Paolo adds that we should create scenarios and discuss specific scenarios and what the options mean for that scenario.

Authenticated channel: Device key and all attributes are secured in the WSCD. <Look at slides for more details>

Johannes adds that in Blockchain Space, there is technology to prove the correctness towards a third party that is active during presentation. Torsten adds that by law Banks are audited and certified and if you hack into a Bank, you can be sure that the data is valid. Christian adds that the authenticated channel allows an attacker that breaks a single secure element to impersonate anyone, creating a huge security risk.

Paolo asks if this solution is legally ok for processes that require non-repudiation.

Paul adds that there might be a compromise with using signed data, but publishing the issuer private key after the credentials expired.

Torsten presents the Funke (germany PID innovation challenge). There are teams implementing every of the options. It is organised in 3 stages with 6 funded teams and 6 non-funded teams.

Time-wise, the scope is also considering long-term solutions / some research aspects. First stage runs until early September and there will be an event presenting the results.

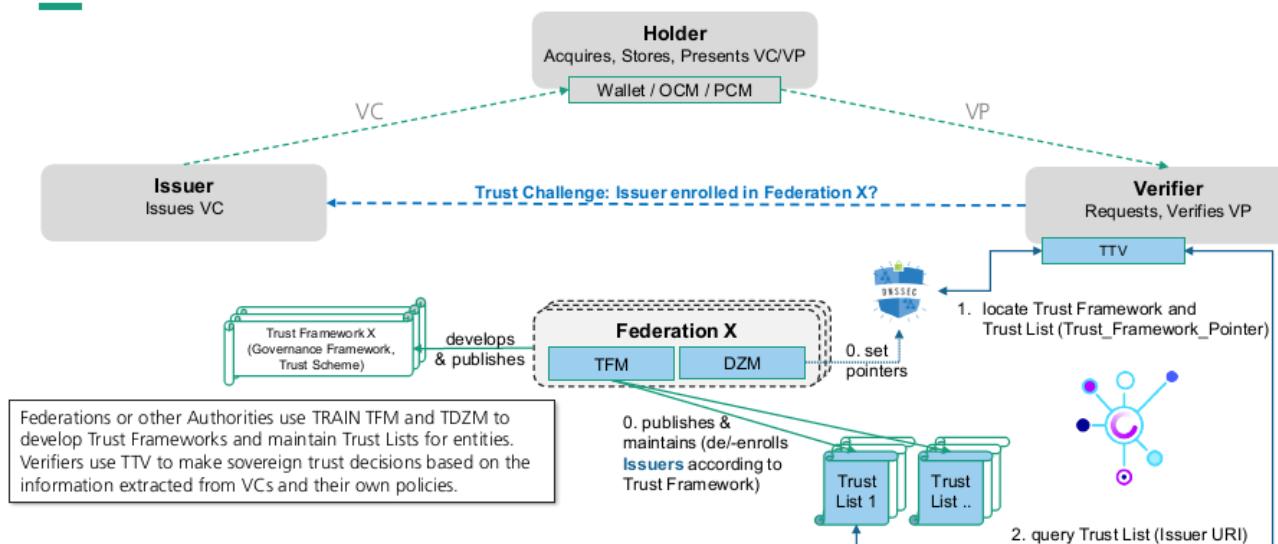
Decentralized Interoperable Trust Registries

Session Convener: Isaac Henderson
Session Notes Taker: Isaac Henderson

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

- The importance of Decentralized Trust registries were discussed
- TRAIN as trust framework approach to bridge different trust anchors was introduced.
- Use case on Gaia-X was discussed
- Difference between TRAIN vs OpenID Federation was discussed.
- Standardization of TRAIN was requested
- There was suggestion to standardize in IETF.
- There was interest to integrate TRAIN with existing wallet providers.

Overview



TRAIN Architecture

TRAIN DNS Trustzone Manager (DZM)

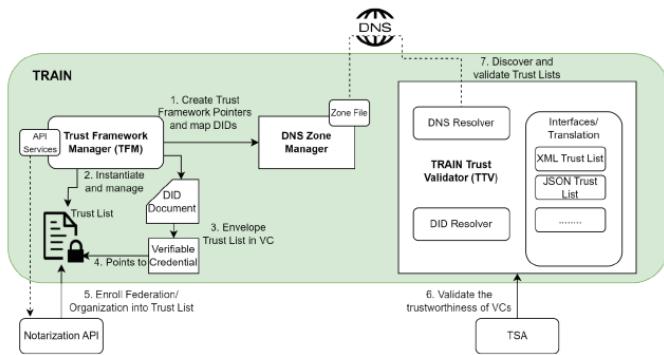
- Anchoring a Trust Framework in the DNS Pointer Resource Record (PTR RR)
- Trust List URI DID is anchored in DNS URI Resource Record (URI RR)
- Global discovery through DNS and DNSSEC for chain of trust

TRAIN Trust Framework Manager (TFM)

- Setup and Configuration of a Trust Framework
- Trust List Management: de-/enrollment of entities etc.
- Provides Federation/organization/participant specific Trust Lists in different formats

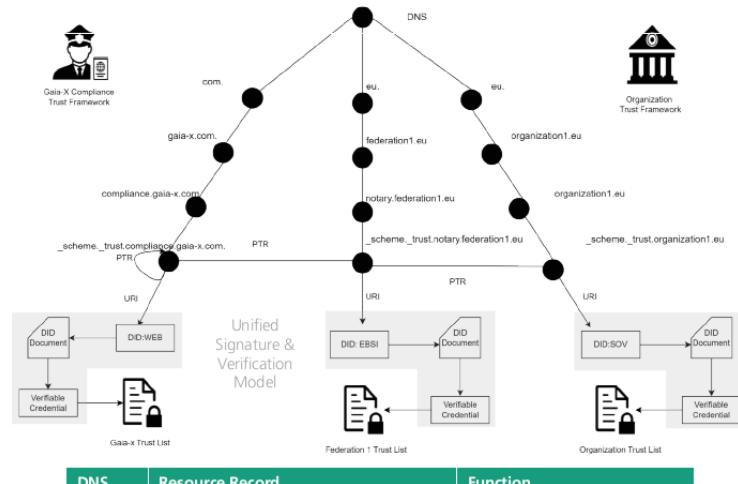
TRAIN Trust Validator (TTV)

- Supports external validation of trust through integration in a Trust Framework
- Global Discovery of Trust Frameworks through DNS Resolver
- Verification of issuer details of the credential with the information of the trust list



Leveraging DNS for creation, publication, and cross referencing of trust frameworks

- To set up their trust framework a federation can use their DNS at e.g., federation1.eu.
- The DNS RR holds the PTR for the trust framework and the URI to obtain the Trust List DIDs
- A trust framework operator, e.g., gaia-x.com, with scheme "compliance" may also chose to trust the trust framework e.g., "notary", of another trust framework operator, e.g., federation1.eu.
- The trust framework operator would therefore add pointer resource records (PTR RRs) to its DNS trust framework entry to point to this other trust framework.
- Allows for hierarchical structure of trust frameworks



DNS	Resource Record	Function
PTR	_scheme._trust.compliance.gaia-x.com	Trust Framework Pointer
PTR	_scheme._trust.notary.federation1.eu	Trust Framework Pointer
URI	http://some.org/trust_list/did.example...	Trust List Location URI

Trust Lists

XML Example

- TRAIN Trust Lists are based on the ETSI TS 119 612 standard and list all the enrolled entities in a specific data file/format certified by the Trust Framework Provider
- JSON-LD and XML currently supported
- Stored on web server or IPFS
- Every trusted VC issuer's details are described under the attribute <TrustServiceProvider>
- The ID (for example URI, DID or UUID) of the issuer is under the attribute <ServiceTypeIdentifier>

```
<ServiceTypeIdentifier>did:key:z6MkkVNpqpURtWDDy9Tx...</ServiceTypeIdentifier>
```

Slide 12 24/06/2024 © Fraunhofer IAO

Integration with Verifiable Credentials via TermsOfUse (W3C VCDM)

- VCs by issuers enrolled in a trust framework via TRAIN must contain a **termsOfUse** property
- Terms of Use contain the **Trust Scheme Pointers** (DNS names) of the trust frameworks(s) that the issuer claims to be a member of

W3C VCDM v1.1 / 2.0 (Candidate Recommendation Draft 03/03/2024):
"Terms of use can be utilized by an issuer or a holder to communicate the terms under which a verifiable credential or verifiable presentation was issued. The issuer places their terms of use inside the verifiable credential. The holder places their terms of use inside a verifiable presentation."

```
<TrustServiceProvider>
<UUID>1144355</UUID>
<TPName>Automotive Federation</TPName>
<TPTradeName>Automotive Federation e.V.</TPTradeName>
<TPInformation>
<Address>
<ElectronicAddress>notary@autofed.de</ElectronicAddress>
<PostalAddress>
<City>Stuttgart</City>
<Country>DE</Country>
<PostalCode>70563</PostalCode>
<StreetAddress>Heilbronner Straße 1</StreetAddress>
</PostalAddress>
</Address>
<TSPCertificationList>
<TSPCertification>
<Type>ISO_9001</Type>
<Value>9386546745</Value>
</TSPCertification>
<TSPCertification>
<Type>EN_62368</Type>
<Value>DE988889999</Value>
</TSPCertification>
<TSPCertificationList>
<TSEntityIdentifierList>
<TSEntityIdentifier>
<Type>LII</Type>
<Value>34701983XD7184FBC41</Value>
</TSEntityIdentifier>
<TSEntityIdentifierList>
<TSPInformationURI>https://autofed.de/informationuri</TSPInformationURI>
<TSPServices>
<TSPService>
<ServiceName>Notary Auto Federation</ServiceName>
<ServiceTypeIdentifier>did:key:z6MkkVNpqpURtWDDy9TxYuKvgSMFTu7kcAEwQfrkyiWqqrKV</ServiceTypeIdentifier>
<ServiceCurrentStatus>active</ServiceCurrentStatus>
<StatusStartTimestamp>2023-12-15T00:00:00Z</StatusStartTimestamp>
<ServiceDefinitionURI>string</ServiceDefinitionURI>
<ServiceDigitalIdentity>
<DigitalID>
<X509Certificate>123example</X509Certificate>
<DID>did:web:notary.autofed.de</DID>
<DigitalID>
</ServiceDigitalIdentity>
<AdditionalServiceInformation>
<ServiceBusinessRulesURI>https://notary.autofed.de/business</ServiceBusinessRulesURI>
<ServiceGovernanceURI>https://notary.autofed.de/governance</ServiceGovernanceURI>
<ServiceIssuedCredentialTypes>
<CredentialType>
<Type>Participant Credential</Type>
<CredentialType>
<CredentialSubjectType>
<Type>Principal Credential</Type>
<CredentialType>
<ServiceContractType>https://notary.autofed.de/contract</ServiceContractType>
<ServicePolicySet>https://notary.autofed.de/policy</ServicePolicySet>
<ServiceSchemaURI>https://notary.autofed.de/schema</ServiceSchemaURI>
<ServiceSupplyPoint>https://notary.autofed.de/sp</ServiceSupplyPoint>
</ServiceContractType>
<issuanceDate>2024-01-18T11:09:10.497Z</issuanceDate>
<type>[<"VerifiableCredential">]</type>
<proof>[{"type": "Ed25519Signature2018", "created": "2024-01-18T11:09:10Z", "verificationMethod": "did:key:z6MkkVNpqpURtWDDy9TxYuKvgSMFTu7kcAEwQfrkyiWqqrKV", "proofPurpose": "assertionMethod", "jws": "eyJhbGciOiJF2ERTQSIsImI2NCI6ZmFsc2UsInNyaXQiOlsiyjY0I1l9..wqaMMzw8vpOnHgZtoFkrvF0fuJTui4hv4Q-yaf-YTFaeclT4i8qUBrQDPFTYF0pxeZ-CckstilVsyMez01ebCA"}]</proof>
<context>[{"id": "https://www.w3.org/2010/credentials/v1"}, {"id": "https://identity.foundation/EcdsaScep256k1RecoverySignature2020/lds-eddsa-secp256k1-recovery2020-0.0.jsonld"}]</context>
<holder>did:key:z6MkkVNpqpURtWDDy9TxYuKvgSMFTu7kcAEwQfrkyiWqqrKV</holder>
<credentialSubject>[{"id": "did:key:z6MkkVNpqpURtWDDy9TxYuKvgSMFTu7kcAEwQfrkyiWqqrKV", "type": ["Participant Credential", "Entity Credential"], "OrganizationName": "Fraunhofer IAO", "OrganizationAddress": "Nobelstrasse 12", "OrganizationLocation": "Stuttgart", "OrganizationCountry": "DE"}]</credentialSubject>
<termsOfUse>[{"type": "train", "id": "https://train.trust-scheme.de/info", "trustScheme": [{"id": "notary.federation1.de", "id": "compliance.caia-x.eu"}]}]</termsOfUse>
<issuanceDate>2024-01-18T11:09:10.497Z</issuanceDate>
<type>[<"VerifiableCredential">]</type>
<proof>[{"type": "Ed25519Signature2018", "created": "2024-01-18T11:09:10Z", "verificationMethod": "did:key:z6MkkVNpqpURtWDDy9TxYuKvgSMFTu7kcAEwQfrkyiWqqrKV", "proofPurpose": "assertionMethod", "jws": "eyJhbGciOiJF2ERTQSIsImI2NCI6ZmFsc2UsInNyaXQiOlsiyjY0I1l9..wqaMMzw8vpOnHgZtoFkrvF0fuJTui4hv4Q-yaf-YTFaeclT4i8qUBrQDPFTYF0pxeZ-CckstilVsyMez01ebCA"}]</proof>
}</
```

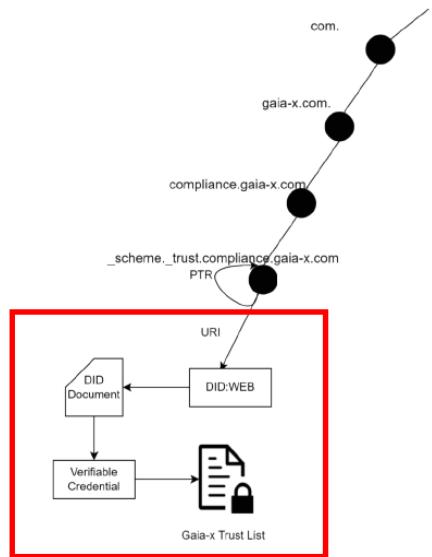
Unified Signature & Verification Model

Trust Lists via DID and VC

Allows trust lists across trust domains with different trust list formats (json, XML) to be signed and verified uniformly using Verifiable Credentials (VC).

Process

1. TFM provides endpoints for trust list initialization with different formats
2. On successful instantiation, the trust list is stored on IPFS/web server, their signature along with a hash is enveloped as VC and stored separately
3. The URI location of the VC can be resolved via a service endpoint of a DID Document



That's it – so far

Next Steps

- Standardization in Gaia-X and beyond
- UNDP Regi-TRUST as global pilot
- Evaluate the use of Ethereum Name Service (ENS) as a DLT-based alternative to DNS (a first concept exists for the GNU Name System)
- Future enhancements include extending the TRAIN implementation to support Open ID Federation Trust Lists and the EBSI Trusted Issuers Registry.



Check out TRAIN in the XFSC Toolbox: <https://gitlab.eclipse.org/groups/eclipse/xfsc/train/>

There is also a demo with documentation that lets you experiment with TRAIN locally:
<https://gitlab.eclipse.org/eclipse/xfsc/train/TRAIN-Documentation/-/tree/main/demonstration>



Paper Based Credentials - Do we need them? Why? How? For how long

Session Convener: Hgath Taylor

Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

No Notes Submitted

SESSION #3

Ethereum Attestation Services (EAS)

Session Convener: Grace Rachmany

Session Notes Taker: Grace Rachmany

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

- EAS allows a list of schemas anchored to the blockchain
- Anyone can attest to anything
- Conceptually, the EAS folks think that there will be reputation issuers who will run AI over the list of attestations to create reputation score algorithms that will issue different types of reputation scores
- That approach appears impractical to us
- It seems highly unlikely that there will be agreement about how to issue credentials and what schemas are acceptable
- In real life there are a couple of different approaches to reputation/ credential issuance
 - Creation of issuer registries (like list of accredited universities)
 - Official authorities that you pay to give you a certification (like the official “Organic” or “Fair trade” type of certifications)
 - Reviews systems
- The EAS approach seems overly generalized and probably not applicable over time
- VC and other types of standard credentialing schemas could use the system
- We don’t really know enough about it-- no experts appeared
- It was an unpopular session, only 2 attendees.
- Conclusion: as usual the Web3 community is reinventing the wheel and thinking they have new ideas.

VC Appearance e-ID with OCA

Session Convener: Michel Sahli

Session Notes Taker: Marco Stähli

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Visualization of VC with OCA

-
- visual representation of the VC depends on different type of attributes like images, text, dates, etc.
 - annotation of VC attributes like labels, sensitive information, encoding etc.is required
 - branding of VC is desired
 - OID4VCI Metadata does not cover a lot of usecases
 - OCA for base information (capture base) like the type and attribute name. Overlays describe then these base attributes with different information
 - OCA should be compatible with OID4VCI Metadata
 - OCA bundle link into the OID4VCI Metadata (new attribute)

discussions:

- governance/versioning on OCA: put link to terms of service into the meta overlay?
- W3C is working on standardising to add a OCA reference into the VC DM
- lifecycle: issued once the OCA seems not practicable, holder doesn't care when you update the branding to get a new VC issued
- overlays might change over time: eg. sensitive overlay flagging attributes
- OCA was not designed for VC specific, it was designed to ensure data integrity
- branding integrity for VC is desired
- updating OCA by the issuer on the fly is considered not a good idea (OCA is retrieved by the wallet once when it get issued the VC)
- VC is the product of the issuer, so the issuer should also be able to brand it like it want (eg. background image, etc.)
- background images are desired in order to build trust and get the same quality as google wallet and apple wallet
- problems from the analog world can not be necessarily solved in the digital world (eg. fake E-IDs which get just visual verified and not with the process)
- declarative approach with branding overlay simplifies existing w3c web approaches which gave too much power as well to the issuer
- where to host an OCA is a governance question
- Is OCA interesting for Verifiable Presentation?
- Would a second authentication to see details make sense for sensitive VCs?
 - Don't show sensitive data and possibility to hide it

Health SSI

Session Convener: Peter Janes

Session Notes Taker: Oliver Deak

(optional) List of Session Attendees:

Thomas Wüthrich

Luc Parret

Maxence Feller

Simon Emig

Anders Lynquist

Patrick Brouwer

Elmar Reif

Dominik Geller

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Introduction

- GovTech Hackathon 2024 challenge award
- Current prototype (work in progress)
- Focus is on use case (not cryptography)

Discussion

- What is the scope of clinical data to be represented by VC? What about MRI data, genetic data etc.?
- How will the practice information systems be incentivised to adopt
- What about tracking replacements, amount of drugs being provided
- Health Keri with chainability capabilities can support tracking of the dispensation of meds
- For adoption need to save doctors time
- A challenge is that numerous clinical systems don't store clinic data in standardized structured form (only free text or proprietary formats)
- Look to solve all the edge cases and see if you end up with a better system
- Saving time in onboarding

Conclusions

- With first implementations only low volume data is envisaged (covering the majority of use cases), i.e. no X-Rays, MRIs, genome data sets
- For adoption, existing solutions shall not be replaced, but rather complemented
- For acceptance, new solutions must add value for practitioner's processes (they don't care about the underlying technology)
- Transitioning will take several years (at least)
- Practical drug prescription and administration process is highly complex
- Health Keri shall be investigated as an option
- Target solution will be an end to end digital process, where relevant health data is captured as early as possible in structured form and passed on without losses

Next Steps

- Continue with Prototype > add user interface
- Demonstrate and discuss to clinical target group to raise awareness

Additional Information

- GovTech Hackathon 2024, Challenge «Digital Health with the new E-ID Trust Infrastructure» - <https://hack.opendata.ch/project/1103>
- GitHub - <https://github.com/Abdagon/health-ssi-2>
- Prototype Implementation Teaser Video - <https://youtu.be/CaEMHeJBKr8>
- DICE 2024 notes - with DIDAS documents - https://drive.google.com/drive/folders/1z1Ban7MKxz-yanZQrFsAx7H5zHR_liag

Security Issues Architecture Zero-Trust ARF 1.4 EUID + KERI - Security Models based on Root-of-Trust Type

Session Convener: Samuel M. Smith

Session Notes Taker: Henk van Cann

Link to slides:

https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI_Security_DICE2024.pdf

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Sam explains his **background** in designing autonomous systems at the University he was professor of.

Also seminal work in machine learning.

He wanted to do AI, but security was bad 10 years ago

Then to identity field, where security became an issue pretty quickly too.

Identity security is broken because it's 30 years old

This security is not working anymore: Barbarians have climbed over the wall.

It's not a Pessimistic view but a realistic view. He gets depressed when people don't want to act.

He calls the baby ugly (they will never forgive him)

Unique approach of security zero-trust trust domains

Armor analogy

All components must be there. If you don't wear full armour you're vulnerable
Helmet is not nice to use (messes up the hair) but that is no reason to not wear it. Even a peasant could easily kill you.
The likelihood (Susceptibility) of being attacked is something else than vulnerability.

Susceptibility - recoverability

Integrity - Confidentiality - Privacy (A US government organisation's mission) -> Sam: WHERE IS SECURITY?!

Don't pretend that your weak security will work in all cases.

If you're building identity systems and not have security as the first priority you will build a system that most probably will be broken in the future.

The rate of exploits are increasingly growing. Read the security magazines with the proofs.

In 2018 we said we all need to go to zero-trust, but we failed.

0. Sam explains the basis of a trust domain - slide.

You need strong crypto-graphical bindings.

Ownership of an identifier is immaterial, who controls an identifier, is important.

1. Sam explains the administrative trust basis - slide.

eIDAS is an administrative root of trust, having two weak bindings: These have Dozens of known attacks on the weak bindings -> your building a system that is vulnerable to begin with.

All the breaches : a bearer token put in the a chat. The organisation blame the customer. Bit they are the cause because building weak systems!

You can't reasonably build those systems anymore, because you know that you will get breached somewhere in the future. Especially when you hold valuable information (honeypot).

Attackers are getting smarter because:

- 30 years to think about it
- chatGPT is making it worse

People are bad in security, even people researching security are bad in security.

2. Algorithmic Trust Basis - slide

Scalability and silos are a problem: you have to trust other ledgers for interoperability.

GLEIF director Wolf explains the ledger wars between service provider he had to cope with in the past: "It never felt right".

Sam explains how he took years to come up with: ->

3. Autonomic Trust Basis

New stuff and new terminology that came with it:

KEL (<https://weboftrust.github.io/WOT-terms/docs/glossary/KEL?level=2>)

Duplicity (<https://weboftrust.github.io/WOT-terms/docs/glossary/duplicity?level=2>)

Duplicity detection (<https://weboftrust.github.io/WOT-terms/docs/glossary/duplicity-detection?level=2>)

Sam explains recoverability mechanisms in KERI

He responds to a question from the participants. A Domain Name can't be a strong binding between a key-pair and the identifier. That's why the Internet is broken.
Validators have a first seen, always seen, never unseen policy. An attacker can't compromise Once I've seen a version of a KEL I can never accept any other.

Certificate Transparency (CT)

Sparse Merkle tree of trillions of Domain Names -> at least they tried to give openness multiple CA can issue certificates!

In KERI only 1 can issue and if there's duplicity this entity needs to reconcile from that.

Sam explains the sheet Why the Internet Protocol (IP) is broken.

Sam explains the sheets Spanning Layer and Solution: Waist and Neck - slide

Trust Spanning Layer

Minimally sufficient! In our DNA.

"KERI light" doesn't work : if you put on too little armor ... (referring back to the analogy in the beginning) : Guess where I am attacking?!

Another of Sam's analogies: "KERI has too many notes" (Salerie in the film "Amadeus")

KERI has been deliberately designed to be minimally sufficient.

ZERO trust ?! eIDAS / ARF

verifiable

not verifiable - Ratio is a (rather terrible 10%)

Dr. Wolf of GLEIF: Don't sacrifice security for convenience

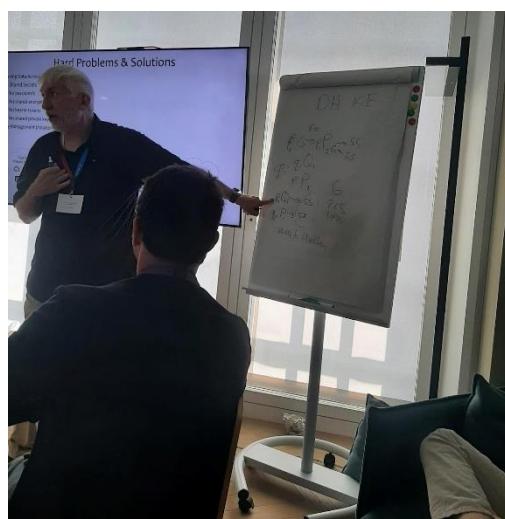
Why are KERI-light DID - web methods vulnerable?

Dead key - attacks

SCI doesn't protect

Sam mentions the education gap: "You could graduate from any University on Identity Systems Security today not knowing what I am talking about."

Sam explains the current problem with the [Diffie Helman Key Exchange](#) (see photo): Conclusion : it's broken.



Tell me about your identifier! Identification Traits

Session Convener: Jan Christoph Ebersbach

Session Notes Taker: Jan Christoph Ebersbach

(optional) List of Session Attendees:

- Drummond Reed
- Mirko Mollik
- Daniel Hardman
- 2-3 others

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

The current DIF effort to collect traits / features of Decentralised Identifiers was introduced: [DID Traits](#)

Together, we worked through the list of traits and assessed their relevance and completeness. A final conclusion wasn't reached. However, the general usefulness and need was confirmed.

Existing efforts like DID Rubric and multiple papers that try to define a taxonomy are good starting points but they're outdated. Esp. the DID Rubric has a different focus, it tries to appraise the level of decentralisation of a DID method.

Multiple new traits were brought forward, like decentralisation of DID method, security, etc. The following things were noted:

- DID traits is an attempt to compare DID methods, not to judge methods. The judging should be done by implementers who know their requirements. DID traits should help to compare and pre-select DID methods. A detailed analysis of the pre-selected DID method is still required by the implementer.
- Not all possible technical aspects can be represented in the traits list while still keeping it useful. The challenge is to identify the traits that best describe the differences between DID methods.

We discovered that:

- Open Wallet Foundation has done some work in this direction, already: <https://openwallet-foundation.github.io/credential-format-comparison-sig/#/resources/Key%20Management>
- Trust over IP Foundation wants to do work in this direction. The attempt is called "verifiable identifier appraisability framework".

We concluded that the efforts should be joined.

Slides: https://presentations.identinet.io/#240619_DICE_DID_Traits

NAO - Now Networked Adaptive Organisms

Session Convener: Charles Blass

Session Notes Taker: Kaliya

(optional) List of Session Attendees:

Kaliya - Dr. Mafa - Yuting

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Brad Degraf - was a computer graphics guy - now a social graph guy - lol based on his name.

Worked on liquid democracy - 2005 paper smartocracy

concept driving affordances from network cooperative concept.

Network cooperative as a new legal form

Platform cooperatives.

Cooperative-ism into the network context and frame - owning and governing data in a network

concept and premise is on the edge of prototyping.

Liquid coordination

coordination and collaboration

Allocating resources might be experts for example in a particular bio-region

Identifying people and populating attributes per domain.

Identity piece -

Charles - new to be leading conversation vs helping make the community help.

Kaliya - helping with FAN Federated Authentication Application

GreenCheck.world

Very good visualizer.

People in the network attest to each other - ½ dozen accounts can be verified - github, facebook, linkedin etc.

LinkedIn helped to populate the network

Emerge conference in Austin -

pre-populate through connections.

Barely more than a dozen. Providing data directly.

250,000 people.

Can claim account - other people can recognize you.

People to People.

sharing resources from the people in the session.

Proof of Person hood.

Stigmergy as a Universal Coordination Mechanism: components, varieties and applications

Many works.

Issues of how people are verified but not having to use their “real name” online.

Limited Liability Personas.

Own our Data together and govern it.

Can it become a [DataUnions](#).

accountable pseudonymity.

Surveillance and being hacked.

Feeling of anonymity can be deceiving.

Can not be accountable for what you do - something not allowed to do anonymity.

BlueSky

ATProtocol

Host server self

FarCaster

Own the key on your phone.

DSNP

Portable Communities - protocol.

Digital Commons

Abundance?

Membranes and boundaries

Need to define and draw these lines

What is the Priority?

OpenID4VC Updates, AMA

Session Convener: Oliver Terbu, Torsten Lodderstedt, Christian Bormann, Paul Bastian
Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Notes are here/Slide Deck:

https://docs.google.com/presentation/d/1FSMWbdM3zdNaJROJUIONfuMG1SJYIA5CukGXoFrkMPw/edit#slide=id.g2e46af1b3af_1_71

SESSION #4

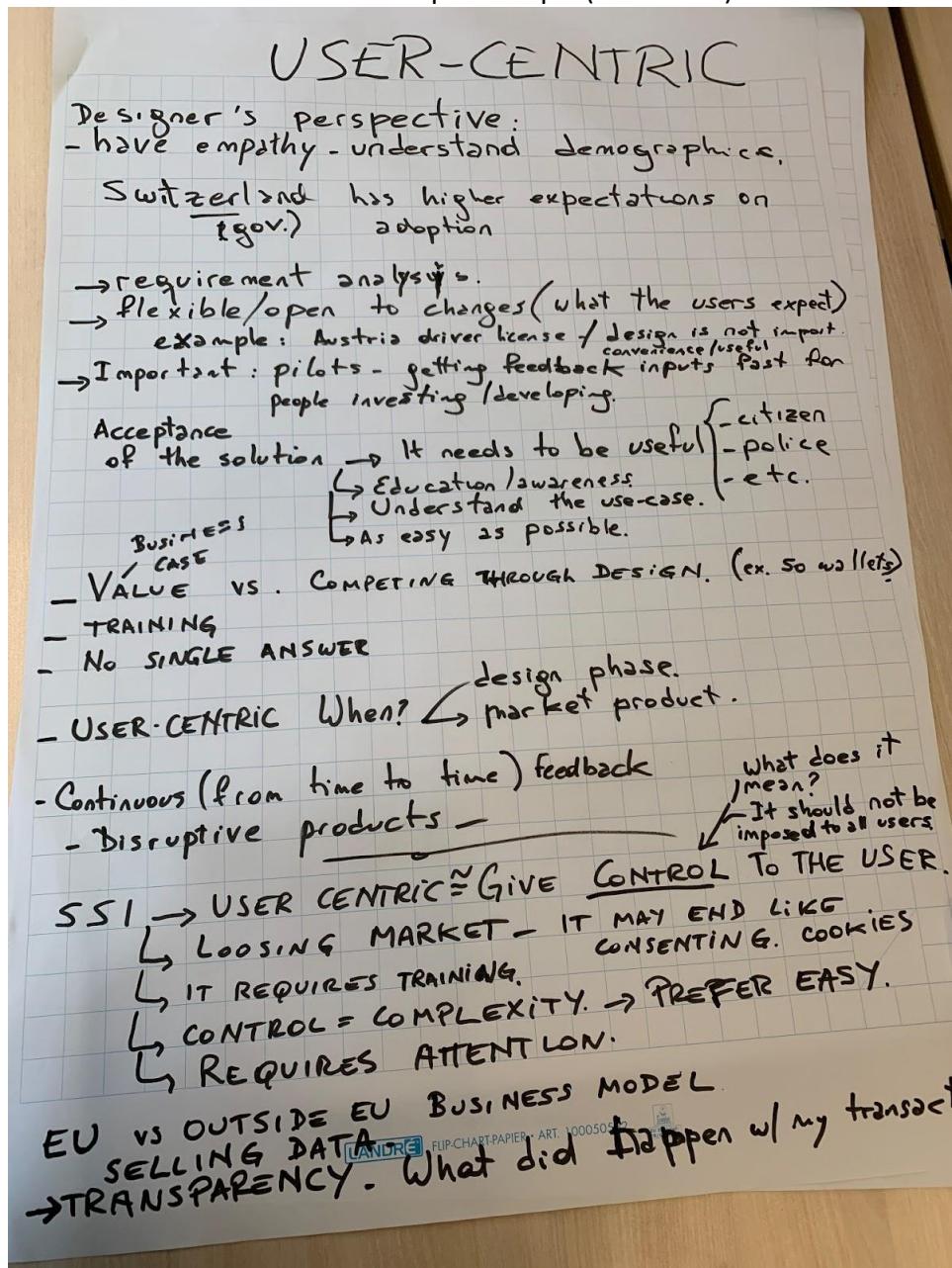
User Centric - What does it mean?

Session Convener: Vero Estrada-Galiñanes

Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

I will add notes later. Here is the poster's pic (see below)

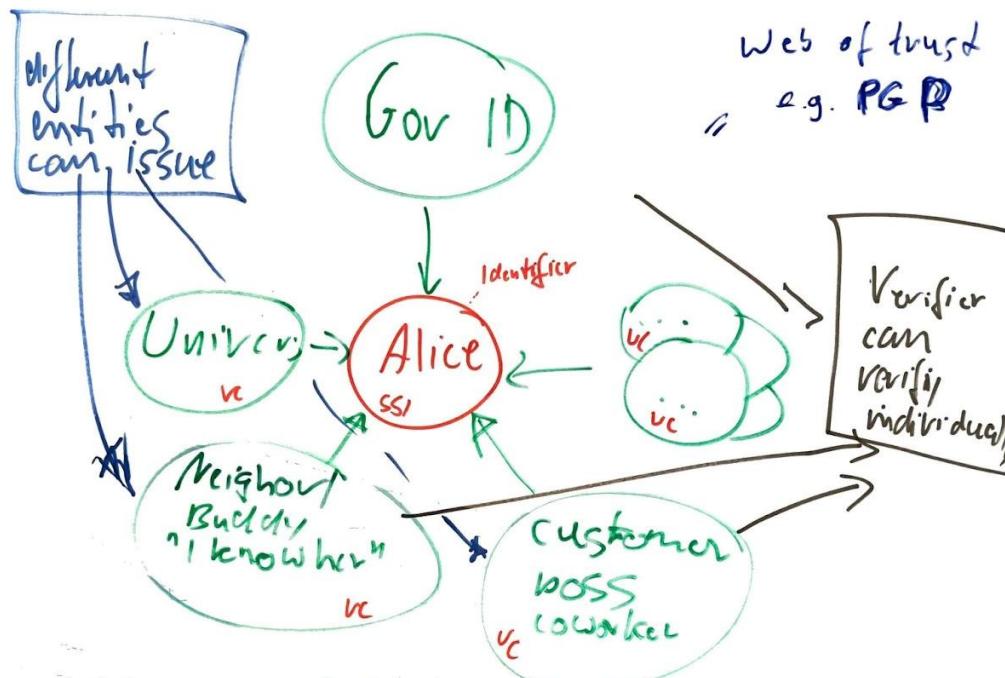


From Identity to Reputation

Session Convener: Ekhard Seeßelberg

Session Notes Taker: Ekhard Seeßelberg

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

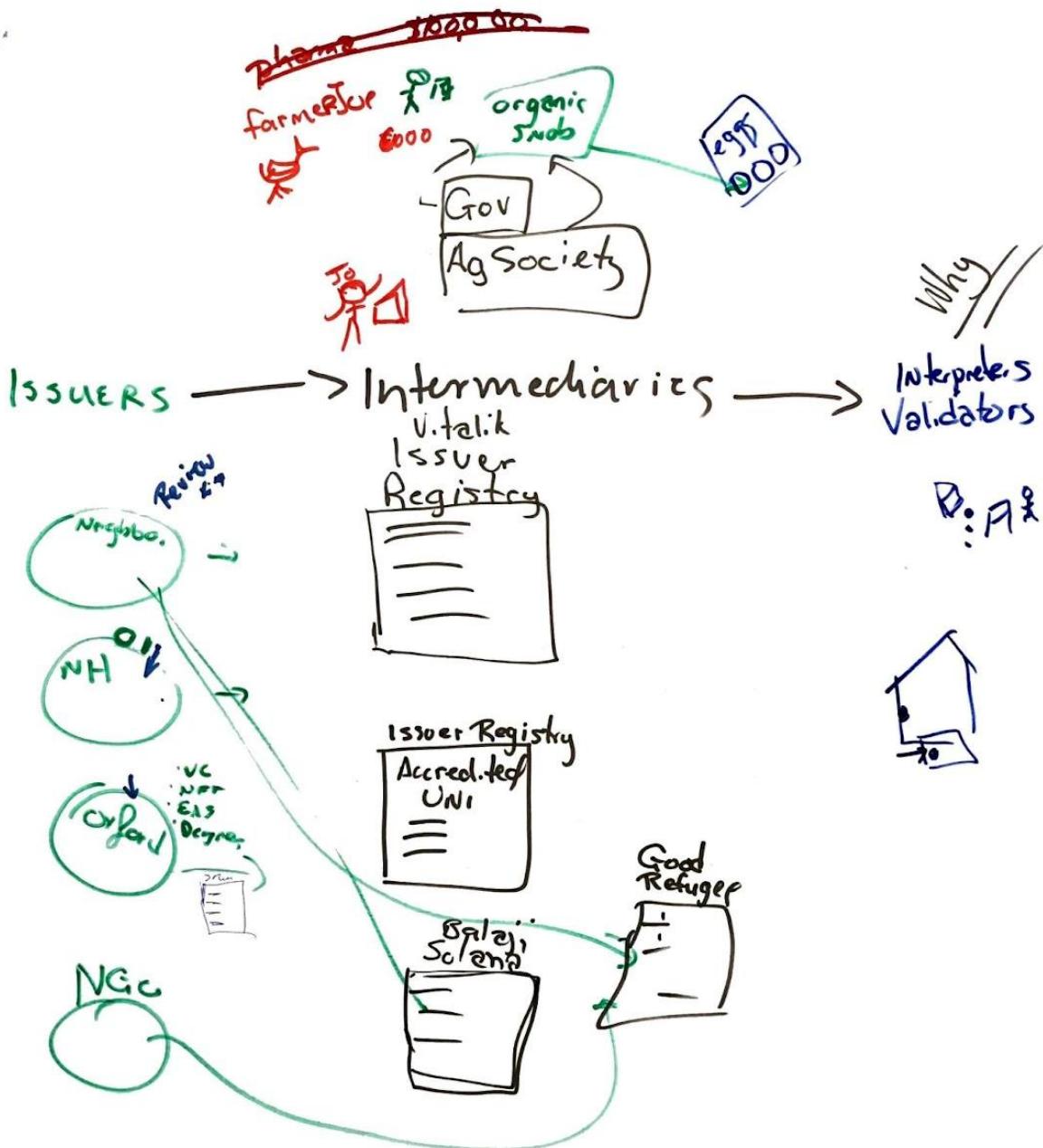


Why? - What is the context?
- what is the purpose - get into a country
- establish reputation - get accepted
 to validate open bank account

Risks: - could it become Social Credit Score?

Alice = generative identity, contextual
Alice might have multiple ones
Gov ID not mandatory

ECHO



Validator decides which credentials he accepts

Summary:

- collection of VCs linked to an identifier could strengthen acceptance of identifier for different purposes
 - e.g. get entry into a country
 - e.g. open bank account
- Government attestation of ID is only 1 datapoint to establish how trustworthy identifier is, but is not mandatory
- Alice could have many identifiers for different purposes
- but highly dependent on purpose
- for many use cases use of VCs is better solution
 - Verifiers decide which VC to trust
 - much more finegrained
 - least disclosure

Pros & Cons of UNIQUE IDENTIFIERS

Session Convener: Laurent Loup

Session Notes Taker: Laurent Loup

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

EU PID definition in early versions of ARF contained four mandatory attributes (name, surname, date of birth, Unique identifier). From version ARF 1.4, the unique identifier has been removed from the list of mandatory attributes. Probable reasons: difficulty to converge to a definition of that UI and potentially also avoid correlation and linkability through this persistent identifier.

A unique identifier could still be added in the optional data field and would be national based and could be linked to the physical document.

In Switzerland, the current project of law foresees also a unique identifier (could even be the physical card number or the passport number).

Is this problematic from a data privacy stand point ?

We need to distinguish:

KYC (5%) that require to be able to uniquely identify people (eg Hotel, banks, airlines). Those require a unique identifier. Relying parties have liabilities linked to people identification. This must usually be linked to physical identity documents

Social networks and ecommerce (95%) that require to authenticate people and do not necessarily need to identify people. The account will be unique but one person could have multiple accounts. Though, often a proof of personhood (POP) is requested (eg captcha)

Conclusions from the discussion are:

A verifier should not ask for that unique identifier number if it is not requested to perform the transaction. Regulation could help to clarify who has the right to ask for (eg health sector for social security number in Switzerland)

If an identification is requested, there are several models:

- Verifier keeps all data to identify uniquely the user
- Trust service provider keeps all data and provides identification services based on ZKP
- Smart contracts

For social networks and ecommerce use-cases, a context-based unique identifier should be used.

For regulatory purposes requiring the passport number (eg airlines, hotels, banks, ...) , a state-issued VC containing all passport attributes would be very helpful, both for the end-user than for relying parties. Often today, verification relies on manual entries or cumbersome chip retrieval processes.

Laurent Loup laurent.loup@sicpa.com

Join the ToIP Fun

Session Convener: Judith Fleenor

Session Notes Taker: Henk van Cann

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Slide 1. Judith: Is Trust a technology thing only? ToIP focusses at both: human side and technology side.

Slide 2. Judith explains how Governance is iterative process. And shows all the parts.

Slide 3/4: Challenges people to join. Drummond explains there are ToIP tools to use.

Slide 5: Explaining the various working groups

Slide 6-?: Judith explains all the Working groups. And mentions that there are a few Tasks Forces missing because they are rather new.

Trust Registry Protocol

Drummond explains that you don't have to use the whole KERI Suite to use the CESR protocol.

Judith adds arguments:

Scalability

Costs

Concludes on the sheet "Ecosystem Foundry Working Group"

This working group focusses on using ToIP component in a cafeteria-like model together with external ecosystems to implement systems.

A participant is interested in the shortest learning path about all the ToIP tools and working groups : how to start today?

Judith lays out the steps:

1. Fill out the ToIP form

2. Get introduced to specific interest groups

3. Jump in! Ask questions in Zoom (or asynchronous in the Slack groups)

3 types of members:

a. Steering Committee members

b. Organisational membership

c. Contributing member individual

The wiki is accessible without membership ! <https://wiki.trustoverip.org/>

Open Wallet Foundation - SIG's, Intention, SDK's, Wallets, Profiles

Session Convener: Mirko Mollik

Session Notes Taker: Mirko

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

In the session the intention of founding the openwallet foundation was explained. They are not focussed on writing standards, but allowing communities to work on open source code for wallets. Some of the projects were presented in the session, Timo and Berend from Animo presented Credo and why they moved the project from Hyperledger to the openwallet foundation. All other projects can be found here: <https://tac.openwallet.foundation/projects/>

Beside the code, two special interests groups were presented. They give an overview over the credential profiles, wallets and agents out there:

- <https://openwallet-foundation.github.io/digital-wallet-and-agent-overviews-sig/>
- <https://openwallet-foundation.github.io/credential-format-comparison-sig/#/>

The audience was happy about the work done in the OWF, that can be used in own products. A discussion about different wallet approaches like native wallets on the smartphone continued after the presentations of the different groups.

Thinking Outside the Wallet - A blueprint for Universal Zero Trust

Session Convener: Manu Fontaine

Session Notes Taker: Manu Fontaine

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

In this session, we outlined what needs to be done at the infrastructure layer, outside the wallet and around the three-party model, to enable “universal zero trust”, i.e. the verification of everything, not just credentials. Confidential Computing is a key enabling technology for complete verifiability.

Feel free to reach out to discuss: manu@hushmesh.com

Overview slides here:

https://drive.google.com/file/d/1NsNfwgA_j6plaqw0mqXLJ123bbBWnhab/view?usp=sharing

Birth Certificates 2.0 aka Foundational Identity

Session Convener: Stephan D. Hofstetter (stephan@secoia.ltd)

Session Notes Taker: Merul & Stephan

List of Session Attendees:

Kaliya Young; Maria Gabriela Sarmiento; Merul Dhiman;

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Index:

- 1 Part 1: Short primer to the topic
 - 1.1 Slide Deck (excerpt)
 - 1.2 Online Documentation:
- 2 Part 2: Discussion notes provided by Merul

Synopsis

As the group was introduced to the world of foundational identity and CEN's standardisation efforts, they became increasingly immersed in the considerable challenges. We discussed the need for government-backed identity in an internationally unregulated environment. We touched on the longevity of the vital event record versus the limitations of trusted technology architectures. We also discussed the anchoring of infants without the very limited suitability of biometrics for this purpose. Anchoring to the mother's identity was touched upon. However, the issue became complex in the case of egg or sperm donation, surrogacy and adoption. An example from India showed a pragmatic status quo, where the event of birth is recorded and linked to the parents identity, and this identity is enriched with a registration number at the age of 3 and a first biometric registration (face) at the age of 5.

The topic was found to be both fascinating and complex, and Kaliya suggested that an IIW Special Topics online event be set up to broaden and deepen the discussion.

Part 1: Short primer to the topic

1.1 Slide Deck (excerpt)

Disclaimer: No use or reproduction without full attribution

CEN

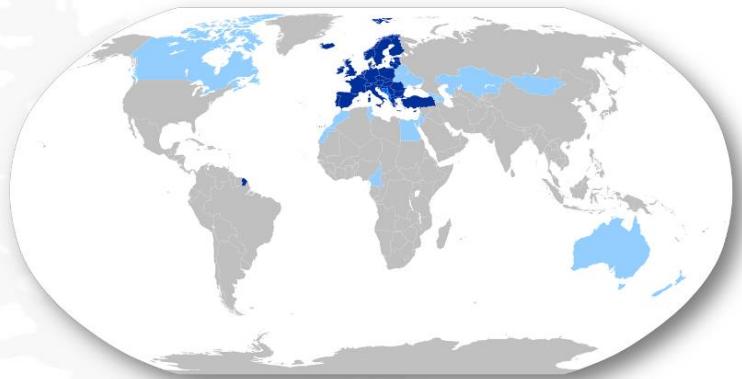
About

- **European Committee for standardization** which is recognized by the EU as being responsible for developing voluntary standards at European level
- "Sisters": CENELEC, ETSI
- Located: Brussels, Belgium



Members

- National Standardisation Bodies (NSB) of 34 European countries



CEN Partners

- Non-European NSBs, (European) Organisations

CEN TC224

CEN TC224: Machine-Readable Cards, related device interfaces and operations

- WG 1 – ICC physical characteristics
- WG 2 – General concepts for ICC systems
- WG 3 – Device interface characteristics
- WG 6 – User Interface
- WG 7 – PIN presentation
- WG 8 – Thin flexible cards
- WG 9 – Telecommunication applications
- WG 10 – Intersector electronic purse
- WG 11 – Transport applications
- WG 12 – Health applications
- WG 15 – European citizen card
- WG 16 – Application interface for smart cards used as Secure Signature Creation Device
- WG 17 – Protection Profiles in the context of SSCD
- **WG 18 – Interoperability of biometric recorded data**
- **WG 19 – Breeder Documents**
- **WG 20 – Ad hoc Group on European Digital Identity Wallets**

CEN TC224

CEN TC 224/WG 19

- "is leading standardization activities specifically for Europe in the **field of Breeder Documents**. It includes, but is not restricted to, **data collection, application, issuance and renewal processes**".
- prepares the CEN Technical Specification (TS) 17489 series "Secure and interoperable European Breeder Documents".



«Breeder documents are used to support applications for identity, residence and travel documents, such as birth, marriage and death certificates».

European Union

Drivers

Strengthened international travel & migration frameworks

- Breeder documents are often **unsecure documents** while they are the basis of the identity for many of these countries.
- Most breeder documents are much **easier to forge than e-passports**, and by using forged breeder documents (via identity theft or fake ID) people can obtain genuine travel documents.
- **No standard format or standard issuance process** for breeder documents.
- As a consequence:
 - can **barely authenticate** a breeder document, if presented as physical document.
 - And digitized civil registries or electronic breeder documents often cannot be accessed or validated in **cross-administration scenarios**, due to technical or legislative constraints.



UN SDG 16.9

- Article 6 of the Universal Declaration of Human Rights and Article 16 of the International Covenant on Civil and Political Rights state that "**Everyone has the right to be recognised as a person before the law**". Several international human rights instruments, such as Article 7 of the Convention on the Rights of the Child and Article 24(2) of the International Covenant on Civil and Political Rights, also recognise a **right to birth registration**.

Standards scope



Part 1: Framework

- CEN/TS 17489-1:2020
- available in German and English



Part 2: Data Model

- CEN/TS 17489-2:2023
- under final balloting



Part 3: Basic technologies

- CEN/TS 17489-3:XXXX



Part 4: Profiles for birth, marriage/partnership and death certificates

- CEN/TS 17489-4:XXXX



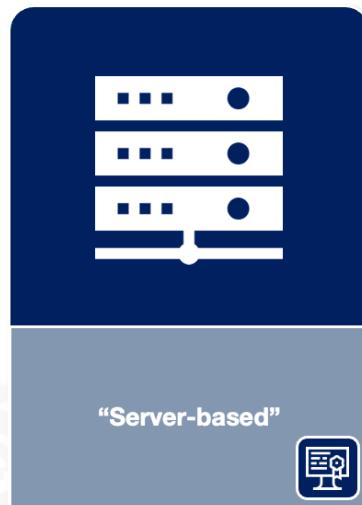
Part 5: Trust establishment and management processes

- CEN/TS 17489-5:2024
- Work in progress: prTS

Form Factors

CEN/TS 17489-1 distinguishes between

Picture credits: Freepik



Data Storage - Constraints

Digital Signature

- Breeder document data **must be digitally signed** to ensure the integrity and authenticity of the data.
- The digital signature can be verified using a public key infrastructure (PKI).
The signature verification can be performed
 - offline (provided that all data required for the signature verification, i.e. public-key certificates and certificate revocation lists, are available), or
 - online (server-based).

Storage-size

- A 2D bar code provides only limited storage space (about 3 kByte).
- The storage space on a chip and on a server is much less restricted.

Validity period

- A digital signature has a limited validity period.
 - After expiration of the validity period, the digital signature cannot be used any longer to ensure the integrity and authenticity of the breeder document data.
 - → Therefore, the breeder documents have to be re-issued after expiration of the validity period unless the digital signature is stored and renewed on a server.

Biometrics

Constraints on the choice of the biometric modality

- Biometric data must be **adequate** and **limited** to what is necessary for verifying the identity.
- It must be **easy to acquire** biometric samples of sufficient quality
 - at the time of breeder document issuance and
 - at the time of breeder document verification.
- The biometric characteristics must be **invariant** over a sufficiently long time.

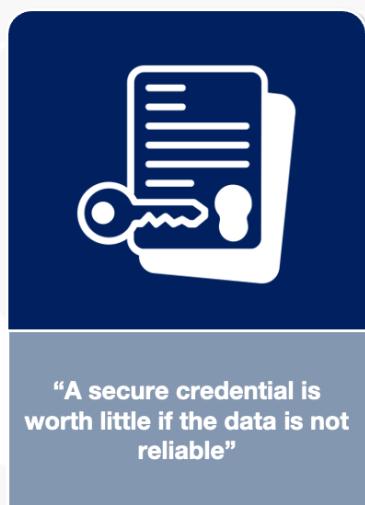


Constraints on the system

- Starting from trusted enrolment system, **integrity and authenticity** of biometric reference data must be ensured;
- Access to biometric reference data must be **controlled; confidentiality** must be protected during transmission;
- **Distinguish** between bona-fide presentations and presentation attacks, data injection attacks or morphing attacks.
- The biometric reference data must be **technically usable** by other suppliers' subsystems.

Dimensions guiding the development

Picture credits: Freepik



Connecting

More information / informal feedback and input

- Stephan D. Hofstetter stephan@secoia.ltd

Formal participation in the working group

- via your national body

Connect with CEN / CENELEC



<https://www.cencenelec.eu>



<https://www.youtube.com/@cencenelec>



<https://www.linkedin.com/company/cen-and-cenelec>



<https://twitter.com/Standards4EU>

Report on this subject provided
by SECOIA



1.2 Online Documentation:

- Part 1: Standardization of Breeder Documents - Part 1 "Setting the scene"
<https://www.secoia-excon.com/post/standardization-of-breeder-documents-part-1-setting-the-scene>
- Part 2: Standardization of Breeder Documents - Part 2 "The standardization effort"
<https://www.secoia-excon.com/post/standardization-of-breeder-documents-part-2-the-standardization-effort>
- Part 3: Standardization of Breeder Documents - Part 3 "Trustframework and Policy"
<https://www.secoia-excon.com/post/standardization-of-breeder-documents-part-3-trustframework-and-policy>

Part 2: Discussion

Aspects

Anchoring

- How to anchor the individual?
- Who executes the anchoring and vets for the trustworthiness?

Special cases

- Adoption
- Surrogacy
- Foundlings

Technology

- Interoperability
- Longevity
- Resilience against manipulation, leaking, failing technology

Life cycle & Resilience

- Migration into new administrations
- Failing states



© 2024 SECOIA Executive Consultants AG | all rights reserved

21

Notes Merul

Birth Certificate

CEN (committee of standardization, it is not EU)

- 34 European countries

Working on Technical Committee 224 - Machine readable cards

WG 18, 19

WG 19

- Standardization group for breeder documents
- CEN TS 17489 Creates a secure and interoperable European Breeder documents

Context

- Breeder document are used to support applications for identities, residence etc, acts as a foundational ID
- Breeder documents are a bit messy when it comes to cross-jurisdiction identification
- Everyone has right to be recognised as a person before the law
- [Object 4 of global compact on regular migration](<https://globalcompactrefugees.org/objective-4-support-conditions-countries-origin-return-safety-and-dignity>)

Form Factors

- Paper-Based
- Hardware-Based
- VC
- Server-Based

Data Storage

- must be digitally signed
- digital signature must be verified using PKI
- Signature must be verifiable offline & online
- storage size on barcode is limited to 3Kbyte
- Storage space on chip and on a server is limited
- Digital signature has limited validity

IETF Token Status List

Session Convener: Christian, Paul

Session Notes Taker: Christian

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Shown slides are here:

https://docs.google.com/presentation/d/1iZSxxLsnxzobFEFLD9tOGfmyG2X_yAnBu2XVH3VvEJA/edit?usp=sharing

We had a good discussion on the current state of the draft and open points like a long discussion about whether or not to keep the unsigned option for the status list.

There was also some discussion about the fact that an easy revocation mechanism like status list works surprisingly well for zero knowledge proofs based on ZKms.

Additionally Bundesdruckerei showed a live-demo of batch-issuance with status-list and revocation of the Credential triggering the batch-revocation of the corresponding status list.

The Missing Principle of SSI: “Trust must be earned”

Session Convener: Mike (Michael Doujak)

Session Notes Taker:

(optional) List of Session Attendees:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

These are the slides that I use to introduce the topic:

Topics in the presentation

The main points of the presentation were:

- Every actor in the SSI trust triangle requires some sort of trust.
- To earn this trust, the actor should collect the evidence (i.e. do the work) required to prove that trust is warranted and present it to the other party.
- Based on this premise, some of the things we take for granted today are questionable.
 - E.g. Forcing a verifier to verify a VC with a trust list relieves the holder from collecting evidence and forces the verifier to do it.
- Done this way, protocols will contain all the data required in the request to validate the request's trustworthiness and the requester. The problem, that a developer fails to implement all the additional checks correctly is moot since the data is already being provided.
 - E.g. if VC status information is already provided, there is no need to fetch it. The check is reduced to signature validation and establishing that the key material is from a trusted source (e.g. a trusted root key)

Topics in the discussion

The discussion was about the following points:

Right after the presentation an excellent example was provided for the problem, that we often delegate the burden of collecting evidence to the “incorrect” party.

- In Switzerland, the burden of proof for issuing organizational IDs (X.509 certificates for digital signatures) is with the QTSP (the qualified CA) and not with the parties that submit the documents.
- This problem is made worse by the fact that the required documentation must be obtained on paper (due to the lack of electronic seals by the commercial register).

It was pointed out that the proposal cannot and will not solve the “root problem”. In other words each actor still needs to maintain for itself a list of trusted roots that it will accept to verify evidence being presented by other parties.

There was a discussion if credential chaining could solve the problem, but it was felt, that credential chaining is not the right solution to this problem and that it would create more issues.

The idea that every actor requires some sort of trust was challenged. Specifically, the example was given that the Swiss government did not require any trust when issuing the E-ID to a citizen. The consensus was found that issuers in general needed to prove to holders that they were genuine and that in this particular situation, the holder (even if the purpose of the exchange was the issuance of a VC) did behave like a verifier and had the right to verify the authenticity of the issuer.

Topics outside the discussion

The topic of scalability only came up after the session:

- Issuers and verifiers are involved in many exchanges during the day. Having protocols where they can prepare not only proof of their identity but also provide revocation status information would allow for a considerable increase in efficiency through caching status information.
- The alternative that the holder's wallet checks the revocation status for every single exchange seems much less efficient.

SESSION #5

Zooko and Houdini - a parable and why it matters to all of us

Session Convener: Daniel Hardman

Session Notes Taker: Drummond Reed

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Daniel presented this Google Slides deck: <https://bit.ly/3VrSMpp>

It is highly recommended to review this deck in full because it explains all the key points about the **problem** — which Daniel calls the Sovereign UX Paradox — that the more we automate SSI processes, wallets, keys, etc. for users, the less actually “sovereign” they really are.

He then focused on one specific **solution** for part of the problem: helping users understand the identifiers that users need to either understand from others or assign themselves and **make good decisions about those identifiers**.

His solution — of establishing simple, understandable UX rules for human-friendly identifiers — is very intuitive and extremely easy to specify and adopt.

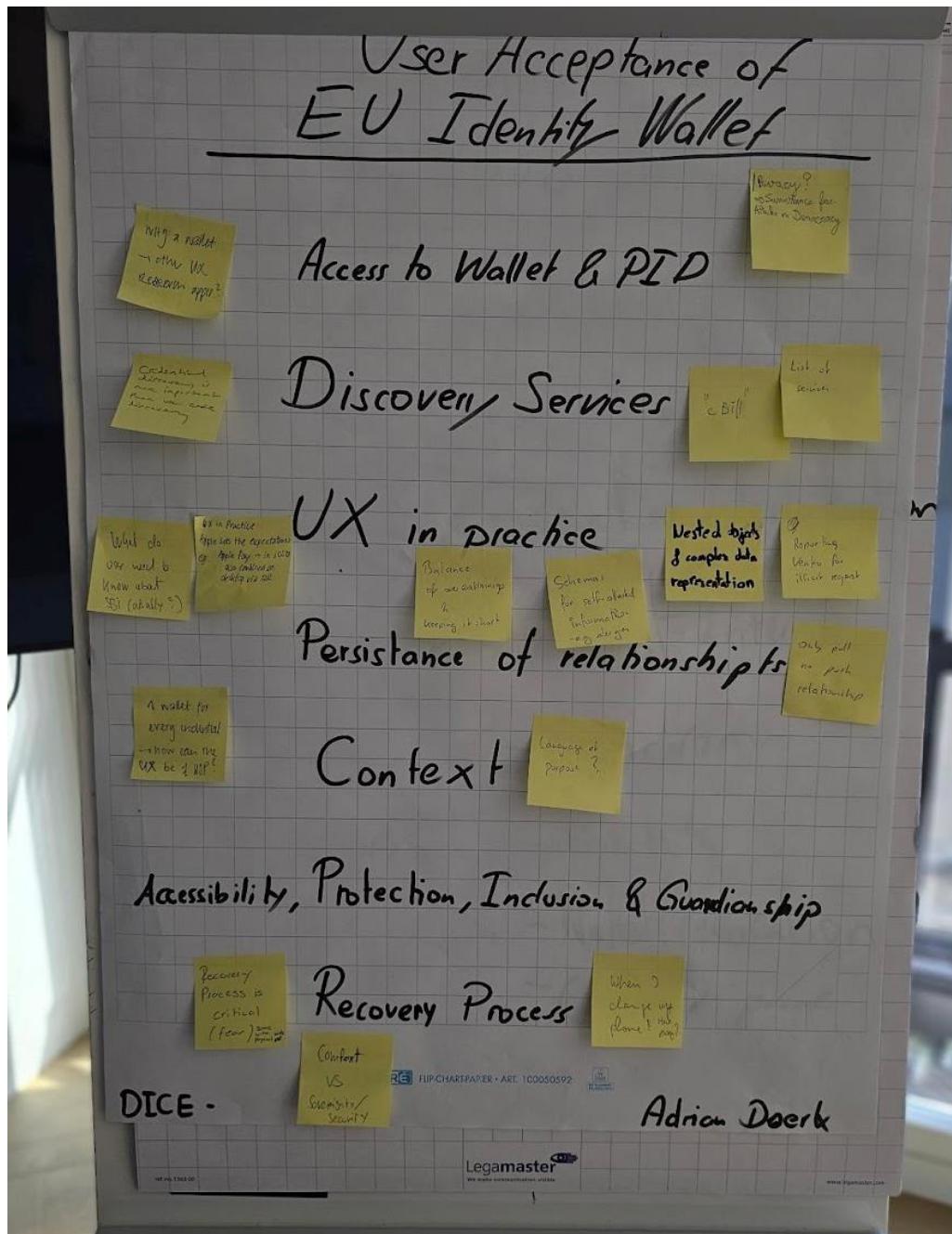
One key conclusion from the session is that the [ToIP Foundation](#) should establish a new task force to write a specification for UX guidelines for human-friendly naming of cryptographically verifiable identifiers.

Session Title: The User Acceptance of the European digital Identity Wallet

Session Convener: Adrian Doerk - Co-Founder Lissi GmbH

Session Notes Taker: Adrian Doerk

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.



User experience focused

Access to wallet and electronic identification mean (PID)

- via notified eID mean in national wallet
- via other nationally available identification service in national wallet
- via european identification service in all certified wallets

Discovery services

- use cases: What can I even do with it?
- Credentials: I need an attestation - where can I get it?
 - Issuers: Who issues such a certificate? Existing repositories

User experience in practice: User guidance and user interface

- Single vs. multi-device flows (QR codes vs. deep links, status displays,
- Linking: backlinks, bounce links
- QR code scan with camera with landing page
- Standardised illustrations for recurring processes (auto-cockpit example)
- Standardised terminology in different applications and languages
- A history of shared information can be viewed from two perspectives: Credential based and organisation based
- Wallet download as a major acceptance hurdle
- Personal profile for self-attested data for easy autofill
- Optional presentation of credentials (e.g. 2 out of 3)
- Option to include digital (PDF) or physical documents
- Execution of GDPR rights
- Multi language support for e.g. purpose of a proof request

Good relationships require persistence

- Push and pull: we need both! With the current ARF, we can only map pull scenarios.
- User-centric interaction history requires recognition of organisations
- Rich relationships require a persistent communication channel

Identity needs context

- Credential exchange alone is not enough
- Additional information (purpose, service offer, privacy information ..) required when requesting information from a user

The protection of citizens

- 800 Pound Gorilla - abuse must be reportable and have direct consequences.
- Consent improvement - Make Terms of Service meaningful
- How can we prevent identity theft and how do we deal with it if it has already happened?
- Tension between user experience and security requirements

Inclusion & guardianship and the protection of those in need

- Guaranteeing accessibility

- Access to the ecosystem with all and without digital devices
- Guardianship affects everyone!

Recovery processes

- Securing the wallet - the "backup"
- Restoring the wallet
- Clarification of the advantages and disadvantages of different methods

General:

Awareness of the solution

- Solution Awareness “Brain Share”
- High bar of expectations from users due to big tech offerings
- Educational / Marketing campaigns
- Solution placement on service provider page

Trust and privacy

- Trust in the security of the Wallet application
- Trust in the protection of privacy
- Trust in organisations that request verifiable data from users
- Trust in politics and the ecosystem as a whole

Education and transparent communication

- Education via various media and adaptation to different target groups
- Information on aspects of security, prevention of misuse, possible applications, risks, etc.
- Restriction vs. freedom for users for the use of sensitive data.
- Differentiation between self-attested and verified data, as well as zero knowledge proofs

Accessibility - How to Design for All

Session Convener: Roman Zoung, Luana Vasconcelos

Session Notes Taker: Roman Zoung

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Managing credential

- Categories with multiple levels
- QR Code are too hard
- Don't autocorrect on bluetooth
- Explicit description of Use case

Security measures?

Delegates Wallet

Representative

Issuer is responsible for Screenreader

Choice command

Joint session: Company Passport & Small Scale Pilots / What if websites were verifiable?

Session Convener: Harmen van der Kooij & Jan Christoph Ebersbach
Session Notes Taker: Jan Christoph Ebersbach

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Harmen shared what the Dutch “Company Passport” program is about and demonstrated examples from Small Scale Pilots that implement “Company Passport” specifications. Company Passport is a “trust framework/ecosystem” on top of e-IDAS 2/ARF (OID4VC as basis) and focuses on how organisations can benefit from eIDAS 2 based wallets and attestations (it doesn’t develop wallets itself but defines specs and involves compliant wallet providers for the actual solutions). Following are some of the organizations that are involved: Dutch Chamber of Commerce (KVK), Dutch Tax Office (Belastingdienst), Dutch Notaries (KNB), ABN AMRO, TNO, Innopay, Unified Post, Digidentity, Sphereon, Animo, Credenco etc

Several of above organizations also present in the room.

Slides: https://dutchblockchaincoalition.org/assets/images/default/CP_Small_scale_pilots_19-6-2024.pdf

Company Passport focuses especially on the functionalities and specs of “organizational wallets” and “organizational attestations” vs “personal wallets” and attestations. Since the EUDI Wallet ARF does not specify much (yet) about organizational wallets and attestations, the stakeholders in Company Passport have started on these specifications (see url below)

The related “Small scale pilots” are all based on the same interop profile(s) and therefore are a showcase of how customers can choose between wallet providers. Harmen demonstrated a live demo in which (web/cloud based) organizational wallets from Credenco and Sphereon interact with OID4VCI based issuers from Dutch Chamber of Commerce and Dutch Tax Office. In the demonstrated pilot also the EBSI issuer trust model is tested as well as the Linked VP spec (see below)

Company Passport Specifications (work in progress → for feedback pls contact harmen.vanderkooij@dutchblockchaincoalition.org):

<https://dutchblockchaincoalition.github.io/CompanyPassport>

One aspect of company passports is to make verifiable data about companies publicly accessible. This aspect is implemented by leveraging the DIF’s [Linked Verifiable Presentations \(linked-vp\) specification](#). Jan Christoph, the author of specification, introduces it to the participants.

The functionality of linked-vp can be applied to many different use cases. The example use case that is presented is the discovery of identifiers and verifiable data when surfing the web. Linked-vp

is used to share company data, e.g. a business registration or trademark credential, and make this information accessible to the end user via a [browser extension](#).

Slides: https://presentations.identinet.io/#240619_DICE_linked-vp

vLEI KERI eIDAS 2.0 European Banking Authority (EBA)

Session Convener: Christoph Schneider (Gleif)

Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

No Notes Submitted

Collating Requirements for a VCaaS (Picking your provider or frame your offering)

Session Convener: Hygiaso AG (Dominik)

Session Notes Taker: Merul

(optional) List of Session Attendees:

Dominik Geller

Josef Sevcik

Merul Dhiman

Ivan Anastasi

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Context

- VC needed for attestation in a Healthcare Use-Case
- Transparent health record is the end goal
- Technology is not the focus of the issuer
- Focusing on swiss and european market

Key criteria

- Standards implemented to avoid lock-in and ensure interoperability,
- Compliance with generally accepted existing standards
- Pricing competitively and sustainably (throughout scaling)
- Verifiable without touching the platform which has issued it (if the issuer dies)
- Archiving capability, longevity of the credential
- Economic and technical stability
- Versatility (can be extended with new technologies/standards)
- Big Tech is entering with their offering, expecting a commoditisation of the offering/shakeout
- Differentiating aspects:
 - Boutique providers exist, yet by definition offerings are converging (standards)
 - Me too offering is good enough because there is more demand than supply
 - Choice on whether device binding is needed/desired
 - Ability to migrate/transfer credentials among wallets

For VCaaS example check -> <https://auvo.io>

Some interesting side discussion on

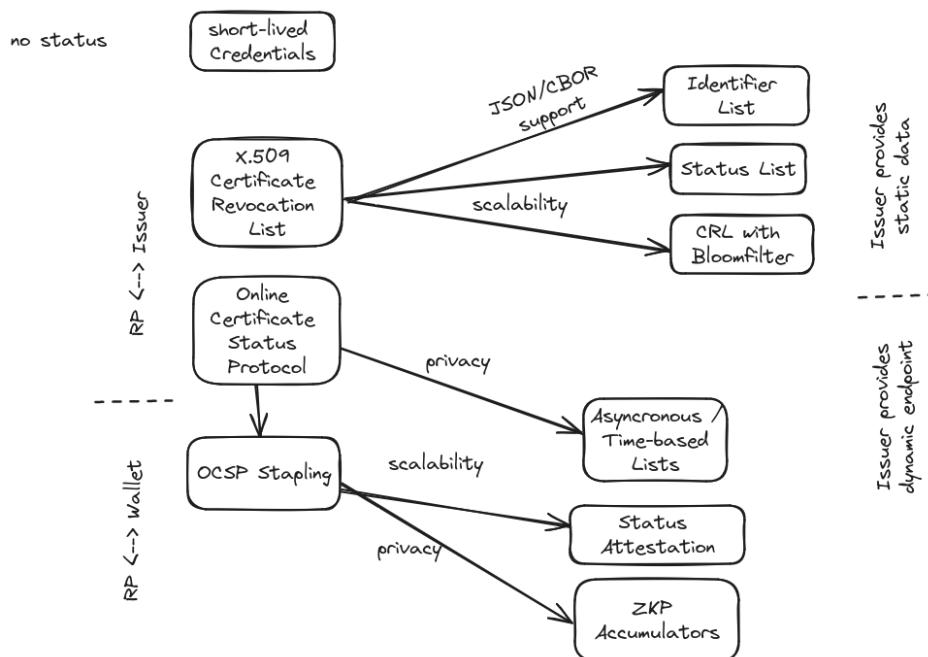
- airline industry and parallels/differences illustrated the complexity of regulated industries.
- VC for attestations on IoT (not only people and organisations have identities and attributes, but also things/devices, which could open a huge new field on assurance around those things/devices).

Revocations / Status Comparison

Session Convener: Mirko Mollik, Paul Bastian
Session Notes Taker: Mirko

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Based on the credential profile comparison Mirko and Paul looked deeper into the status mechanisms since the currently used approaches like CRL and OCSP did not scale well. They looked at different approaches and how they are trying to compare them:



Prior comparison

1: solvable with batch issuance
 2: theoretically possible with malicious issuer
 3: avoidable by daily requesting assertions

	Short lived credentials	Token Status List	Bitstring Status List	CRL	OCSP	OCSP with stapling	Status assertion	Accumulators
Credential formats	any	SD-JWT-VC / ISO mdoc	W3C-VC-DM	x509	x509	x509	potentially SD-JWT-VC	Anoncreds
TRL	10	5-6	6-7	10	10	10	2-4	1-10
Status Tracking by Verifier	None	yes	yes	yes	no	no	no	no
Holder tracking by Issuer	none	no ²	no ²	no ²	yes	yes	yes/no ³	no
Unlinkability	no ¹	no ¹	no ¹	no ¹	no ¹	no ¹	no ¹	yes
Complexity	0	2	2	1	3	4	5	6
Scalability	4	1	1	0-6	3	3*	3	5
Offline/ Caching	yes	Verifier caching	Verifier caching	Verifier caching	?	Holder caching	Holder caching	?

The complexity and scalability values were different to define and the audience was sure that there is not a perfect mechanism that fits for everything. In some situations like supply chains you want to track something and do not care about privacy but a maximum in efficiency.

Paul and Mirko want to continue the work and dive deeper into the complexity part to point out the required resources.

Credential Schema & Layout Standards

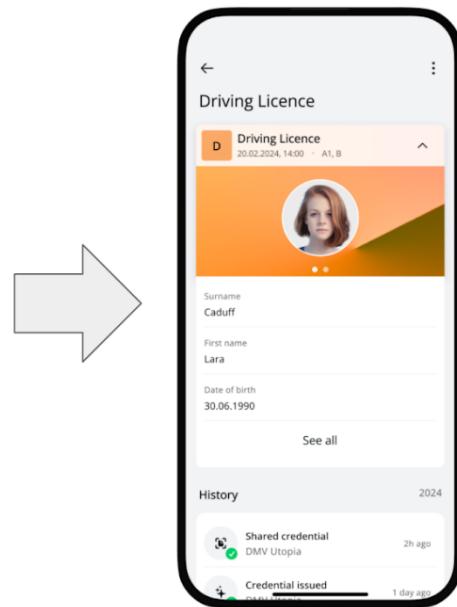
Session Convener: Sven

Session Notes Taker: Sven

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

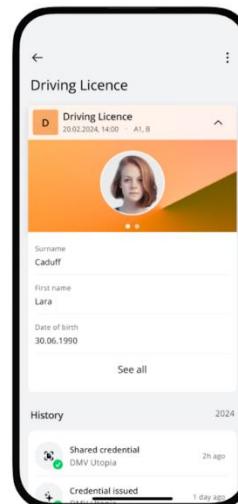
Motivation

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "id": "http://university.example/credentials/3732",
  "type": ["VerifiableCredential", "ExampleDegreeCredential"],
  "issuer": {
    "id": "https://university.example/issuers/565049",
    "name": "Example University",
    "description": "A public university focusing on teaching examples."
  },
  "validFrom": "2015-05-10T12:30:00Z",
  "name": "Example University Degree",
  "description": "2015 Bachelor of Science and Arts Degree",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "ExampleBachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  }
}
```



Dimensions

- Data schema (technical)
 - Structure, namespace(s) of attributes
 - Type of attributes (string, bool, enum, etc.)
- Layout properties (visual)
 - Background images, logos
 - Formatting of attributes (e.g. embedded documents, images)
 - Translations!
 - Challenge: Needs governance



Mdocs (format)

- Identifier: doctype
- No embeddable references for schemas or layout

- Schema for mDL doctype is defined as part of ISO 18013-5
 - However: Implementers tend to use custom doctype with their own extensions, but include ISO namespaces there

VC (format)

- Identifier:
 - Type Property
 - SD-JWT VCs: vct claim ("verifiable credential type")
- Flexible mechanism for referencing/embedding schemas
 - JSON-LD type is a schema
 - No datatypes
 - "credentialSchema" attribute
 - Flexible container for data schemas
 - Could be abused for rendering information as well
- Separate mechanism for referencing/embedding layout
 - "renderMethod" attribute (VCDM 2.0 only)
 - However: marked as at risk and likely will be removed

Other formats

- AnonCreds
 - Schema is published on the ledger
 - Specifies schema and attribute name only

- ACDC
 - Credentials can use (composable) JSON Schemas

Other approaches and standards

- OpenID4VCI
 - "display" property
 - name/logo of issuer
 - name/logo/description/background of credential
 - name of credential attribute
 - Supports localization
- DIF Credential Manifest
 - Standard format to describe credential layout properties
 - No built-in support for localization
 - <https://identity.foundation/credential-manifest/>

References

- Discussion in ARF: <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/arf/#52-available-standardised-formats>
- DIF Credential Manifest: <https://identity.foundation/credential-manifest/>
- OIDC4VCI Display: <https://openid.github.io/OpenID4VCI/openid-4-verifiable-credential-issuance-wg-draft.html#section-11.2.3-2.11.1> (issuer)

Session Notes Day 2 / Thursday June 20 / Sessions 6 - 10

SESSION #6

Ask Me Anything about U.S. Department of Homeland Security (DHS) Digital Credential Infrastructure

Session Convener: Anil John

Session Notes Taker: Drummond Reed

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Anil gave some background about DHS. It touches on all security issues in the U.S. except for defense and healthcare.

With regard to identity, the federal government has a very small role because government-issued identity documents (usually a driving license) is handled at the state level. All the federal level, the only controls are on requirements about the use of state-issued identity credentials in federal facilities, in nuclear facilities, or on airlines.

There no restrictions on how a mobile drivers license issued by a U.S. state can be otherwise can be used or how much a state could charge for its online use.

US Customs and Border Protection (CBP) was the first use of verifiable credentials in the U.S. federal government. The second was the U.S. Citizen and Immigration Service (US CIS) that provide the U.S. green card. USCIS also issues the permanent resident card and the credentials for foreign students studying or working in the U.S.

Those are the highest-value credentials issued directly by the U.S. government.

Anil talked about standards and clarified that profiles of standards are needed in order to actual produce interoperability.

There are debates going on within ISO about splitting out mDoc into its own work. However since the U.S. government does not issue drivers licenses, they won't be using it.

The DHS focus for verifiable credentials is based on the JSON-LD compact form. The reason for focusing on JSON-LD is the semantic understanding of the claims in the credentials. Anil acknowledged that there want to leverage JSON-LD in order to not require centralization and registries for claims and schemas. Anil referenced Nancy Norris of BC Gov as describing this approach as "publish and describe".

Anil also explained the reasons that DHS was using Data Integrity Proofs because they support parallel signatures. Even though the U.S. government does not have needs for selective disclosure—goods or people who want to pass borders must share specified information—but they acknowledge that there are many reasons for using privacy-preserving signatures.

DHS also had to develop a specific API for exchange of supply chain credentials — the Trace API — used org-to-org.

Anil explained that the W3C VC 2.0 standard is using JSON-LD, full stop. Developers who want to use VCs with the U.S. government must support JSON-LD.

The W3C VC 2.0 standard also supports the compact format, CBOR-LD. This is small enough to provide a QR code version that can be presented in person.

Q: What is the U.S. government doing about misinformation and election integrity?

Anil: There is a division of DHS that deals with these topics (CISA) that does focus on these areas.

Q: Can you tell us more about the org-to-org credentials and the Trace API.

Anil: All the specs are published at the W3C Credentials Community Group. The supply chain credentials (“product passport”) are standard W3C VC 2.0 JSON-LD credentials. The CBP then uses a presentation format called a Traceability Presentation so that they can get the data needed to analyse the trade data.

CBP is building their own verification infrastructure internally. All the major players in the supply chain are implementing their own solutions.

Neoflow, Transmute, Measr.io are the three DHS SVIP portfolio companies working on supply chain credentials. Anil said that domain-specific knowledge is very important to vendors in this space.

Most of these vendors are focused on building value-added services because the base-level supply chain VC services are going to be commoditized.

This new VC-based infrastructure is replacing PDFs and SOAP.

CBP also has a “Trusted Trader Program” that enables suppliers to have expedited approval if they are compliant with this digital product passport program.

Q: In Germany, the process is quite complex, requiring a large number of certificates and permits, including of the devices. How does that compare to the U.S.?

Anil: The U.S. has an overall set of security and privacy controls — FISMA compliance — at the infrastructure level and at the application level. But they apply to federal infrastructure and not to all private companies. That is more on an individual case level.

Q: Does the U.S. see the implement of a “federal wallet”? What’s the roadmap?

Anil: Yes, the U.S. will be distributing a free wallet that will also act as a free mobile verifier service. The roadmap is roughly over the next year or two. They are doing this because the market of issuer/holder/verifier services is not “moving forward evenly”. This should help both grow and harmonize the market.

Q: What about interoperability with Apple and Google?

Anil: We will never build to Apple or Google APIs. We will only build to open standards that Apple or Google can decide to support or not.

Some of the U.S. states are entering into arrangements with Apple and Google that are problematic.

There is work going on at W3C led by Apple and Google on wallet APIs within the browser. Anil said it is very important for browsers not to have access to the credentials within the wallet as that would raise major privacy and data control issues.

Q: What other use cases are DHS looking at?

Anil: Travel use cases. Especially for travelers wanting to come into the U.S. — without requiring the use of a U.S. wallet.

Q: What information would the U.S. require for a traveler?

Anil: The same information required for a traveler to enter the U.S. today.

Q: Could it become an EID?

Anil: That is possible. The necessary decision makers in the U.S. government are the ones Anil is working with today (CBP). Anil is not sure exactly how the requirements will evolve. But he believes that if the authorities of the other countries are trusted, it is certainly possible. However it will also involve the context of a particular credential. For example:

- The DID of the entity itself.
- The schema of the credential itself.
- The relationship with the issuer.

Anil said that most of the policy about mutual recognition exists in paper form. If it is recognized that can be applied digitally, that should expedite the process.

Q: How will it affect the visa process?

Anil: The U.S. Department of State and USCIS have a close relationship. They have already done a test of a person using a verifiable credential to apply for a passport, and they saw it streamlined the whole process.

Anil mentioned Sharon Leu, the entrepreneur-in-residence for the Jobs for the Future program. She is focused on digital educational credentials.

Q: Could the notary system help with this?

Anil: Talk to Joe Andrieu. He is thinking deeply about this. It makes sense that we could have digital notaries. Many aggregators and data brokers operate in a similar capacity today.

Q: Is there more info about the Traceability Presentation?

See the W3C Credentials Community Group — everything is linked there.

Q: How about digital KYC processes? Is there a way of validating KYC credential data with DHS?

Anil: There are ways to request info from DHS about specific status info about immigrants or green cards. However we want to get away from the need to “phone home” for verifying this information. Rather you can simply relying on the digital signature on a credential from a U.S. agency. All USCIS issuers will be using did:web to make their public keys available.

Anil recommends the verifiers use Oblivious HTTP to provide privacy for verifier requesting that public info.

Q: Can we use these verifiable credentials from DHS agencies today?

Anil: The first issuance of VCs by DHS will actually be a physical credential — the green card — with a QR code on the credential. That allows a physical credential to be digitally verifiable, using did:web to obtain the public key.

Anil said that DHS will slow move into digital credential issuance.

Anil does not agree with the fundamental assumption of the ISO mDL standard (18030-5?) that digital presentation was necessary. It can work with physical credentials.

Q: What's the future of did:web?

Anil: I like the ideas behind did:tdw very much. He'd like to see some of those ideas rolled into the next version of the DID specification.

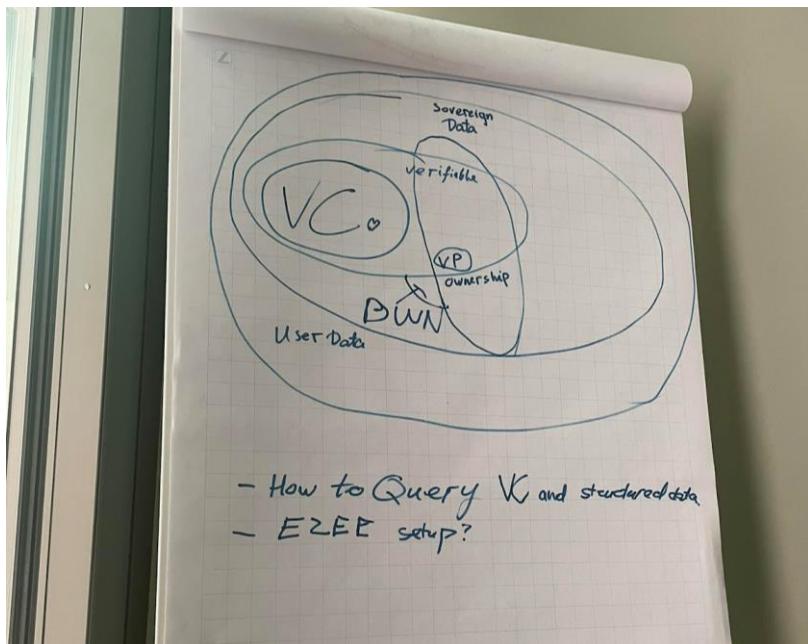
Sovereign Data beyond VC

Session Convener: Volodymyr Pavlyshyn

Session Notes Taker: Volodymyr Pavlyshyn

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Video summary of session 8 min: <https://www.youtube.com/watch?v=imd4Y8C6OuA>



We all love VC, and VC solves a wide amount of use cases but

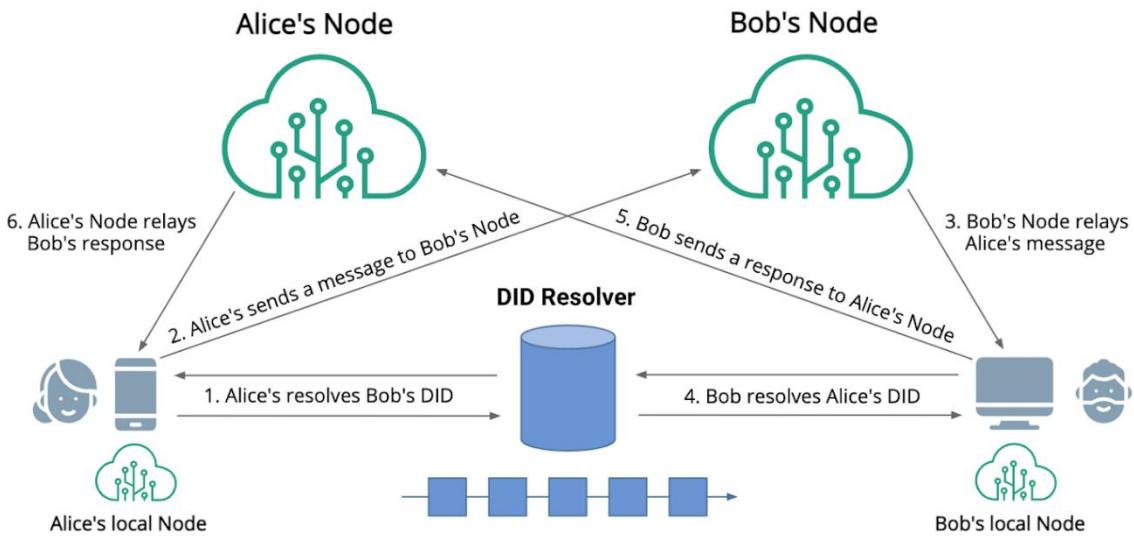
How to query VC that has the max value of some field and how to make smart wallets and smart vault that allow us to do so

I turn the wallet to a database with triple store and sparql

<https://medium.com/@volodymyrpavlyshyn/wallets-verifiable-credentials-as-a-decentralised-semantic-database-json-ld-and-beyond-289167ac2c3a>

Next challenge - how to store a user data that is not in form of VC but still could benefit from Ownership?

We found DWN <https://identity.foundation/decentralized-web-node/spec/> quite useful for this challenge



We were happy with DWN that store any data with ownership and permissions but

We need the ability to run queries on data and DWN does not offer this capability

So we gets back to good old databases !!!

<https://vlcn.io/docs/cr-sqlite/intro>

CRDT Logs + DB allow us to store structured data in a decentralized setup, but we are still working on a secure E2EE sync layer and we need more help

Wallet Attestations in context of eIDAS 2

Session Convener: Paul Bastian

Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Slides taken from: <https://www.kuppingercole.com/get/1530 - 1550 bastian paul wallet security.pdf>

- Discussions around Wallet Attestations in eIDAS 2
- requirements from eIDAS legal text
 - RP needs to verify wallet instance
 - revocation of WSCD
 - revocation of wallet instance by the user
- discussion on proposed concepts from the slides

Verifiable Government

Session Convener: Timothy Ruff
Session Notes Taker: Merul

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Notes best viewed in Markdown :)

link to presentation

https://docs.google.com/file/d/1kO9AVj9x67ncJ5wzr5sD7hxZ8Pd_FFWL/edit?usp=docslist_api&filetype=mspresentation

Verifiable Government

Principles and goals of verifiable government

> on off values might be some governments just want it, however autonomy is a spectrum

Utility	Security	Autonomy	
(on/off)	(on/off)	(dial)	
Usefulness & Flexibility	Zero Trust	Privacy	
Guardianship* & Inclusivity**	Mutual Authentication	No surveillance	
Comprehensiveness	Fraud Prevention	Consent and control	
Portability & Vendor Lock in	Data & Systems Protection	Confidentiality	
Paper & Offline	Recoverability**	Least disclosure	
Adoptable and easy to use	Mutual Auditability	Transparency	
	Recourse		

* Allow delegation of responsibility to someone else when someone is not capable to do it themselves

** Inclusive of visitors, residents and citizens regardless of financial or any other background

*** Systems can't go down

- Shared secrets are detrimental to systems
- Security of any system is only as good as its weakest system
- Average time before someone has been breached is 1 YEARRR!!!
- Identity systems based on shared secret are insecure
- Keri Allows keys to not be mis-used with anchored issuance
- ISO 18013 has a mode which allows to turn on surveillance
- A system which allows someone to just turn on surveillance is a BAD thing

Foundation: Verifiable State ID

3 concepts:

- Guardianship
- State Endorsement of Identity
- Autonomic Identifier -> User-created, User-controller

Example:

1. User brings it's own Identity
2. Organization issues an endorsement with the identifier
3. Added layer of Guardianship if needed

LexDAO x DeScier = JoLE -> Journal of Legal Engineering - feat. decentralized peer review -> call for papers on identity & privacy

Session Convener: Charles Blass

Session Notes Taker: CB

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

decentralized peer review -> call for papers on identity & privacy

target publication date, October 2024

<https://lexdao.org/>

<https://descier.science>

please feel welcome to join and spread the word on a small informal telegram group, where more details will be shared as they become available

Legal identity, proof of identity and responsibility to protect

Session Convener: Maria Gabriela Sarmiento

Session Notes Taker: Maria Gabriela Sarmiento

(optional) List of Session Attendees: ten-eleven people? Kaliya Young, Tim Weingärtner, Grace, Yu..., Marc, Charles B ...

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Introduction to the problem:

What's the key to access basic human rights?

R/ An ID. (A German citizen did not agree, because he is never asked for the ID to access any basic services, because he is already registered in the municipality, in the city, in the state, and that's enough)

You acquire human rights from the moment of conception, when you are a foetus.

However, when you are born, these human rights will be conditioned - by law - to registration.

Birth registration followed by the issuance of an ID makes up what is called by international and domestic laws: "legal identity".

If you do not have an ID, it will become very difficult for you to access or enjoy services related to education, healthcare, nutrition, shelter, social assistance, formal work, etc. This status of "being a person before the law" and possessing a "legal identity" is granted to human beings by States as from the moment newborns are registered, which is followed by the proof of identity these newborns will be granted and that can adopt many forms.

One billion people in the world do not have legal identity. This is a most probably disputed global figure that is around publicly since 2018 (World Bank Source).

International Law does not have a clear definition of what identity is. It is clear though that to be recognized as a person before the law of a country, you must be registered in the official registrar of the country and the State must grant you a legal identity followed by an identification (the proof of identity).

How could a regular migrant end up with no valid document?

These situations occur when the country of origin of the migrant is run by a failed State, by kleptocrats, dictators, autocrats, whatever you want to call it, and for reasons of civil war or external or foreign war, invasion and other predictable or unpredictable acts.

How come there are people out there with no nationality or citizenship who are called stateless persons? Because of political reasons, State discriminatory and exclusion policies, etc.

Why are refugees, forcibly displaced persons and asylum seekers falling into a very vulnerable situation, if there are international conventions out there ratified by many countries that foresee that States should grant a travel document to refugees (also to stateless persons)?? They fall into very vulnerable situations when they lack legal identity and proof of identity, probably because of political issues as well.

Different communities of affected migrants, refugees and stateless persons joined forces to tackle this problem and the vacuum the States have created by not acknowledging the problem and not providing any solutions to it. It is unbelievable that human beings have conditioned the access to basic human rights to the presentation of an ID, and worst, that 1,000,000,00 persons in the world are INVISIBLE to all and cannot enjoy in a similar or equal manner, the human rights that we benefit from.

Apatride Network (coalition of stateless persons in Europe), Coalition 4 Venezuela (USA registered Federation with 100 legal entities as members), The Rohingya Project (coalition of refugees and stateless persons of Rohingya origin in Malaysia) and Save My Identity (Swiss-registered association of Venezuelan migrants and refugees) launched the Blockchain for Human Rights Initiative focused on digital identity and decentralized identity. We propose a community based or a non-State decentralized digital identity to tackle the problem described above. We believe we have to fill the gap and emptiness that the State leaves when not solving the problem or ignoring it.

We thought about blockchain because we come from countries where the authority will alter or modify our personal data or retain our IDs to extort us. We think that with blockchain we could mitigate grand corruption. With decentralization, we believe that we will not have to depend any longer on kleptocrat, predatory and autocrat regimes compromising our personal data and control our identity documents.

Participant's comments:

- On the funny side I should talk about the Tom Hanks movie.
- Check the North Carolina case where there is a special economic zone issuing its own community based identity, they build different regulations for each offshore.
- The right long term solution has to be chosen, and it is not known whether Blockchain will be there forever, because it is an uncontrolled network.
- How do you choose the people who are going to benefit from this community based id? Pay attention to the people who are going to benefit from this card.
- How would you achieve legal recognition of this type of identity
- We have to think what is the future we want to live in?
- We have to think these State institutions will change
- We have to provide community based solutions
- There should be an alternative State type of organization
- There are a lot of movements who would like to finance these types of solutions.
- Biometrics and blockchain are good solutions for this problem.
- What type of content would the ID have?

- Define more clearly what you want to solve, what you want to achieve, prioritize the outcome of what you want to achieve.
- What is your business plan and business requirements to know what technology would be useful or required.

The presentation is pasted in the following pages:



**About legal identity, proof of identity
and the responsibility to protect**

Dr. iur. Maria Gabriela Sarmiento, LL.M

**Digital Identity unConference Europe
DICE 2024
2nd. Edition**

Trust Square Zürich, 20 June 2024



The problem



**Autocrats / Kleptocrats | grand corruption/
failed States** can become a hindrance even if
they are 8,000 kms away from **YOU**

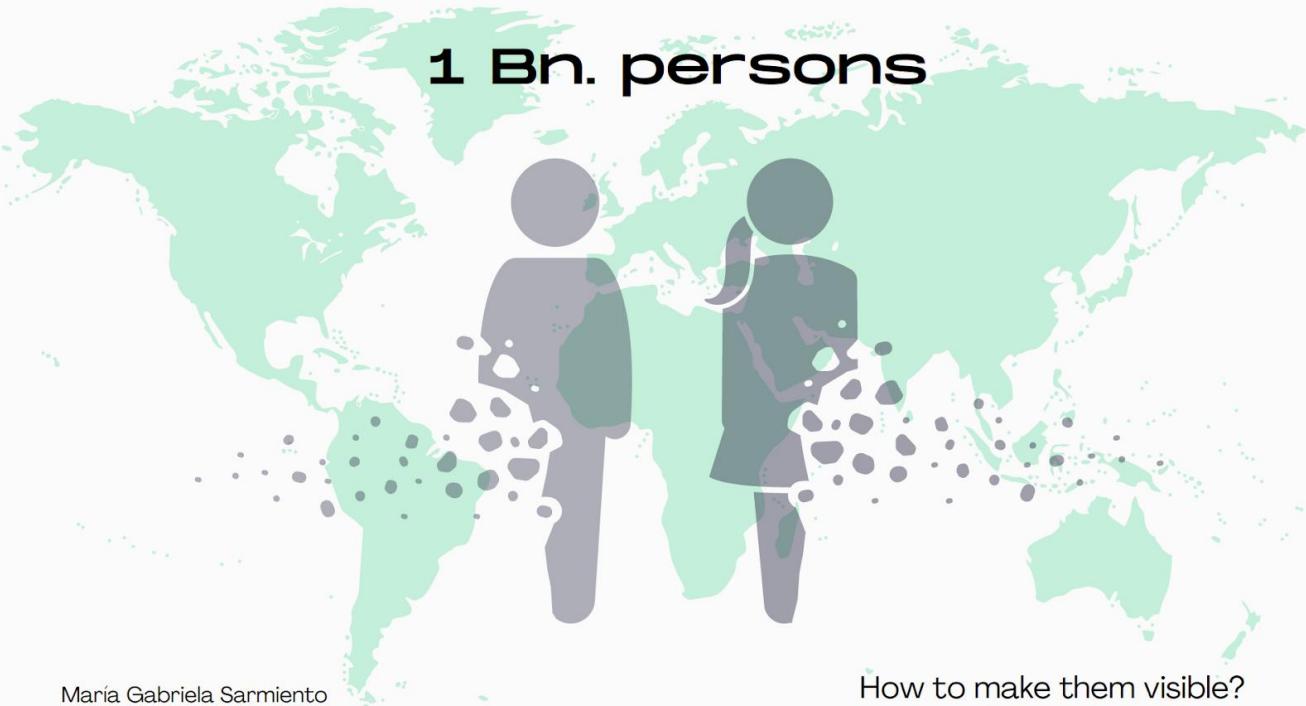
Maria Gabriela Sarmiento



The invisible



1 Bn. persons





The solution



Refugee
Migrant
Stateless person



Public-private organization



BLOCKCHAIN



User

to mitigate
grand
corruption
(extortion)

Maria Gabriela Sarmiento

The partners

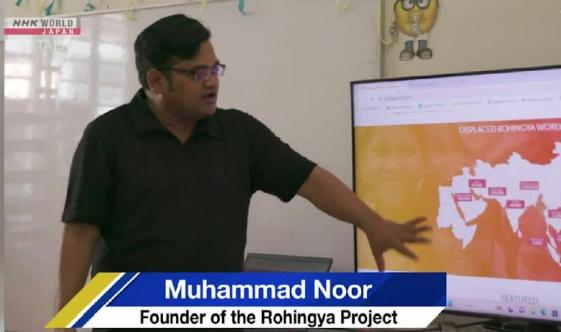
Maria-Gabriela Sarmiento
is a lawyer, vicepresident @ Save M
tity and Senior Legal Counsel @ Sa



Coalition for Venezuela
557 followers
3mo •

te al Catálogo de Talento

¡busca tu talento y Coalición por Venezuela te inv
nslation



Ieksejs Ivashuk and 9 others

The civil society organizations

Nancy Arellano Suarez

Vice-president

Calle Junín 142 of 601, Miraflores,
Lima, Peru

Tel. +51949179924

E-mail:

vicepresidencia@coalicionporvenezuela.org

Web: <https://www.coalicionporvenezuela.org/>

LinkedIn:

<https://www.linkedin.com/company/coalicionve/>

IG: <https://www.instagram.com/coalicionve/>

X: <https://twitter.com/coalicionve>

FB: <https://www.facebook.com/coalicionve>

YouTube: @coalicionporvenezuela



Maria Gabriela Sarmiento

Founder and Vice-president

CH-8032 Zürich, Switzerland

Tel. +41765068087

E-mail: legal@savemyidentity.org

Web: <https://savemyidentity.org/>

Linkedin: Save my identity SMID

IG: @smidvenezuela

X: @smidvenezuela

FB Main Group: Save My Identity Global

YouTube: @savemyidentity



Aleksejs Ivashuk

Founder

Kiev, Ukraine

Tel. +41798464077

E-mail: aleksejs@apatride.eu

Web: <https://apatride.eu>

LinkedIn: Apatride Network

IG: apatride.network

X: @ApatrideNetwork

FB: Apatride Network



Muhammad Noor

Founder

B2-10-M, D'Suria, 68000 Ampang, Selangor, Malaysia

Tel. +60192421874

E-mail: noor@rohingyaproject.com

Web: <https://rohingyaproject.com/>

<https://www.linkedin.com/company/13592154>

X: <https://twitter.com/rohingyapro>

FB:

<https://www.facebook.com/Rohingyapro/>

YouTube: @RohingyaProject





Next steps



Reach out to contribute or collaborate to the Blockchain for Human Rights Partnership.

- Scoping study (of available technology).
- Feasibility study,
- Technology partner,
- Fund raising.
- Pilot project.

Maria Gabriela Sarmiento

Creating B2B ecosystem (Open Discussion)

Session Convener: Douwe Lycklama (INNOPAY), Beau Schellekens (INNOPAY)

Session Notes Taker: Douwe Lycklama (INNOPAY), Beau Schellekens (INNOPAY)

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Reusable KYC VCs Issued by Banks: Banks creating and issuing Verifiable Credentials (VCs) for KYC purposes introduces several advantages:

- Broader Applicability: The reusable KYC product is not limited to financial institutions. It can be utilized by various sectors, thus widening the scope and utility of the KYC process. This inclusivity benefits customers across different industries, facilitating smoother interactions and transactions.
- Support for Small Businesses: Smaller businesses often struggle with stringent KYC requirements. Reusable KYC VCs can simplify compliance processes for these businesses, reducing barriers to entry and fostering a more inclusive market environment.
- The added value of such reusable KYC VCs increases once the KYC process is centralized across the EU. This law has been accepted and will become reality.

Business model for reusable KYC VCs can be:

- Per-Verification Pricing: Charging on a per-verification basis provides flexibility and scalability for businesses. They pay only for the verifications they need, making it cost-effective and adaptable to varying business sizes and needs.
- Reuse of Verification Data: Allowing the reuse of verification data reduces redundancy and lowers costs for both businesses and customers. This reuse can streamline processes, as previously verified data can be utilized for subsequent transactions.
- Tiered Services and API Integration: Offering different service tiers and API checks for reverification caters to businesses with varying needs. Advanced KYC requirements can be met through higher-tier services, ensuring that all businesses find suitable options within the platform.
- Identified gaps in eIDAS concerning the B2B space: Authorization for delegates, administrators, and empowered individuals.

EUDI Wallet Adoption: Discussing the potential low adoption rate and the need for compulsory measures to drive adoption. Identifying key players in the ecosystem like tax authorities and universities.

Other notes

1. Verification as a service is a clear role in the b2b ecosystem. Not much attention is given yet to this side of the market
2. We will have a AML-A credential for opening accounts, in April this law will pass
3. The “Queen Bee effect” will drive the adoption of ecosystems, bootstrap ecosystem, break chicken and egg problem —

4. Centralised issuing vs decentralised technology. The tech is decentralised, while the trust and legal certainty is organised centrally (through laws and regulations)
5. Credentials for skills are a business case where historically quite some effort is being put in. Check out NGDIL.com project: verifiable credentials in education.
6. Law firm Fragamen at EIC using verifiable credentials for their immigration services, the 'posted worker' directive can also work as wallet
7. Vida: how to prove the invoice comes from a real company ? Tax authority will require this , vLEI can be a good use case

SESSION #7

Looking for Issuers Verifiers on ‘Swiss’ trust Infrastructure

Session Convener: rolf.rauschenbach@bj.admin.ch

Session Notes Taker: rolf.rauschenbach@bj.admin.ch

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Preliminary remarks by the e-ID-team of the Swiss government

- During the next participation meeting on July 4, 2024, 4-6 pm, important announcements will be made with regard to the sandbox 2.0, available in the beginning of 2025. The quality and functionality of the sandbox 2.0 will be considerably higher than the current “Public Sandbox Trust Infrastructure”. It is recommended that potential issuers and verifiers tune in, as it might make sense to experiment with the trust infrastructure as soon as possible.
- The E-ID-team is aiming to have the following VCs/issuers ready at launch of the e-ID:
 - Federal Office of Police: e-ID
 - Federal Office of Justice: criminal record
 - Federal Office of Social security: European health insurance cards, form A1
 - Federal Office of traffic: ePDL, mDL (not yet ISO-compliant)
 - Cantonal Debt registries: debt registry
 - Municipalities: Residence certificate
- The E-ID-team is aiming to have the following verifiers ready at launch of the e-ID:
 - AGOV (login of public authorities, including health record and registry for the donation of organs)
 - At least one trust service provider (qualified electronic signatures)
 - At least one bank (opening of a bank account)
 - At least one telecom-provider (subscription to a mobile-plan)
 - At least one merchant of alcohol and cigarettes (age-check)
- Other issuers and verifiers are more than welcome to join the effort to use the trust infrastructure. Due to constraints in resources, the e-ID-team will however not be able to provide substantial support towards these efforts. For questions or if you wish an introductory meeting with a representative of the e-ID-team, contact rolf.rauschenbach@bj.admin.ch.

Q&A The main part of the session was a Q&A

Transcription of the flipchart

Issuers

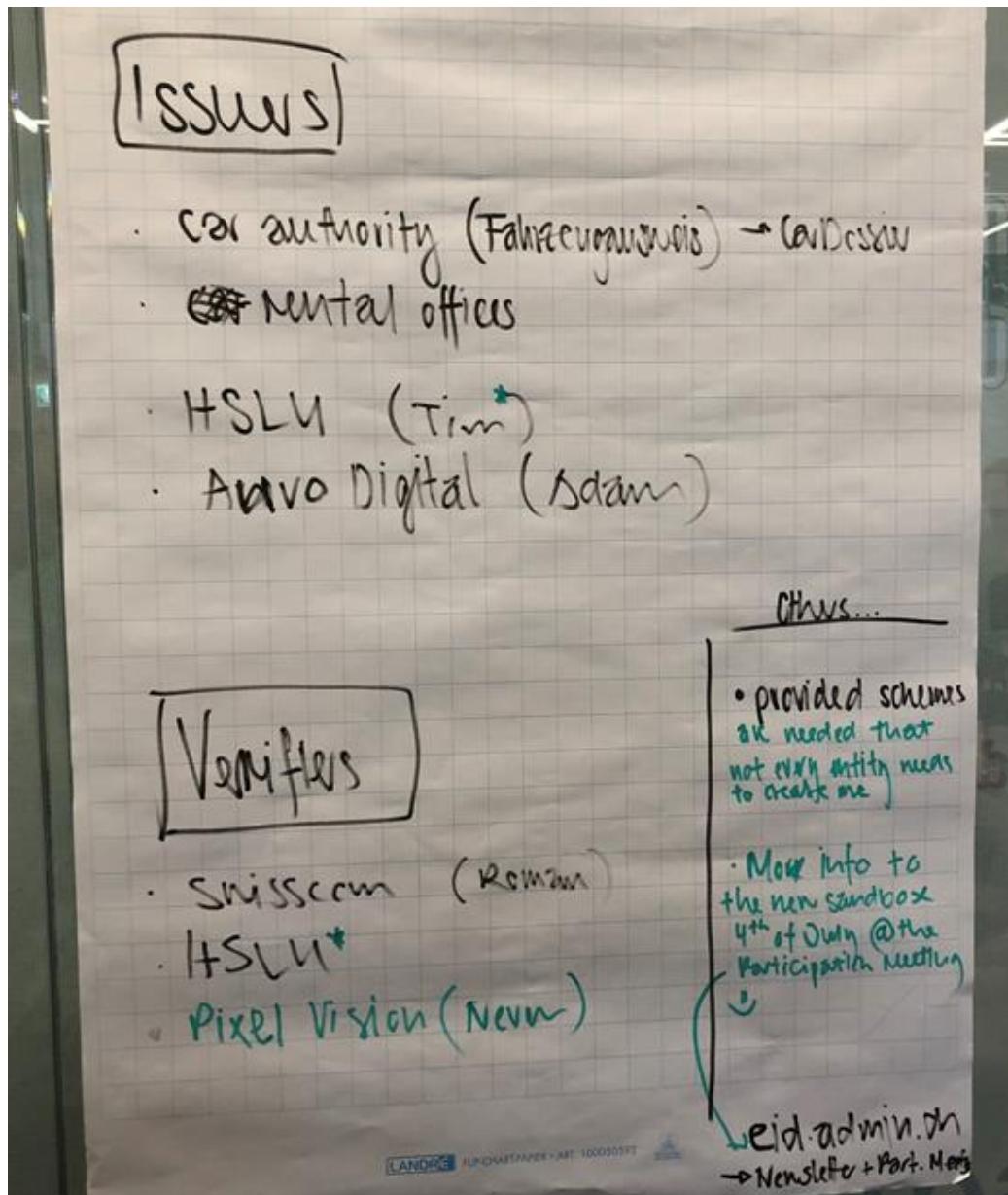
- Car authority (Fahzeugausweis), car-dossier
- Rental offices
- HSLU (Tim)
- AUVO Digital (Adam)

Verifiers

- Swisscom
- HSLU
- PixelVision

Other remarks

- Provided schemes (not everything needs to be created new)
- More information on the sandbox 2.0 during the participation meeting on July 4, 2024
- www.eid.admin.ch



Challenges in Designing Alonecasting Ecosystem

Session Convener: / Stefan T.

Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

No Notes Submitted

Duplicity Evident

Session Convener: Samuel M. Smith

Session Notes Taker: Henk van Cann

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Link to slides:

https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI_DuplicityDICE2024.pdf

KERI-light not possible if not dangerous

KERI is system, you can't take things out. It'll be insecure.

So view KERI as the minimally efficient system.

Ambient verifiability -> not yet done in KERI! (It's too early, we're in the bootstrap)

Force detected compromise -> Duplicity evident

Attacks

The reason people attack is incentives: ransomware

If you can detect in Milliseconds, and then recovery (you automatically rotate) in Milliseconds and not in a year (!) the incentive to attack is gone.

Sam explains slide 1 to 5, the conclusion:

KERI's innovation -> proof of keystate

The HARD Problem that remains: alternative key state or duplicity.

Cryptographic agility in KERI means we can upgrade the cryptography over time; WITHOUT CHANGING THE CODE. That's why we had to invent CESR.

Pre-rotation means non-repudiability of any statement / data anchored in the KEL (via a seal)

No ambiguity in KERI, it's duplicity evident, that's a richer concept.

Inconsistency : about the data Duplicity: about the actor and provable.

Question Timothy Ruff:

If the attack is focussed on the controller, could he impersonate as the controller:

Answer Sam: Yes, if there's no 2nd factor between controller and witness.

An attacker:

1. Can only get control over an interaction event
2. They can't do it if the controller has a second factor with the witness (example 2nd factor: secure channel)
3. They are NOT ABLE to attack an establishment event, because they don't have the

Sam explains the duplicity game.

The only attack possible on an agent is a DDOS attack

Breaking the promise of global consistency is a provable liability (of Cate)

The role of Qualified Trust Service Providers under eIDAS 2.0 - EU Regulation 2024/1183

Session Convener: Jörg Lenz, Steffen Schwalm, Adrian Doerk

Session Notes Taker: Adrian Doerk

Find the relevant legislative text here: <https://eur-lex.europa.eu/eli/reg/2024/1183/oi>

Qualified trust service provider: Offer services such as the creation of qualified electronic signatures, seals, or timestamps, which are certified and classified as "qualified" according to eIDAS. The QTSP is always responsible to provide evidence of their processes and take over responsibility for their services.

Existing trust services

- timestamps
- Validation of signatures
- Preservation
- Seal
- Signature
- Delivery
- QWAC

New trust services under eIDAS2:

- QEAA - Qualified electronic attestation of attributes
- management of signature creation device
- Archiving
- qualified ledger

The market:

- There are around 250 QTSPs.
- Spain, Italy and France do have the most QTSPs
- Industry trend “Trust service as a Service”
- Big organisations tend to buy smaller QTSPs
- ETSI 3 19 401 incorporates NIST2 requirements
- Many QTSPs want to see more harmonisation across member states
- possibility for differentiation
- planning security is essential for investments - and this is not given for a lot of aspects

Changes & opportunities:

- use a QEAA (in or outside the EUDI-Wallet) for personal identification
- usage of PID cost savings
- market expansion with higher frequency of QES
- new market opportunity with QEAA issuance
- It's unclear which QTSP will provide the QES to the nationals EUDI-Wallets
 - We expect Bundesdruckerei / D-Trust to provide the QES for German wallet(s)

When offering a government service (e.g. municipality) you need to support:

- Any EU-Wallet
- Any Qualified attestation (QEAA)
- Any Signature (QES)
- Any Seal
- Support issuance of QEAA

Outlook:

- Waiting for more details from ARF and the 42 implementing act
- setting up the new Large Scale pilots
- ENISA trust service conference - 25 - 26 Trust service forum - focus on regulation
- CEN / ETSI Conference also in beginning of September, which is more focused on technology

Challenges / open questions:

- QTSPs are required to offer natural citizens with a qualified electronic signature for non-professional purposes

This might be inspired by Austria - where the taxpayer is paying for the service, which is provided by A-trust.

Privacy and Unlinkability with and without ZKPs

Session Convener: Stephen Curran

Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

More notes to come, but here is a link to the [slides used to facilitate the discussion](#).

Great discussion and thanks to all that contributed!

Dreams and Nightmares: Real Talk combined with Beyond Statist ID

Session Convener: Kaliya Young + Matthew Schutte

Session Notes Taker: Group (add yourself if you contribute to the notes)

(optional) List of Session Attendees:

charles blass - Matthew Schutte - Kaliya Young - plus

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

4 paths

1. China Surveillance State/ India (aadhar) (sort of China light)
2. Surveillance Capitalism
3. Crypto Anarchy,
4. SSI - decentralized, IPFS, Coordi-nations

Notes from Casey Below:

Why we're here:

- learn
- important questions
- philosophy
- big picture
- so what? why are we doing this?
- what keeps people up at night?
- big overview
- finding the lesser of 2 evils
- worry about the uber-identifier
- how do we see the impending nightmare and bring about something else?
- this is the interesting stuff, it's the shadow side of things

- how do we find the middle path?
- the technologies that we're building have dark potential
 - how do we bring about the light side?
 - IIW was started out of asn.planetwork.net; how do I represent myself in these spaces and not have my identifiers controlled by these corporations and governments?
 - should I keep working on this technology?

4 box matrix for how things will ultimately turn out, all in field of play right now

top-right: Chinese surveillance state

top-left: Surveillance capitalism (pervasive and dead-end, not good)

bottom-left: Crypto-Anarchist Liberalism

bottom-right: SSI, Decentralized Identity, IPES, DWS

Cordi-nations, how do we get civil society to use this tech that hasn't nothing to do with governments? With VCs we get to issue them and use them and come up with the reasons for why and what we do with them? We can actually do creative things with this technology.

Can we get beyond Statist-ID?

Are we heading for nightmares or dreams?

We split out into groups of 2-3 and talked for 10 minutes, then reconfigured the groups and did it again. Then we reconvened for further discussion.

- SSI spirit is morphing into a more centralized issuing. Can we have a parallel system where attributes are community-driven? An SSI system could be used to understand what others are thinking and/or doing?
 - Can it dispel collective illusion?
- TESCREAL? Trans-humanism... Look it up :)
 - TruthDig has a piece on it. Timnit Gabru argues that it's about eugenics. Crypto-anarchists
- Book: The Every from Dave Eggers; a look at a world where everything is verified
- Our current states are formed in a way to exploit part of our nature that is egocentric, but we also help each other. How can we encourage this part of our nature?
- Violence and Discretion: Discretion is hard but tech could help us do the discretion part better. Sharing things, private/public. Everything seems anchored in violence now. Seduction around scale that is pervasive, it's also important to engage with neighbors and there are important things going on to ME that is not at scale.
- What is the meaning of freedom in a living system? My body's regulatory system keeps things in check ahead of time; regulation is different from enforcement. We've been misusing the term "regulatory system". Even in mechanical systems there are "governors".

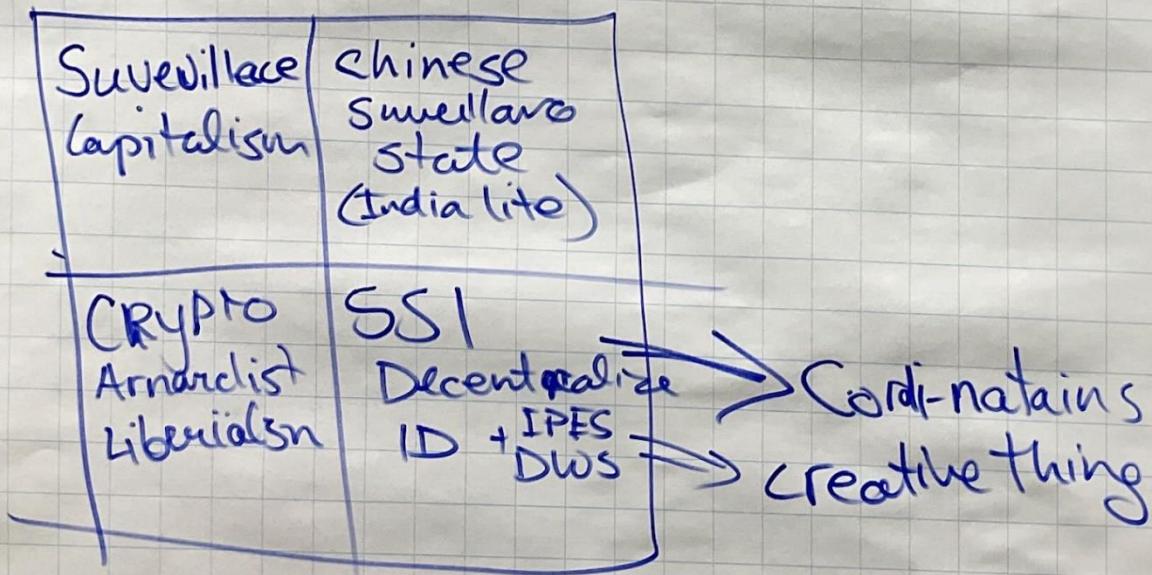
- learn
- important Questions
- philosophy D&N
- Big Picture
- So What?
- what keeps PPI up @ Nig
- Big overview
- Are D&N common
- Less 2 Evils
 - Have nightmare
 - ↳ Bring opposite
 - ↳ Follow law but not just
- interesting stuff Shadow
- The middle wall "third attractor"

Dreams & Nightmares w/ ID

Beyond "Statist" ID

Relying Party check if my wallet is "attested"

asn.planetwork.net



TESCREAL

-> eugenics

cf. Timnit Gebru, Emille Torres

OPEN ID Federation

Session Convener: Maarten Boender (Sphereon) and Timo Glastra (Animo)
Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

References:

OpenID Federation 1.0 - draft 36

https://openid.net/specs/openid-federation-1_0.html

Authlete - OpenID Connect Federation 1.0 overview

<https://www.authlete.com/developers/oidcfed/>

Connect2ID - OpenID federation and trustchain explained:

<https://connect2id.com/learn/openid-federation>

Davide Vaghetti (GARR) - eduGAIN OpenID Federation POC

<https://indico.cern.ch/event/1325302/contributions/5753884/attachments/2790679/4866600/eduGAIN%20OpenID%20Federation%20POC%20-%20FIM4R%20Copenhagen%20TIIME.pdf>

Findynet OpenID Federation implementation status sharing to external stakeholders

<https://findynet.fi/en/news/oidf-3/>

Findynet OpenID Federation implementation status events

<https://findynet.fi/en/news/oidf-4/>

SESSION #8

Self-Sovereign did:web

Session Convener: Jan Christoph Ebersbach

Session Notes Taker: Jan Christoph Ebersbach

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

This is a presentation about a new open source service called did-web-server that was recently developed. The service is focused on making the did:web DID method more self-sovereign by enabling DID holders to update their DID documents using just DID and Verifiable Credentials / Presentations. No legacy shared tokens (JWT) or passwords are required.

In the session multiple ideas for extensions were discussed, e.g. adding support for VC status lists, Linked Verifiable Presentations, support for did:tdw - another did:web based DID method.

Slides: https://presentations.identinet.io/#240620_Self-Sovereign_did-web

Trust Statement Standardisation

Session Convener: Michel Sahli

Session Notes Taker: Michel Sahli

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Not a lot of people showed up but we could conclude that an organisation has to be verifiable as a statement and their action should be described and machine readable. Next step in the group will be to create a first concept of a syntax to describe organisation and actions.

ge-Scale KERI Network Design

Session Convener: Martin Burkhart ([Cyber-Defence Campus](#), Switzerland)

Session Notes Taker: Martin Burkhart

Many, including Sam Smith (KERI), Judith Fleenor (ToIP), Philippe Page (HCF), Mike Doujak (Ergon), etc.

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Lucas Falardi presented the intermediate results of his master thesis. The goal of the thesis is to design a potential Swiss E-ID base registry architecture based on KERI. Slides are here: [Link](#)

Challenges:

- decentralization (KERI) vs. centralization (Swiss E-ID infrastructure)
- Complexity: Which components of a full-blown KERI network are needed and why?

We don't need global consensus, but just a sufficiently large segment of the network without duplicity. The jurors detect different KEL versions between watchers.

All sectors should run their own watcher pools. A user of the future E-ID will have to configure the set of trusted watcher pools - or use a public service, a “**super watcher**”, that watches the watcher pools (those that are state provided and those from industry).

Follow-up question: Who runs the super watchers? It could be anyone. We could also use a ledger as a watcher.

HCF: **Running a watcher pool requires governance** and has some reliability implications.

Legal implications: Could a citizen be reliable for actions based on duplicitous events? Maybe the state should guarantee that users can't be taken to court if they are using/trusting the state-provided watchers.

How about privacy: The witnesses and watchers in the central infrastructure are all run by the state. So the state could correlate all the information. That would have to be addressed. One could introduce a proxy watcher that watches the state watchers for the citizens.

A fundamental problem is that actions can be observed and tracked on the network (IP) layer. So anyway, there must be some kind of a mixnet/TOR service in between. **Privacy is agreed to be a difficult problem and has not been addressed in this thesis.**

The trust spanning protocol (TSP) specified by ToIP could help.

Lucas: Scaling KERI would require CLUSTERS of trust. One cluster could be the state, another could be a foundation. But then the user has to choose. For the E-ID: How can an average (non-nerdy) user make this decision?

Implementation: There is a Rust library (from HCF) and the Keripy library by the KERI team. Why are there two implementations? The licence is different: EUPL for Keriox, Apache2 for Keripy. HCF had a rust-based infrastructure already.

ToIP could serve for discussing technical and governance topics around KERI and the ecosystems.
There is already quite a lot going on.

Consensus Building

Session Convener: Drummond Reed / Henk van Cann

Session Notes Taker: Henk van Cann

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

All slides with notes: <https://drive.google.com/file/d/1sD5tS9Jm-Q5fc6nOdz9eLqDVBy8GwCLL/view?usp=sharing>

<https://github.com/trustoverip/ctwg-main-glossary> repo

<https://github.com/blockchainbird/spec-up-t>

<https://trustoverip.github.io/ctwg-main-glossary/> Spec-Up-T based glossary

KERISSE.org : Docusaurus based Glossary (Documents -> Glossary)

AMA - Holochain = a free, open-source framework for building peer-to-peer applications. / Matthew Schutte

Session Convener: Matthew Schutte

Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

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

VC-Catalog for non-public vc

Session Convener: Roman Zoun

Session Notes Taker: Peter Janes («Piet»)

(optional) List of Session Attendees:

Timothy Rabozzi - Marcel Eichmüller - Dominik Geller - Lara Schwab - Adrian dork - Ivan

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Discussion

- Focus on **semantic** interoperability
- Coordination driven by [DIDAS Adoption Group](#)
- [VC-catalogue governance](#) currently being drafted and discussed
- Driven by specific use cases «as needed» (no definitions in advances)
- Nothing new - data modelling has been around for many years
- VC-catalogue is an application of existing practices, applied to VCs
- Existing standards are used where available, e.g. schema.org, <https://hl7.org/fhir/> (health), [openEHR](#) (health)
- Use case examples - certificate of residence
- Organizational ownership DVS (Digitale Verwaltung Schweiz)
- Envisaged platform [I14Y](#) (planned to be migrated to [Lindas](#))
- There should be an official place where relevant schemas are published (and where interested parties are looking for schema definitions before defining their own schemas)
- Schemas should be machine readable
- Relevant for credentials used outside the own organization, i.e. relevant to multiple parties
- Strict schema versioning is prerequisite - relevant schema version must be available while dependent VCs are in effect
- VC-catalogue initiatives are not yet defined in the EU space

OID4VC - Advanced Topics

Session Convener: Oliver T and Paul and Christian
Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

No Notes Submitted

Discussion on Binding Users, Holders, Subjects

Session Convener: Peter Langenkamp
Session Notes Taker: Maarten Boender

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Opening statement introduced the concept of binding mentioning 4 types of binding:

- Device binding
- Wallet binding
- Holder binding
- Subject binding.

The ARF 1.4 only specifies Device binding using WIA and WSCD, but not to Holder or Subject.

Device binding.

[Note MB: During Session 6 (Wallet attestations) Paul Bastian and Torsten Lodderstedt explained why WIA and WSCD for wallet binding is simply not enough).

Peter Langerkamp mentioned that in The Netherlands particularly the banks are nervous and unhappy about just Device Binding: currently the banks have control over users because they use the bank's apps. They do not like to lose that control and are pushing for holder/subject binding.

The possibilities of Holder/Subject binding using biometrics were discussed, either leveraging the OS-native functions or storing them in a WSCD. Concerns were raised if this would be acceptable (for the users).

Circumvention of these bindings were discussed. Giving my pin or password or phone to my partner/neighbour/spouse/etc. is done today and can hardly be prevented.

The insight from the discussion was that these circumventions are acceptable as they are basically giving consent to another person, a form of explicit delegation.

Another complication that was discussed was about people wanting to have multiple identifiers: for official use, for their social presence, for gaming, etc. and/or using multiple devices.

Technologies such as Selective Disclosure or ZKP were discussed, but some participants agreed that these by themselves would not prevent correlation and as a result the possibility of tracking.

An insight was shared, unrelated to the topic, but interesting nevertheless, that in the past Relying parties were free to decide what data to ask for and what format they were willing to accept. They had that freedom and that control. With eIDAS2.0 this is no longer the case: they will be obliged to accept eIDI Wallets.

Will this shift the issue of liability? Will that depend on the context/use case? Or on specific RPs depending on their governance rules set by regulators?

About the context/use cases it was discussed that there will probably be various levels of risk that will lead to rules on what RPs must or are allowed to do. For instance:

- Voting is seen as most sensitive and will be highly restrictive and regulated
- Banking less than voting, but still highly regulated
- But buying alcohol or visiting a club will be much less regulated.

Lastly it was discussed that non-qualified Issuer (non-QEAs), so EAAs, are not required to register within a Trust Registry and that a Holder is free to accept a data sharing request from a non-registered EAA (issuer). This can lead to several risks:

- Over-asking
- Phishing attacks
- Fraud

How to protect users?

Some remarks were made that this is happening today as well. The over-asking with Cookies on websites, organizations and hotels making copies of ID-documents, etc.

Participants felt that this was one of the main reasons behind eIDAS2.0 and these kinds of 'abuse' would be reported and would be stamped out over time.

Identity, Social Media & Democracy

Session Convener: Yuting JIANG

Session Notes Taker: Yuting JIANG

(optional) List of Session Attendees:

Nicolas Gimenez, Gabriela Sarmiento, Charles Blass, Grace Rachmany, Marco Luthi, Adam Eunson, Merul Dhiman, and more

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Disinformation on Social Media

- Fake news, Troll farms and keyboard armies
 - This could be solved with identity verification. For example, Bluesky.
- However, official newspapers are biased and manipulative, because they only tell you what they want you to know. "Selective disclosure" of reality. Even education, culture, and religion are often "manipulative" - they teach you what to think, rather than how to think.
 - Maybe we could provide a better UI to make it easy for users to see and provide the source of information for each post.

Anonymity on social media

- Pros
 - It's like the "old days" of the internet, where people care more about exchanging ideas & information than showing off.
 - Anonymity protects vulnerable people, including minorities and women, to speak out. Whistleblowers too. It's important for freedom of speech.
- Cons
 - People are more mean because they can't be punched in the face -> no accountability.
 - Spam
 - which could be solved with verifiable anonymity

Anonymity seems to have a bad reputation, as most low-quality content (including spams and trolls) is generated from anonymous accounts. Having verifiable anonymous accounts (with anonymous proof of personhood, etc) could help prevent repeated posting from different accounts.

What matters the most is the intent -> are you using anonymity for protection, comfort, or malicious intent?

Moderation

- Karma may be used to bully those whose opinions differ
- Decentralise Moderation: **Slashdot: Concentrate more on promoting than on demoting.**
<https://slashdot.org/>
- Sanction vs Regulation

- AI moderation is very limited

We'd like to drive a cultural change on people's behaviours on social media

- agree to disagree
- intent matters
- always check the sources

Book to read: Plurality by Audrey Tang



SESSION #9

Funding Community Organizations & Community Work/Leadership, a discussion about what is working & challenges

Session Convener: Kaliya Young Identity Woman

Session Notes Taker: Gabriela Sarmiento

(optional) List of Session Attendees: Charles, Grace, Stephan, Yuting, eight persons (three female participants) plus Kaliya.

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

FUNDING COMMUNITY

There are a lot of ideas about community driving.

Who would be supporting the implementation would be interesting to know. Stephan.

Collectives, cooperatives, communities, we should call it more. Charles.

Blockchain world has been looking for funding mechanisms.

Finding partners for collaboration. UK. Who is doing what? What are they doing? How could we work together? These are things which are difficult to find out.

We need to get resources, we need to get partners, actually it is all about money.

Yuli wants to learn from this group, and is trying to run a startup.

This is where the cookies are!!!!

I work with community CCG, co-shares, etc. and maybe I could be a co-share but have no time for that, I am a socialist

Money, getting money, fundraising ... I want to go into the verbs and the emotion, the narrative in the fundraising is important, but the community gardening of the conversation is important for him and the community memory for the story telling of the community.

A participant is a founder of a NPO project. He is talking to big tech companies and he needs legal support.

We are thinking of a foundation of 500 members with 20 funding members. Is being funded by a very small group of people.

There are different funding models, and structure models, I will name some of the models

- CCG Credentials community group Is a community group not making standards, it meets once a week, it has three co shares, it has critical infrastructure for VCs, and is vibrant. Is not that time intensive, is 3-4 hours a week.

- OpenID Fnd

We have two models:

- There are all volunteer groups, resources only group. We are not captured
- We do everything with money. We are captured.

There should be a third model with a business model partially financed by third parties.

I am great at writing grants in how I speak to influence the government or I convince the NPOs to get funded.

If you use our technology you get funded.

We learned about a grant in the European Commission called Next generation internet. a 10 pages proposal with special format and resource allocation and a business model developing an idea on how the project could be sustainable, and we applied as natural persons. 100K. This saved us from pitching to investors. We submitted directly twice, and the third time we applied as a company and then we got it.

There are other programs between 0-50K in the Next Generation Internet of the EC.

THE HUGE GRANTS require the academia to be involved.

How much you can raise is an issue.

In both grants you have deliverables, managing the grants ends up being the work you are doing instead of the work of the foundation. Then this is not the greatest way to go.

Well, a year grant is manageable.

The EU Horizont Projects are resource taken.

In the UK they are not that difficult, they are more flexible, but if you do not comply or show the impact of your business, then you do not get funds again.

It is better to get these grants instead of having private investors.

In the tech industry we are all focusing on the same donor. CA o CIA there are corporate consortiums that are in standard development spaces. W3C is an international STO.

Personal pinpoint of Judith: decentralized identity foundation Judith we started collaborating and OpenWalletFoundation came up and all the funding went to the OpenWallet Foundation. It was confusing and very bad.

Working Groups Chairs and WG contributions by members should be created.

After a year of conversation there were enough differences in the funding models of both foundations and fiscally it was not good to merge both foundations, for tax wise reasons.

Do fundraising like gofundme, do paid membership fee,

Linux foundation was god for reputational reasons but there was an issue (I could not write....Judith comment)

Is there a cross foundational working group???? Yes, there is.

Is all about conversation and realising that a story was already told ten years ago and then we work together through MoUs. Now they point to each other. Are they still alike? Do they work together? NO.

In THE WG for digital wallets and another WG is a formal procedure that has to happen to connect two or more WG. These WG are generally unfunded.

The W3C staff responsible for the DID WG proposed Kalija to co chair the WG but KY cannot work unpaid and there is a challenge for KY to work self-funding.

Relationships are very important In this industry.

The individual people are fragmented, ending up in the wrong place because that one pays them.

The crypto industry gives funds. The Ethereum foundation is financing some of my events.

The crypto have too much money, some of that money should have more continuity

Community plus communication is the BASICS. It has to do also with moderation, leadership, posting, internal communication, fund raising, and so on.

If you have a project which conflicts with another project, then they do not want to help the previous project. There are conflicts of interest.

There is a parallel society that we want to create that respects the way we want to live. Take care of each other. We got our own money, not taxable money, etc. The voice of Humanity Ethereum Foundation is going towards a place where we project each other independently of the money we could raise.

The movement back in the 60s they were making music, living in a different way, we should learn from them,

Culture and Technology, Democratic Surround books, American democratic propaganda, academic movement,

Stephan's idea: Create a DICE "lion's den" where you pitch a concept or business idea. Add maybe 20 francs to the DICE entry fee and put that towards funding the pot. This could make a pot of 5-10kCHF (possibly including the event sponsors). The grant(s) themselves may be more important than the money, as being able to claim a grant from a community like DICE can attract significant other grants.

The most funded projects are the ones that create more money. It is about telling the right story to the right crowd. Republicans and Democrats want to fund the Fire foundation?

We are competing with each other.

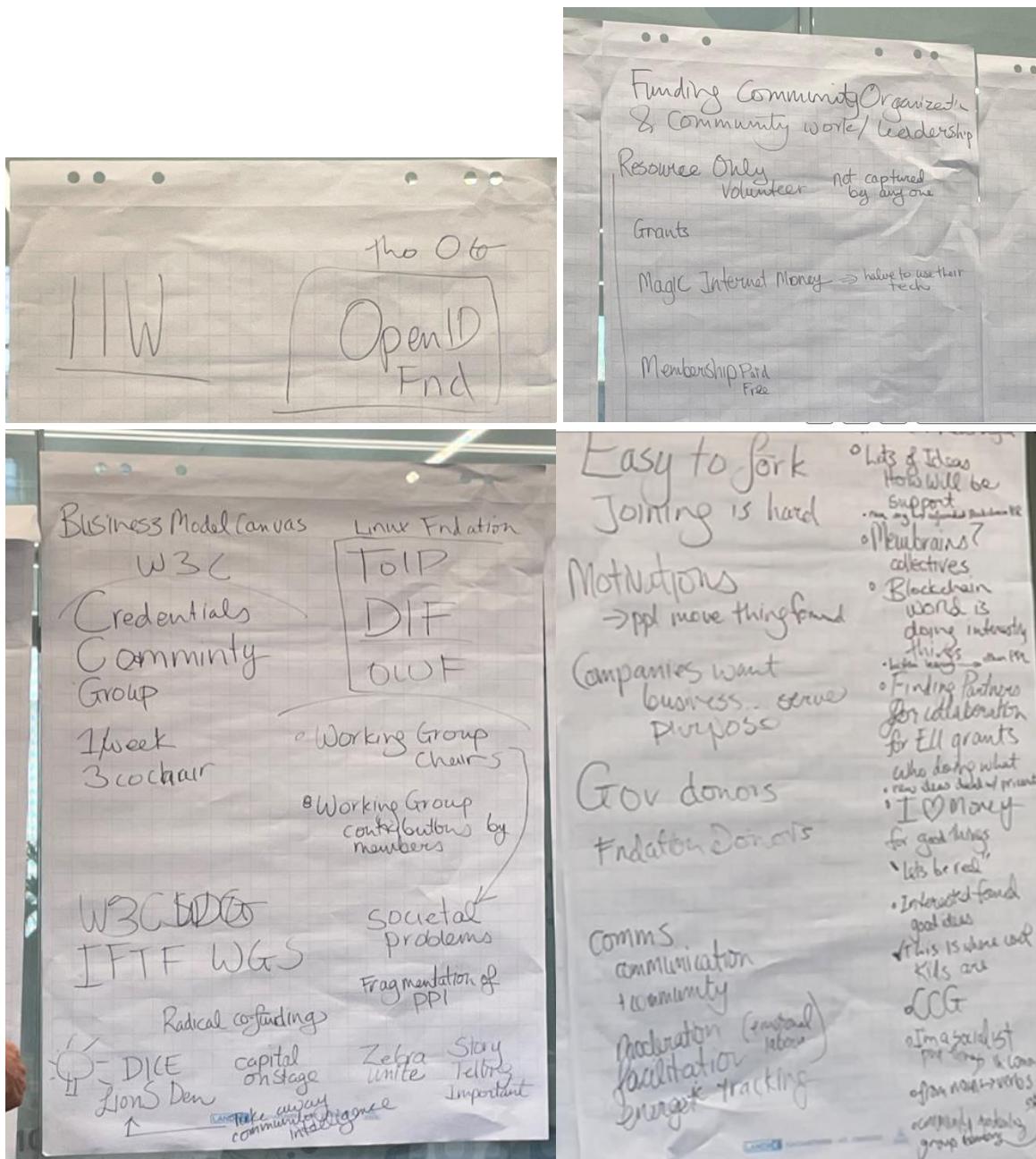
Radical co-funding.

How do we put collective intelligence in where the money goes?

Would it be possible to recognize the contribution of each volunteer's impact?

First round, short list, and ...

NEXT PAGE: THE FOUR WRITTEN PAPER-BOARDS...



- New Tech \Rightarrow Needs Legal
- Lots of Ideas
 - How will be support
 - new org w/ reformed Blockchain HR
- Membranes?
 - collectives
- Blockchain
 - World is doing interesting things
 - listen heavily \rightarrow other PPL
- Finding Partners for collaboration for EU grants
 - Who doing what
 - new ideas deal w/ priority
- I ❤ Money for good things
 - Let's be real
- Interested found good ideas
 - ✓ This is where weh kids are
- CCG
 - I'm a socialist
put things in common
 - from nouns \rightarrow verbs
 - community building
 - group bonding

Build your decentralized identity use case in less than 1 hour!

Session Convener: Kai, Marco and Robin

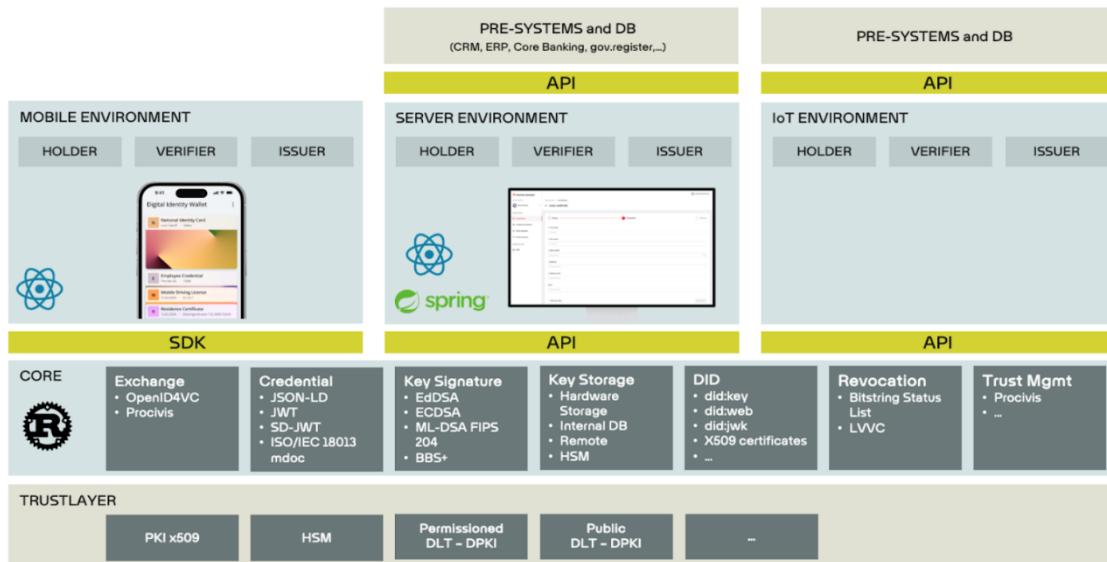
Session Notes Taker: Kai

(optional) List of Session Attendees: ca. 12 people in a way too small room, getting excited about trying out their ideas for new credential schemas, designs and user flows that utilize them. (Mostly from private sector consulting side and public sector E-ID project side)

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

People were introduced to the recently launched Pro civis One Trial environment that allows for quick prototyping and designing of credential and wallet driven use cases in an end-to-end trial playground for product managers, consultants and developers, both in a no-code or API style interaction.

<https://docs.procivis.ch/trial/intro>



Legal Person (wallets) what makes them different & lessons learned.

Session Convener: Maarten

Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

No Notes Submitted

Beyond the Issuer-Holder-Verifier-Model - Collecting use cases

Session Convener: Sebastian Zickau (Stadt Köln, City of Cologne)

Session Notes Taker: Sebastian Zickau

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Beyond the Issuer-Holder-Verifier-Model

Collecting use cases

The session is about finding use cases and their initial requirements that may need additional functionalities not supported by current standards and approaches.

Motivation

The primary motivation for this session comes from a use case on the German health certificate in which the holder of the initial credential has to pass it on to his/her employer. The employer becomes the new holder/guardian/delegate and will show it to a verifier during the employment. After the employment, the employer returns the activated (within three months after first issuing) credential to the employee.

The members of the session were presented with these concepts and the described use case to start the discussion.

- Delegation
- Guardianship
- Forwarding
- Handover

- Invalidation
- Composition
- Chaining
- Controllership
- Attestation
- Witness
- Nesting
- Embedding
- Merging
- Linking
- Binding
- Augmenting
- Impersonation (s.th. to avoid)

Use cases that were collected:

Financial support for parents whose children are students

In Switzerland, parents of students can get financial support. This support is paid by an institution, known as Ausgleichskasse, through the student's employer.

The difficulty in the process lies in proofing

1. the parenthood
2. of a student

to this institution, Ausgleichskasse. The parent needs to get a credential from the child to proceed with registering for such financial support. So, this use case is also in the area of guardianship/delegation.

Additional: Health and parenthood related

For the rest of the session, we discussed use cases within the delegation of rights in health-related situations, such as when a patient becomes incapable of dealing with his/her credentials or is either too young or too old. Here, we discussed a possible breaking-glass scenario in which the credential owner nominates a guardian/relative in advance. This is also not true for situations where the owner is an infant, for example. Also, we discussed if there needs to be a third party involved in the process or if this can be done at the holder wallet level. In the latter case, getting credentials of your baby child might be possible through an additional party/process.

It was also discussed that there are situations in which it is maybe better that there are no records of a delegation, for example, in the case in which a minor may get a prescription for contraception related to the religious beliefs of the parents.

For the rest of the session, we discussed use cases in which a notary is required to prove that someone is a child of deceased parents in inheritance cases. In some countries, you get a birth certificate stating your parents' identity. In some other countries, you have a family history book. For example, you prove who you are in France by stating who your parents are.

Permissioned Smart Contracts

Session Convener: Titus Capilnean / VP GTM @ Civic.com

Session Notes Taker: same as the convener

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

- The idea of a permissioned smart contract is that you can enforce more rules than just those that govern who can write to the contract, update it and control it
- With the right set of rules on-chain, you can enforce also who can interact with the smart contract, like in the use case of an allow-list
- The blockchain world is embracing the fact that not everything needs to be purely decentralized and some level of centralization is needed for specific use cases, like adhering to local regulations in specific markets. The concept translates well into identity, where there are cases where self-sovereignty is diminished for the purpose of protecting an asset or the entire chain
- Instead of hardcoding the allow-list in the smart contract, an organization can check for the existence of a valid soulbound token (active state) to enable use cases like real world asset (RWA) tokenization, stock market tokenization, bond tokenization, commodities, decentralised physical infrastructure networks (DePIN) - like in the case of Civic Pass
<https://docs.civic.com/introduction/what-is-civic-pass>
- This technology is enabled by a new token standard on Solana (SPL 2022), with transfer hooks - <https://github.com/civicteam/token-extensions-transfer-hook>
- Process at high level
 - Application needs users to have valid Passes to access an asset on-chain
 - Users go through verification using either/both biometric data and ID verification to receive a Pass
 - The result of the biometric scan can be stored in an encrypted state (salted, with a key tied to the user wallet) for uniqueness verification
 - App then checks for the user Pass and then lets them transact
- We debated how to best explain to the user the process of verifying the biometrics data and storing an encrypted vector output that has no PII value, and that it's revocable by design
- Other use cases/methods discussed
 - zkPassport
 - Proof of Passport
 - zkEmail and DKIM/SPF authentication for senders
 - Argent social account recovery
 - genAI avatar IDs that can interact both on and off-chain
 - DAO voting use cases
 - MPC wallets with extra security
- We discussed <https://ucan.xyz/> (could replace the way Metamask does authentication, for example) , <https://KERI.one> , did:key, did:dht as an alternative to blockchain use case

Use cases vs Business Cases

Session Convener: Merul

Session Notes Taker: Merul

(optional) List of Session Attendees:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

We had a nice discussion around how a use case is different from a business case

What is a use case

A use case is a detailed description of how users (actors) interact with a system to achieve a specific goal.

What is a use business case

It outlines the **rationale** for the project, including the **benefits**, **costs**, **risks**, and **impact** on the organization.

Potential Interop OiD4VCi (track 2)

Session Convener: Jan Vereecken, Linas Isganaitis (Meeco)

Session Notes Taker: Jan Vereecken

(optional) List of Session Attendees:

Mostly participants in the interop event from BDR, Blockverse, Lissi

As well as a few other observers.

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Very hands on session after all of the presentations the last couple of days.

We introduced the goal of the the Potential Interop Event. Link to the document that describes the profile can be found https://gitlab.opencode.de/potential/interop-event/-/blob/master/track2/description/LSP_POTENTIAL_Interop-Event_Description_Track2_v2.pdf?ref_type=heads

(requires you to be registered, not public)

Had a very good session where companies were able to test their Wallet and Issuer implementations against each other and quickly debug and even fix some issues on the spot. There were also a few things that need to be followed up on at a later time.

SD-JWT VCDM

Session Convener: Oliver

Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

No Notes Submitted

Let's make something fun with / about SSI - in sports, inbusiness, in family

Session Convener: Thomas Wüthrich

Session Notes Taker: aaa

(optional) List of Session Attendees:

- Adrian Doerk und Sebastian Bickerle / Lissi
- Oliver Schläpfer / Swisscom

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Our Motivation: Win people's hearts and trust where it's less sensitive (educate by building habits)

=> Apple and Google Wallet for payment as Inspiration!

General Thoughts

- How can we create habit forming situations for using credentials and the associated technology
- It's really not attractive to be issuer...and verifiers paying for using credentials are unlikely unless they are legally forced to proof that they verified something for delivering their services
- To penetrate the market...you need to be 10x better than today's solution!
 - What are everyday unmet needs?
 - Let people in your house...

Some Use Cases we discussed...

1) Reward Voluntary Work

- Pain: Missing Recognition of Voluntary Work...and it's getting harder to find people
- Background Voluntary Work in Swiss Sports:
 - [Some Stats and Figures from Switzerland](#)
 - 73 million working hours per year!
- Convince existing solutions/providers to start issuing credential as verifiable proof of voluntary work
 - <https://www.benevol.ch/>
 - <https://www.swissvolunteers.ch/>
- Find verifiers willing to reward voluntary work...leveraging the interoperability of SSI
 - Swisscom offers anyone who has a verifiable credential for voluntary work (event) 10% off for the mobile subscription

2) How to make personalised (Football) Game Tickets a cool experience

- Pain: Personalised tickets is a nightmare if 50k people try to access a venue in a short amount of time, also it feels slightly dystopic
- Background: Issuing personalised tickets to go to sports events is a likely reality in Switzerland due to ongoing problems with hooliganism

- <https://www.kkpd.ch/newsreader/einheitliche-umsetzung-des-hooligan-konkordats.html>
- Use SSI to minimise cost for verification at the arena entrance...use existing technology
 - legacy system for access management are difficult to work with
- Reward fans with credentials for actually being there...loyalty programs
 - Have them use their credentials both in the stadium and the digital world

3) SSI and Match-Making (for relations, sports, whatever you like to do together)

- Use something that works...and deliver what is hard to provide...trust
 - in information provided...verifiable credentials
 - in people associated with it...eID as definitive proof
- Example: Let's say you want to build the tinder for finding running buddies...
 - You share and see only verifiable information about potential matches...you get a similar experience like other matching platforms but you can trust the information!
 - Million Dollar Question: Who pays for it...
 - Business Model: Combine it with the opportunity for brands to connect with community members 1:1...have these brands pay for getting access to this trust marketplace
 - Probably needs to be a non-profit organisation in order to keep it minimally extractive and be more attractive than existing alternatives
 - The Tinder or Running with the opportunity to monetize your information

SESSION #10

Go To Market Strategies for Wallet Ecosystems

Session Convener: Adrian Doerk

Session Notes Taker: Fraser Edwards

(optional) List of Session Attendees:

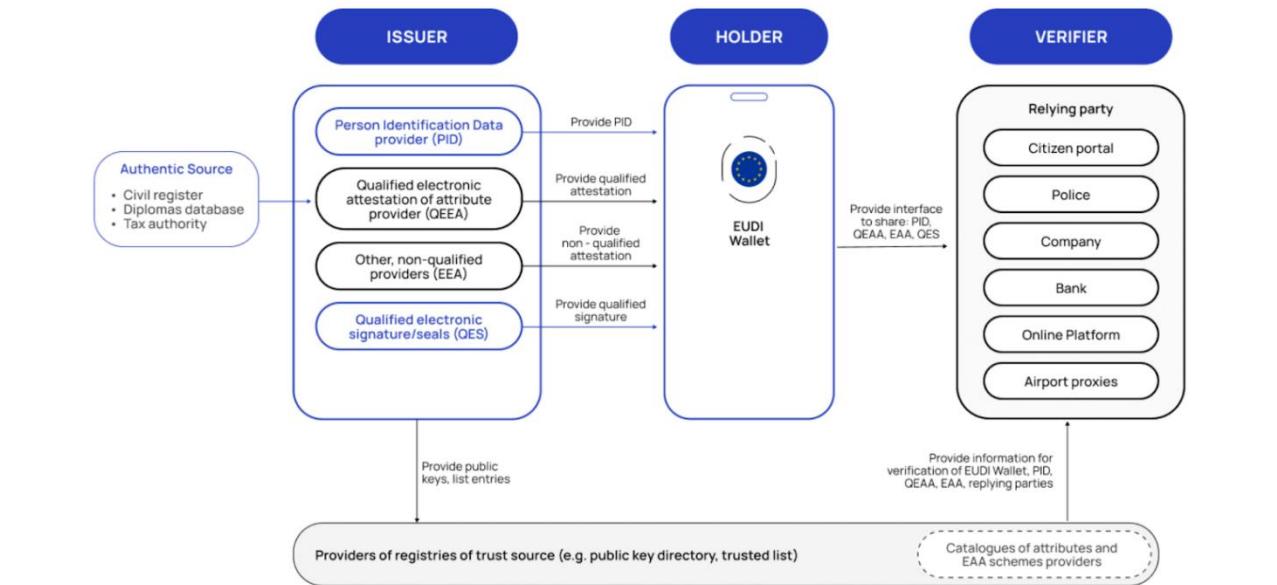
- Adrian Doerk
- Fraser Edwards
- Stefan Textor
- Titus Capilnean
- Ivan Anastasi
- Stephan Hofstetter
- others...

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.



Roles in eIDAS2 | 11

Depending on the use case you can have multiple roles in the ecosystem



- Two primary routes currently:
 - Regulated industries with strong requirements which move slower
 - Here need to go for specific industry use-cases as the requirements and regulations are extremely specific
 - Unregulated where projects can move quickly without needing to wait for regulatory clarity

- Iterate quickly and focus on PMF
- Consortiums
 - Seem to be typical GTM at the moment
 - i.e. Wallet is built as part of use-case / consortium deployment
- Crypto / Civic:
 - Seeing demand for KYC for a blend of:
 - Preventing sybil attacks & geo-gating across (typically US) for:
 - Airdrops, testnets, testnet faucets
- Wallets are typically being funded by selling other services, typically SaaS for issuance or verification:
 - This presents a problem if the SaaS fails, i.e. no revenue to maintain wallets
 - Civic experienced this years ago
- Germany:
 - Is setting up a WG on wallets, inc. how to fund these.
 - SPRIN-D has two tracks:
 - Funded - typically start-ups bringing innovation
 - Unfunded - typically larger participants, e.g. Samsung, Google, etc
 - Likely that these orgs will offer wallets as a loss-leader or build services atop these
- Incentives for ecosystem participants:
 - Crucial but currently missing in eIDAS 2.0
 - Very little work being done on this yet as work is being driven out by the governments
 - Itsme (Belgian wallet) - Subscription model for verifiers to pay issuer via agreed scheme
 - NGS focuses on cost-saving
 - Likewise Ingo (eStatus)
- Likely that initially there will be lots of fragmented wallets, e.g. Ingo, Itsme, Swiss
- Will likely need ecosystem, use-case or service specific “meta-wallets” longer term which aggregate over multiple data stores
 - Google have already demonstrated a “credential picker” at a previous IIW which allows you to pull credentials from multiple stores as appropriate
 - Definite risk that Apple and Google will clear up
- Wallet UX will be king, especially for “meta-wallets”
 - Will need to offer additional services beyond just data storage which will become commoditised
- EUDI:
 - Even EUDI participants in one pilot cannot see work of other EUDI pilots which is extremely unhelpful
 - For those on the outside, these are entirely opaque
- Accessibility:
 - One idea for differentiated GTM was to focus on accessibility as this isn’t being considered much right now
- The lissi team has created a use case evaluation sheet, which you can find here:

- https://docs.google.com/spreadsheets/d/1orAgUYMX0CyH2xHyHODluDTQnzSe803ywb7_DIWHoUA/edit?usp=sharing



Use cases for the **EUDI-Wallet** can be found in almost all areas of life



Bank / Insurances

- Strong customer authentication (EAA / 100x)
- Payments (QEAA / 100x)
- Proof of insurance (QEAA / 5x)
- Authentication call center (EAA / 5x)

Telecommunication

- Sim card application (PID, QEAA/ 0.3x)
- Authentication call center (3x)

Facility management / Rentals

- Access management (EAA / 200x)
- Physical access (EAA / 400x)

Public sector

- Municipality datacard (QEAA / 20x)
- Season tickets (EAA / 20x)
- Social pass (EAA / 20x)
- Leisure pass (EAA / 20x)
- Fishing license (QEAA / 10x)
- Instructions on infection protection (QEAA / 5x)
- Permission for street musicians (QEAA / 50x)
- Itinerant trade allowance (QEAA / 50x)
- Volunteering card (QEAA / 10x)

Commerce / retail sales

- Customer card (EAA / 50x)
- Discount voucher (EAA / 10x)
- Checkout/ payments (QEAA, 100x)
- Customer onboarding / registration (10x)
- Age verification (QEAA / 5x)
- Product warranty (EAA/ 10x)

Education

- Pupil IDs (EAA / 25x)
- Student IDs (EAA / 50x)
- E-Learning Certificates (EAA / 5x)
- Library card (EAA / 10x)

Traffic / Public transport

- Season tickets public transport (EAA / 200x)
- Ticket booking (EAA / 25x)
- Cars/ Scooter rental (PID, QEAA / 4x)

Logistic / Supply Chain

- Organisation Identity (ODI, QEAA / 50x)
- Masterdata management (ODI, QEAA, EAA, 50x)
- Supplier onboarding (QEAA, EAA, 50x)
- CO2 - evidence (EAA /, 20x)
- Product pass (EAA / 400x)

Work

- Employee identity card (EAA / 200x)
- Access Management (EAA / 400x)
- Passwordless login (EAA / 1.000x)
- Password reset (EAA / 3x)
- Proof of profession (QEAA / 10x)
- Qualifications / trainings (QEAA, EAA / 5x)

Tourism

- Check-in (PID, QEAA / 5x)
- Cure & guest card((QEAA / 5x)
- Hotel-/ room card (EAA / 14x)
- customer card (EAA / 5x)
- Travel voucher (EAA / 3x)

Media / Social Media

- Passwordless login (EAA / 300x)
- Customer onboarding (EAA / 10x)
- Age verification (PID / 4x)

Leisure

- Membership pass (EAA / 50x)
- Access management (EAA / 50x)
- Event tickets (EAA / 20x)
- Playing-/start allowance (EAA / 20x)

How to read: Use case (Credential type, number of usage per year)

- Country provided wallets:
 - Will focus on storage of government issued attribute credentials and typically cost-saving routes, e.g. simplifying ID checks from driving licences to criminal record checks.
 - Opportunity will then be to build atop these with value added services.

ZKP Growth 16 Alternatives to BBS Signatures / Dima

Session Convener: Dima

Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

No Notes Submitted

How can we harmonize the user experience of consent and what is needed there?

Session Convener: Kai & Marco

Session Notes Taker: Kai

(optional) List of Session Attendees: ca. 12 people mostly from SSI product companies and the expert space on digital credential exchange protocols and Wallet UI/UX as well as a few people from government Wallet projects.

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

The session uncovered (again) that our community is discussing governance and trust questions a lot in many places, but does not take enough effort in providing an interoperable, implementation agnostic and ideally standardised approach to policy management, handling and presentation.

This problem space is about situation where either

- A. The user is offered a credential from a issuer
- B. The user is requested to share a (selective) presentation of its wallet contents

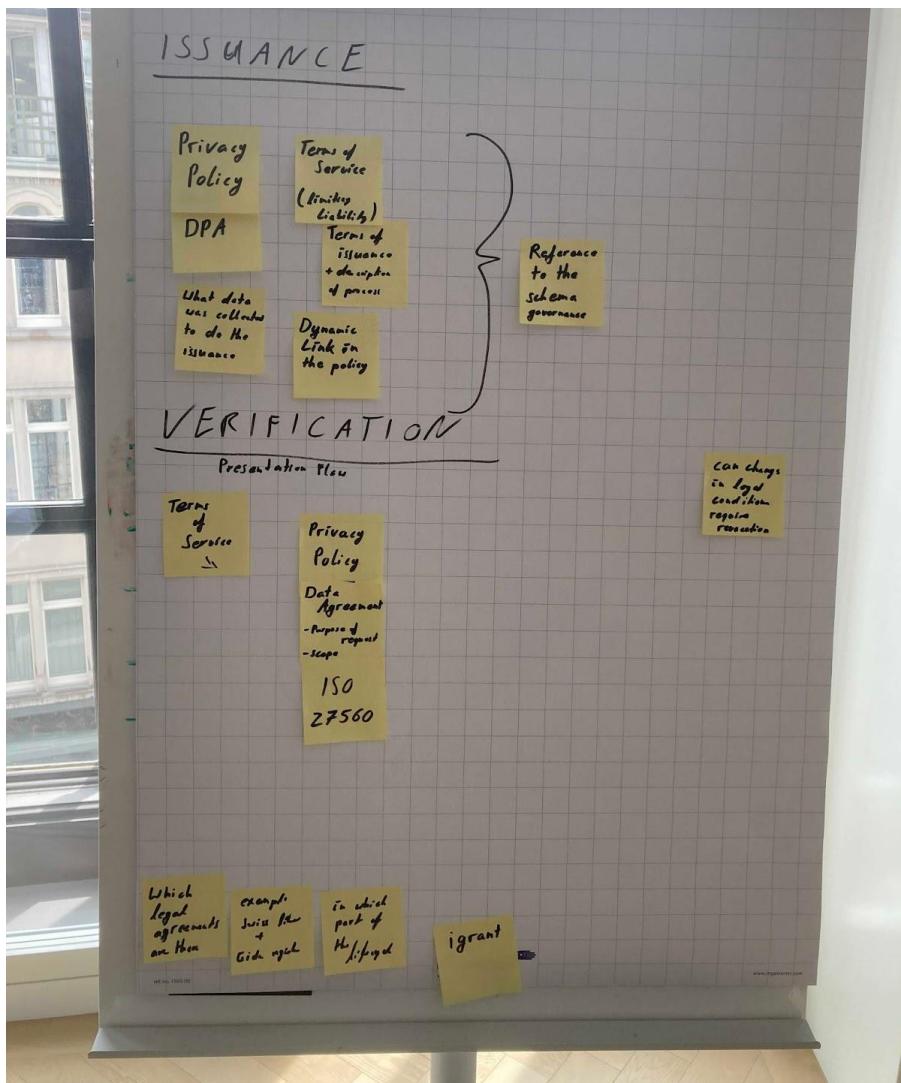
Our discussion came to the agreement that at a minimum end users can expect certain policy documents to be shared with them in the process of both issuance and verification. Also they can expect at a minimum to be able to properly notice and read these documents before continuing in their process and that these documents need to be provided in a way that allows the user to read them again and take reference to them in the correct version based on the interaction history they have stored in their wallet associate with the respective issuer/verifier interaction.

These minimum documents are:

- A **Privacy Policy (PP)**, informing the wallet user about how the issuer/verifier is accessing, storing, treating and processing her personal data.
- A **Terms of Service Policy (ToS)**, that either refers to the applicable law or makes concrete stipulations about the contractual nature of the issuer/verifier interaction

Open discussion points we did not agree on, but had a very productive exchange on:

- Some welcomed the idea to have a standardised way of requesting, recording and revoking consent to these policies as a wallet user.
- These policies (especially ToS) can be very basic, but the more basic they are, the more risk is on the side of the policy provider, since they risk having to solve a dispute in court rather than based on the policies the user agreed to in the interaction.



Credhub - a cloud wallet at open wallet foundation

Session Convener: Mirko Mollik

Session Notes Taker: Mirko Mollik

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

While Edge wallets can be used offline and traceability is limited by the provider, the current lack of good libraries make the implementation quite challenging. By moving the business logic and data into the cloud, the device becomes just a client that needs to render the information. In the session Mirko also explained why he did not use any ssi framework like credo or veramo: they come with features that are not required and need to be maintained.

The project is an open source implementation based at the open wallet foundation:

<https://credhub.eu/>

But Should We?

Session Convener: Grace

Session Notes Taker: Grace

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Very few people showed up, so we concluded that we shouldn't.

Identity for Universal Private Compute

Session Convener: Manu Fontaine

Session Notes Taker: Manu Fontaine

(optional) List of Session Attendees:

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

This session outlined why “universal zero trust” is necessary. We outlined what needs to be done at the infrastructure layer to enable “universal private compute”, i.e. the global assurance that private data is only exposed to verified, privacy-preserving code. Confidential Computing is a key enabling technology to make this possible.

Feel free to reach out to discuss: manu@hushmesh.com

Overview slides here:

https://drive.google.com/file/d/1OQz9vMNs-apY7eKAp5_-ucx68OFuYUnc/view?usp=sharing

What is missing? Looking forward from ARF 1.4

Session Convener: Christian

Session Notes Taker: Christian

Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

The session began with an overview of what pieces of the puzzle that is called eIDAS2 seem to be solved or on a good track to be solved - namely, online protocols, p2p encryption, hardware protected key-binding, selective disclosure.

Then, there was a discussion on the technical building blocks and capabilities that we already know that are missing or in a somewhat weird state in the current iteration. This also includes topics that might not make it into a first iteration of eIDAS2 - topics that might be interesting in the long run. We covered topics like Offline presentation that is credential format agnostic (currently only ISO mDoc), offline issuance (but were not convinced this was really needed), transaction authorization as something that is work in progress but no one in the room had knowledge or experience how that would map to payment and existing payment functionality.

We had a long discussion on the topic of delegation and guardianship with several use-cases that were discussed like power of attorney for legal entities (e.g., signing a contract in the name of the company) and delegated authorization for people use-cases (e.g., a tax attorney handing in taxes on your behalf). We had some discussion if we do believe there would be a common approach on how this could be handled but the consensus seemed to be that there will be no common approach for all of these.

We then had a longer discussion on the non-technical aspects and problems. We tried to figure out if there are problems, people, or use-cases that we are ignoring in the current discussions. There was a good discussion on the fact that a PID alone does not solve the problem for everyone (e.g., residents that are not from europe) and cases like migration also likely need some kind of digital ID. Another topic that was discussed for some time was digitally signed documents about family relations (e.g., proving that a child is your child) while traveling.



Attendee Posts about #DICEurope 2024



Animo @AnimoSolutions · Jun 18

...

At the opening of **#DICE2024**, [@beat_jans](#) shares some interesting insights on the Swiss eID, which is planned to launch in 2026! 🚀 The law is already approved by national council, but the tech stack is still to be decided on.



1

1

3

141

144

Rolf Rauschenbach • 1st

Informationsbeauftragter E-ID, Bundesamt für Justiz BJ / Communications Offic...
2w •

...

News on the Swiss e-ID in English

As more and more people are interested in the Swiss e-ID who speak neither German nor French, we are offering an Executive Summary in English following the regular participation meeting on a trial basis. The most important topics from our participation meeting will be summarized in English. Questions can also be asked.

On July 4, 2024 from 6 to 7 p.m., the following topics will be addressed:

- Decision on technology / tech roadmap
- Sandbox 2.0
- Q&A

The Executive Summary in English will also take place as a WebEx session. It is the same link that will be used for the participation meeting. This will be sent to all newsletter subscribers by e-mail on the day of the meeting; it is also available at the end of this post. Registration is not necessary. The easiest way to participate is via a web browser. It is not necessary to install the Webex application on your device.

<https://lnkd.in/dBdHBTN4>





Matthew Schutte • 1st

Drawing inspiration from nature to improve the vitality of society.

1mo •

...

Heidi Nobantu Saul opening the unconference (i.e. the fun) portion of Digital Identity unConference Europe (#DICE) in Zürich. I'm looking forward to the sessions!

Is there anything in particular that you would like this community of identity geeks to explore?





Mirko Mollik • 2nd

Identity Architect @ German EUDI Wallet; OWF contributor; Combinin...

3w •

...

Two days, 80 sessions and over 250 people came to Zurich to discuss about identities, sharing new ideas and challenge new approaches at **Digital Identity unConference Europe | DICE**

The Swiss E-ID Team gave some interesting insights how they are planning to roll out their solutions to the citizen. Compared to Germany it's easier for them to start since they do not have a digital solution that needs to compete with an older one.

While there were some great talks about simple solutions that can be used in the near future, more complex solutions like zero knowledge proof based ones were also presented.

And last but not least the gap between security and usability. When responsible providers are not able to offer solutions that get acceptance by the users, the users will move to unsecure solutions. Regulations will not help with the digitalisation in Europe when the solution is a nightmare in UX.





Yuting JIANG • 1st

Co-Founder & CEO of ZKorum | Break Barriers, Build...

3w •

• • •

Daron Acemoglu and James A. Robinson described #democracy as a “narrow corridor” between social collapse and authoritarianism. At Digital Identity unConference Europe | DICE last week, Nicolas and I had the opportunity to meet and connect with brilliant minds — technologists, entrepreneurs, lawyers, and government officials — all committed to defending this corridor of liberty.

Besides from privacy-preserving national identity programs, I also learned about innovative identity solutions for stateless people and engaged in deeply insightful conversations about how we could use freedom technologies to counteract the status quo of Digital Dictatorship and Surveillance Capitalism. I also had the chance to host a session on “Identity, Social Media, and Democracy,” where we discussed the challenges of disinformation, governance, privacy and free speech on the internet.

A heartfelt thank you to Kaliya IdentityWoman Young, Heidi Nobantu Saul, and TRUST SQUARE for organizing such an impactful event, and to all the participants who make it so worthwhile!



Traditional Women's Breakfast!



Harmen van der Kooij • 1st

Co-initiator FIDES/Lead Digital Identity & Interop at Dutch Blockchain ...

3w • 🔍

•••

Last week I joined the **Digital Identity unConference Europe | DICE** in Zürich.

Many others already "reported" about this event on LinkedIn. Just want to summarize it as "fantastic and extremely valuable".

Except from the high quality and open discussions we had an epic first run with DICE Running Team 🏃

Fabrice Rochette Philipp Wirth Douwe Lycklama 💯

#DICE2024



Peter Janes (He/Him) • 1st

Data Driven Business Models || Digital Interoperability | Program Mana...

3w • 🔍

•••

A few impressions from the **Digital Identity unConference Europe | DICE** 2024, with contributions from **Kaliya IdentityWoman Young, Heidi Nobantu Saul, Beat Jans, Daniel Saeuberli, Adrian Doerk** 🇪🇺 🎧 , More ...more



DICE 2024 - Digital Identity unConference Europe

youtube.com



You and 40 others

6 comments - 2 reposts

Great Compilation Video with Music!
<https://www.youtube.com/watch?v=r1wJFhb8Vv0>



Andreas Tölke • 1st

Head FinTech & Digital Trust at Swisscom | Digital Leader | Entreprene...

[Visit my website](#)

2w •

🎥 Best of **Digital Identity unConference Europe | DICE**. What are the Key Takeaways? Have a look and enjoy the impressions of a great unConference. 🎥 🎤 Thank you again to all speakers, participants and organizers of this fantastic event. Let's continue the dialog about **#Digital #Identities** and **#Digital #Trust!**

[#aftermovie](#)



Link to Swisscom After Movie:

https://drive.google.com/file/d/1-5cWLLeCzTWDYfxb_spOJaJ1W0pm30KJ/view



Adrian Doerk • 1st

Co-Founder Lissi | IDunion | EUDI-Wallet & eIDAS

[Visit my website](#)

4w •

...

The future of **#conferences** and digital **#identity** at the same time? Yes, this is possible! The **Digital Identity unConference Europe | DICE** combines both topics as **#UnConference**.

The format ensures an interactive and participatory experience, where attendees co-create the agenda in real-time, fostering dynamic discussions and collaboration.

Participants can engage with a diverse community of governments, citizens, and companies to explore crucial topics such as technical standards **#eIDAS2**, self-sovereign identity **#SSI**, and user centric solutions among others.

The unConference setting promotes open dialogue and innovation, making it a must-attend for those shaping the digital identity landscape in **#Europe**.

I'm very much honoured to co-facilitate **#DICE24** together with **Kaliya IdentityWoman Young** and **Heidi Nobantu Saul**. Our job as facilitators is to guide, not to lead or direct. Facilitators set the stage for the event by explaining the principles of the format, encourage participation and enable the free flow of ideas and information as part of the multiple parallel sessions.



DICE: Digital Identity Unconference Europe

Co-facilitating community work



TRUST SQUARE

5,729 followers

3w • Edited •

...

2nd Iteration of the Digital Identity unConference Europe | DICE

We just wrapped up three transformative days at Trust Square, exploring the future of digital identity. The event began with an inspiring statement from Bundesrat **Beat Jans**, highlighting the importance of a legal basis for electronic identities and that «our trust infrastructure must accommodate in parallel more than one technology». Numerous insightful presentations made for a great start and transition into the Open Space unConference on Days 2 and 3.

Quotes from the Participants at DICE

"Honored and thankful for the fact that Federal Councillor Beat Jans was opening the unConference at TRUST SQUARE" **Daniel Säuberli**

"The unConference setting promotes open dialogue and innovation, making it a must-attend for those shaping the digital identity landscape in Hashtag #Europe." **Adrian Doerk**

"One highlight was certainly the statement of our federal council that he now only signs digitally. " **Dominic Schlegel**

"Was very impressed by the huge amount of expertise in this room with lots of bright minds " **Jörg Lenz**

Event Highlights:

200 global innovators

81 participant-led sessions

Topics ranged from Swiss **#eID** to European **#eIDAS** and beyond

What struck us most? The power of self-organization and collaboration in tackling complex challenges.

Huge shoutout to our amazing facilitators, **Heidi Nobantu**

Saul Nobantu and **Kaliya IdentityWoman Young**, for their expert guidance, and to the tireless Trust Square team for their behind-the-scenes magic. You all made this event truly special!

Thanks to the Supporters:

Swisscom / DFINITY / Procivis AG / SICPA / Global Legal Entity Identifier Foundation (GLEIF) / digitalswitzerland / DIDAS / AYANWORKS / cheqd / esatus AG / Kosma Connect / Validated ID



Martina Kolpondinos, PhD (She/Her) • 1st
SSI Adventurer | Digital Design Strategist | Gamification Pro | Founder of Kosma...
2h •

...

#DICE2024 - an unofficial paraphrased proceeding teaser

In summary, it appears we are experiencing an increased human touch in the self-sovereign identity space ([#SSI](#), [#decentralizedIdentity](#))

Democracy

or, when the spirit of it enters the technology space

Trust

or, recognizing how it is felt is important, too

Standards

or, rather the patchwork of them

Interoperability

unisono yes, but how to get there is complicated

VC Protocols

or, indeed, they do not tell how to design UX

Sovereign UX Paradox

or, how to avoid fake sovereign users by considering different dimensions of human friendliness (hint: addressing technology paternalism with Zooko and Houdini)

Identifiers

or, how did:tdw has been gaining traction across [#IIW](#) and [#DICE](#)

Sources:

Welcome speech by Federal Councillor Beat Jans, Head of the Federal Department of Justice and Police FDJP

"Digital identity - Why it's crucial for a trusted digital society," by [Andreas Tölke](#), [#Swisscom](#).

"The global protocol challenge and the art of timing," by [Andreas Freitag](#), [#Procivic](#).

"From ARF to Large Scale Pilots: Understanding eIDAS 2.0," by [Franziska Granc](#), [#NimbusTechnologieBeratung](#).

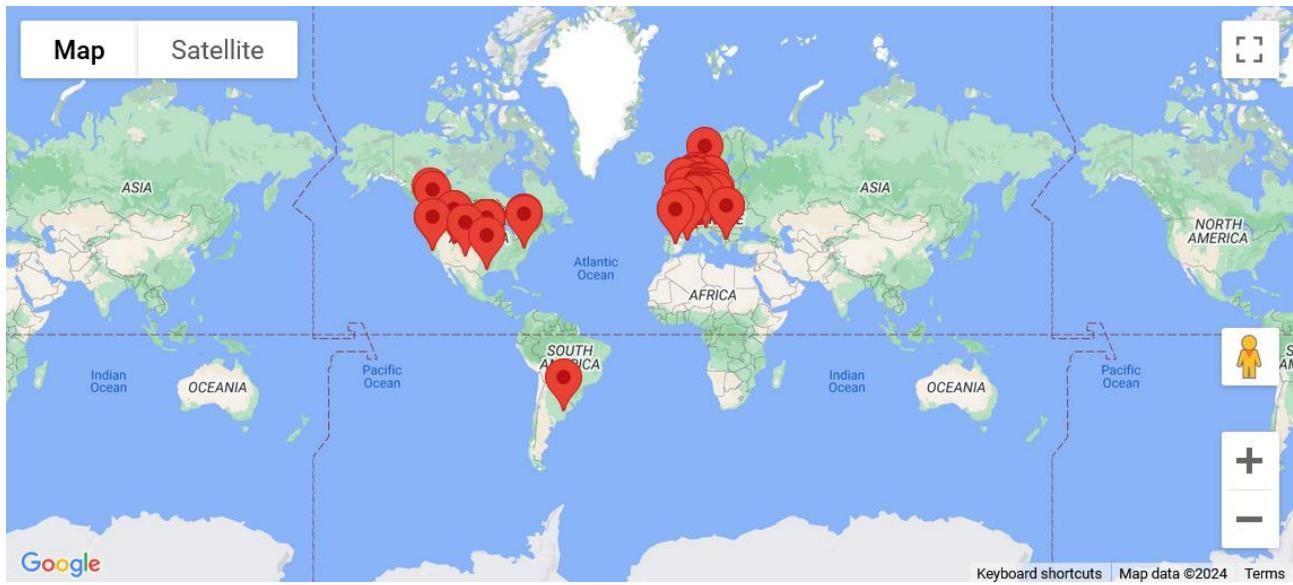
"Open Discussion on the Missing Pieces of OID4VC," by [Torsten Lødderstedt](#), [Oliver Terbu](#), [Christian Bormann](#), [Paul Bastian](#)

"Zooko and Houdini - a parable and its relevance," by [Daniel Hardman](#)

"Trust DID Web - A new web-based DID Method," by [Stephen Curran](#)

Link to Photo Library from DICE 2024

https://drive.google.com/drive/folders/1rj1d25XBosSoazoLqeFVk_HSFqfnQY6N?usp=sharing



Digital Identity unConference Europe #DICEurope 2025

Follow DICE and Trust Square on LinkedIn

Follow the Digital Identity OpenSpace unConference Europe on [LinkedIn](#) and TRUST SQUARE on [LinkedIn](#) to see posts about this event and to hear about plans for #DICE 2025!

DICE 2025

Initial planning for DICE 2025 is already underway with some new plans moving forward!

Sponsorship opportunities will be published in late August and registration will open in early September. Look for updated information at www.diceurope.org in early autumn.

Open Space unConference Facilitation: Heidi Nobantu Saul & Kaliya Young & Adrian Doerk
Notes Collection & Compilation: Heidi N. Saul

Upcoming IIW and IIW Inspired Events

