



#DICE2023  
June 7 - 9, 2023  
Zurich Switzerland

## BOOK OF PROCEEDINGS

The Book of Proceedings is a compilation of the notes submitted for the Sessions that were called and convened by participants during the 2-day OpenSpace unConference



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

# Thank You to our Documentation Center/Book of Proceedings Sponsors: AyanWorks and CURITY



## Contents

Thank You to our Documentation Center/Book of Proceedings Sponsors: AyanWorks and CURITY..... 1

About the Digital Identity OpenSpace unConference Europe..... 4

Thank You to our Sponsors and Partners! ..... 6

Daily Schedule ..... 7

Agenda Creation = Sessions Called and Hosted by Attendees ..... 9

    Thursday June 8, 2023 ~ Day 1 / Sessions 1 - 5 ..... 9

    Friday June 9, 2023 ~ Day 2 / Sessions 6 - 10 ..... 10

Session Notes Day 1 / Thursday Day 1 / Sessions 1 - 5 ..... 14

SESSION #1 ..... 14

    US SVIP - Digital Wallets & Verifier Solicitation ..... 14

    DNS and Decentralised Systems Design ..... 14

    Mapping our non-technical problems ..... 16

    Does GDPR Need to be Part of the SSI Solution? ..... 18

    How to evaluate Tech-Stacks for Future Ecosystems? ..... 19

    Collaborative Identity Proofing..... 21

    Digital Ethics - How to balance value tensions in Digital Identity..... 22

SESSION #2..... 24

    Open ID for Verifiable Credentials / OpenID for VC - Interop - Profiles & Experiences..... 24

    Explaining and Communicating E-ID ..... 26

    Making Verifiable Credentials SPEAK! VC-based voting/ polling/survey ..... 31

    The Big Mountain Behind the SSI Hill (part 2) (How to use “OCA” & “KERI” in Healthcare) .33

    W3C VC-Edu Task Force: Verifiable Credentials for Education ..... 35

    Universal DID Operations (resolve, create, update, deactivate) ..... 36

SESSION #3..... 37

    US SVIP - Digital Wallets & Verifiers Solicitations / SVIP Program Info. .... 37

    How to solve subject binding? ..... 47

    Does INDY Have a Future? / @ Giorgio Zinetti CTO ProCivis AG ..... 48

    Hopepunk Futures: What are our stories..... 49

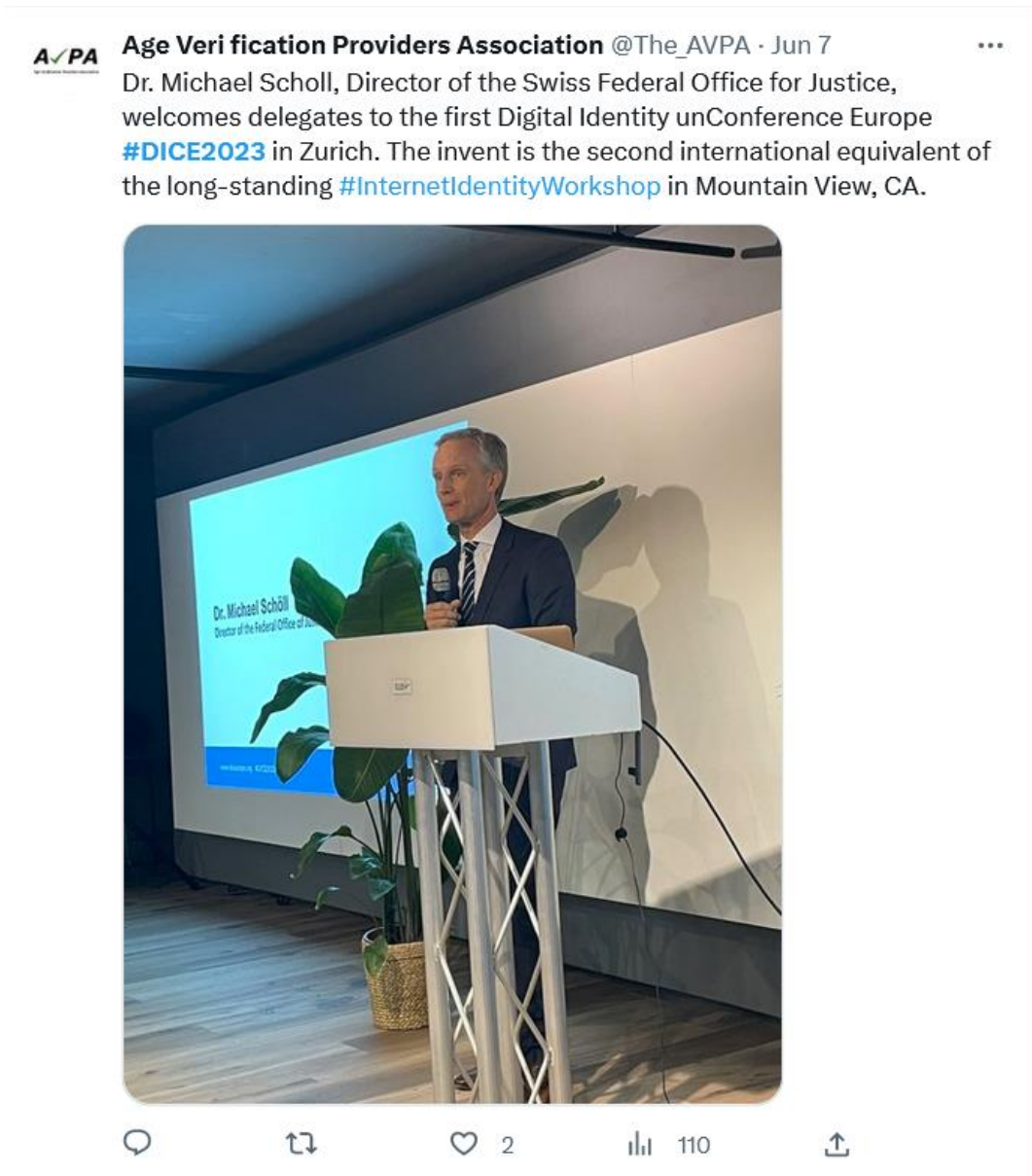
    VC lifecycle, especially recovery in face of the national E-ID..... 50

    Get an Overview of Technologies to Implement SSI..... 54

    Kicking off an SSI Agent Comparison Task Force..... 55

<b>SESSION #4</b> .....	<b>57</b>
A Framework for Wallet Security - device binding - holder binding - wallet authentication - DEMO / .....	57
Trust Registries for global Interoperability & The Role of Trust Frameworks in two-sided Markets .....	60
Ask the Swiss eID team everything ;).....	61
Biometrics, Credentials & Privacy .....	64
POC for Wallet Based EHR & Being Part of a SSI Use Case Implementation project on health data. ....	68
How can we connect SSI with supply chain?.....	71
<b>SESSION #5</b> .....	<b>72</b>
AI (ML etc) and SSI / Identity in the age of Generative AI .....	72
Human experience within SSI.....	79
Requirements for Org Wallets .....	82
How to kick off the E-ID-ecosystem? .....	85
Sustainable business models without a dominant party. How does the marketplace look? ..	85
<b>Notes Day 2 / Friday June 9 / Sessions 6 - 10</b> .....	<b>86</b>
<b>SESSION #6</b> .....	<b>86</b>
.ZKDID Decentralised DNS Web3 TLD protocol .....	92
Introducing the Use Case Canvas for VC use-cases .....	94
The road to hell is paved with identity. Designing and building for humans. ....	95
Sam Smith’s tech-stack explained (KERI and other buzzwords) .....	96
OID4VCI & SD-JWT deep dive .....	97
AMA about the Polygon ID Solution .....	99
<b>SESSION #7</b> .....	<b>106</b>
Revocation .....	106
Role of Government to build up an elb-encryption and within as established Trust Framework .....	107
USEFUL Interactions with trusted relationships DIDcom .....	107
Where does PRIVACY end and SECURITY begin...or... Where does SECURITY end and PRIVACY begin? .....	109
<b>SESSION #8</b> .....	<b>112</b>
Using Humor & Visual Communication to Gain TRUST 101 / Chance .....	112
Beyond Use Cases: Communicating guiding visions for Digital Government .....	112
Building Blocks, Abstraction Layers & Multistack environments - discussing long-term perspectives & how to survive multi-year ecosystems in an volatile tech environment....	115
“Circle of Specialists” - Do’s & Don’ts learned the hard way: Tech - Marketing - Governance .....	118
Decentralized Social Media + SSI.....	121
Legal Values for SSIs - Binding SSIs to eIDAS.....	121
<b>SESSION #9</b> .....	<b>122</b>
eIDAS 2.0 EUDIW ARF .....	122
Open conversation on data vaults .....	124
Trust frameworks practical (technical) implementation what is out there?.....	124
Models of Identity and Interaction - An Exhibition ? .....	125
Practical: Overview and roadmap of Aries Framework Javascript! (it supports more than you think).....	125
<b>SESSION #10</b> .....	<b>126</b>
The usability and privacy trade off - A Technical/Standards bases/ Timo .....	126

Make Credentials Look Good. Together. Today.....	126
Standardization and wallet overview.....	128
<b>Attendee Comments on Participating in #DICE2023.....</b>	<b>129</b>
<b>Digital Identity OpenSpace unConference Europe #DICE2024 .....</b>	<b>134</b>
Follow DICE on LinkedIn.....	134
DICE 2024.....	134



## 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.

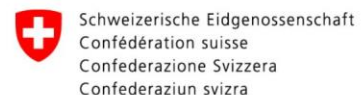
Read about [how to prepare for an unConference here](#).

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



## Thank You to our Sponsors and Partners!

Thank you to our sponsors



This first Digital Identity unConference Europe would not have been possible without the Sponsors and Partners who stepped up to make this initial gathering feasible, whether through financial support or enthusiastic promotion of the event!

Some of the best interactions at an OpenSpace unConference happen over a drink or meal. Fundamentals Sponsorships help keep ticket prices low, even with all meals included, making it available to all who want to attend, participate and contribute.

If you are interested in becoming a Sponsor of DICE 2024, please contact Heidi N Saul @ [Heidi@HeidiNobantuSaul.com](mailto:Heidi@HeidiNobantuSaul.com) Sponsorship opportunities for DICE2024 will be published in late August 2023.

## Daily Schedule

# DICE 3 Day Schedule

<b>WEDNESDAY June 7 / Pre unConference ½ Day</b> Start and Welcome to the DICE Pre-Conference at <b>13:30</b>			
Official Welcome & Welcome by Swiss Government - Dr. Michael Schöll Director Federal Office of Justice	13:30-14:00	<b>Breakouts:</b> “SSI applied - Swiss Proof of Concepts” 3 Examples <b>Internet Identity:</b> End of User Name & Passwords w/Dfinity Foundation	15:30-16:00  16:00 - 16:30
Keynotes and Presentations 2 Tracks <b>Room 1:</b> Intro and Basic Topics/ SSI, DID, VC <b>Room 2:</b> Advanced Topics/Secure Digital ID, Trusted Lists, Scaling SSI	14:00-15:30  <b>3 Sessions in Each Track</b>	Panel Discussion “International Digital Identity Programs – a Government Perspective”	16:30-17:30
<b>DICE Welcome Reception - 17:30 til late @ Trust Square</b> <b>Sponsored by - SICPA</b>			

<b>Open Space unConference Day 1 - THURSDAY June 8 / Doors Open at 8:00</b> Light Breakfast - Coffee/Tea			
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	12:30 - 13:30	Conference Dinner	18:00 - 20:30
<b>Conference Dinner for all Attendees</b>			



Open Space unConference Day 2 - FRIDAY June 9 / Doors Open at 8:00			
Light Breakfast - Coffee/Tea			
Women's Breakfast	8:00 - 9:00	Lunch	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		
<b>No Host Post Event Gathering / Suggested Location to be Announced</b>			



**Age Verification Providers Association @The\_AVPA · Jun 7**



Great panel to close the first day of #DICE2023 with reps from governments of UK Finland Bhutan USA Austria and our hosts Switzerland.



Department for Science, Innovation and Technology



120



## Agenda Creation = Sessions Called and Hosted by Attendees



56 distinct sessions were called and held over 2 Days.

We received notes, slide decks, links to presentations and photos of whiteboard work for 51 of these sessions.

### *Thursday June 8, 2023 ~ Day 1 / Sessions 1 - 5*

#### **Session 1**

- 1A/ US SVIP - Digital Wallets & Verifier Solicitation / Anil John
- 1B/ DNS and Decentralized Systems / Michael Herman
- 1C/ Mapping all our non-technical PROBLEMS / Adrian
- 1D/ Does GDPR Need to be Part of the SSI Solution? / Katrin @provicisAG
- 1E/ How to evaluate Tech-Stacks for Future Ecosystems? / Jonas
- 1F/ Collaborative Identity Proofing / Max
- 1G/ Digital Ethics: Balancing Value Tensions in Digital Identity / Jeroen

#### **Session 2**

- 2A/ Open ID for Verifiable Credentials / OpenID for VC - Interop - Profiles & Experiences / Victor Martinez, Markus, Paul, Micha
- 2B/ Explaining Communicating E - ID / Rolf
- 2C/ Making Verifiable Credentials SPEAK! - VC Based Voting / Nicolas Gimenez Zkrum
- 2D/ NO SESSION
- 2E/ The Big Mountain Behind the SSI Hill (part 2) (How to use "OCA" & "KERI" in Healthcare) / Philippe Page
- 2F/ W3C VC-EDU (Verifiable Credentials for Education Task Force) / Dmitri Zagidulin
- 2G/ Universal DID Operations (resolve, create, update, deactivate) / Markus and Azeem

### Session 3

- 3A/ US SVIP - Digital Wallets & Verifiers Solicitations / SVIP Program Info. / Anil John
- 3B/ How to solve subject binding? / Maaïke v. Leuker
- 3C/ Does INDY Have a Future? / @ Giorgio Zinetti CTO Provicg
- 3D/ Hopepunk Futures of SSI - What are our stories? / Will Abramson
- 3E/ VC lifecycle, especially recovery in face of the national E-ID / Mike and Sven
- 3F/ Get an Overview of Technologies to Implement SSI / Richard
- 3G/ Kicking off an SSI Agent Comparison Task Force / Samuel

### Session 4

- 4A/ A Framework for Wallet Security - device binding - holder binding - wallet authentication - DEMO / Paul & Micha & Markus & Sebastian
- 4B/ Trust Registries for global Interoperability & The Role of Trust Frameworks in two-sided Markets / Isaac Henderson & Douwe
- 4C/ Ask the Swiss E-ID Team Anything :- ) / Andi
- 4D/ NO SESSION
- 4E/ How do I use a Digital ID in person? & Biometrics, Credentials & Privacy / Sebastian, Zickan, IDunion
- 4F/ POC for Wallet Based EHR & Being Part of a SSI Layer 2 Implementation project on health data. / Peter Janes & Dominike Geller
- 4G/ How can we connect SSI with the Supply Chain? / Pascal Gottret

### Session 5

- 5A/ A.I. (Machine Learning LLMs) + SSI & IDentity in the age of Generative AI / Dmitri Zagidulin & Tom
- 5B/ Human Experience within SSI & How can we design a wallet our parents would use? / Zoe and Marco
- 5C/ Requirements for ORG Wallets / Andre Kudra
- 5D/ How to Kick Off the E-ID-Ecosystem? / Vitus
- 5E/ NO SESSION
- 5F/ NO SESSION
- 5G/ Sustainable business models without a dominant party. How does the marketplace look like / Jan Vereecken

## **Friday June 9. 2023 ~ Day 2 / Sessions 6 - 10**

### Session 6

- 6A/ Did:web 2.0? Improvements and Next Steps / Dmitri Zagidulin
- 6B/ ZKDID - Decentralized DNS Web3 TLD Protocol / no name
- 6C/ Introducing the Use Case Canvas for VC use-cases / Adrian
- 6D/ The road to hell is paved with identity - A practical guide for Designing & Building for humans, not identities / Bart and Andrew
- 6E/ Sam Smith's tech-stack explained (KERI and other buzzwords) / Michael, HCF Argon AUtHS
- 6F/ OID4VCI & SD-JWTs Deep Dive / Markus, Micha, Paul
- 6G/ AMA About the Polygon ID Solution / Silvia

### **Session 7**

- 7A/ REVOCATION - The perfect revocation method does not exist yet... but here is hoe? / Andreas
- 7B/ Role of Government to build up an elb-encryption and within as established Trust Framework? / Jan
- 7C/ USEFUL Interactions with trusted relationships DIDcom / Adrian, Sebastian
- 7D/ NO SESSION
- 7E/ NO SESSION
- 7F/ NO SESSION
- 7G/ Where does PRIVACY end and SECURITY begin...or... Where does SECURITY end and PRIVACY begin. / Adam Eunson & Keran Kocher

### **Session 8**

- 8A/ Using Humor & Visual Communication to Gain TRUST 101 / Chance
- 8B/ Beyond Use Cases: Communicating guiding visions for Digital Government / Rob S
- 8C/ Building Blocks, Abstraction Layers & Multistake environments - / Andi, Jonas, Raphiel, Carsten
- 8D/ NO SESSION
- 8E/ "Circle of Specialists" - Do's & Don'ts learned the hard way: Tech - Marketing - Governance / Stephan & Secoia
- 8F/ Decentralized Social Media + SSI / Dmitri Zagidulin
- 8G/ SSI's with Legal Value Binding SSIs to Eldas (?) / Andreas Abraham

### **Session 9**

- 9A/ eIDAS 2.0 EUDIW ARF / Granziska, Adrian, Andre
- 9B/ Open conversation on data vaults / Maaike
- 9C/ Trust frameworks practical implementation what is out there? / Gabriel Marquie
- 9D/ Models of Identity and Interaction - An Exhibition ? Will Abramson
- 9E/ Practical: Overview and roadmap of Aries Framework Javascript! (it supports more than you think) / Timo Ajay
- 9F/ NO SESSION
- 9G/ NO SESSION

### **Session 10**

- 10A/ The usability and privacy trade off - A Technical/Standards bases/ Timo
- 10B/ NO SESSION
- 10C/ NO SESSION
- 10D/ NO SESSION
- 10E/ Make Credentials Look Good Together Today / Christian
- 10F/ Standardisation & Wallet Overview / Maaike`
- 10G/ 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**

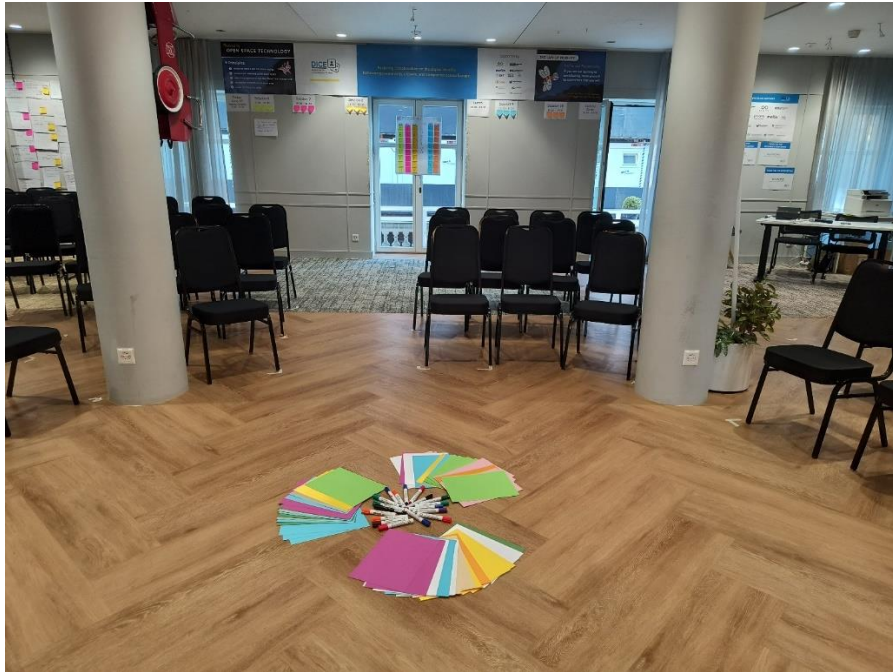
### **Session Convener:**

- 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 Qiqo 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 / Thursday Day 1 / Sessions 1 - 5

### SESSION #1

#### *US SVIP - Digital Wallets & Verifier Solicitation*

Session Convener: Anil John

Session Notes Taker:

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

Link to Slide Deck:

<https://qigo.s3.eu-west-1.amazonaws.com/fdu4046qi11dihdhk92ewuyzzc73>

#### *DNS and Decentralised Systems Design*

Session Convener: Michael Herman, Web 7.0 Foundation

Session Notes Taker: Michael Herman, Web 7.0 Foundation

(optional) List of Session Attendees: 7 attendees

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

- Primarily an information sharing session/panel
- Original intended focus was around unconventional uses of traditional RFC 1035 DNS (<https://www.rfc-editor.org/rfc/rfc1035>) in decentralized systems for things like DID Registries and Trust Registries; for example
  - DID Registry applications: <https://hyperonomy.com/2019/12/03/trusted-digital-web-first-trusted-web-page-delivered-today-dec-3-2019/>
  - Trust Registry applications:  
<https://www.youtube.com/watch?v=nWLOx8bR8Ks&list=PLU-rWqHm5p44AsU5GLsc1bHC7P8zolaAf&index=11&t=0s>
- For an overview of how RFC 1035 DNS works, checkout <https://hyperonomy.com/2019/01/02/dns-domain-name-service-a-detailed-high-level-overview/>

- About half of the attendees had experiences to offer and about half were at the sessions to learn about the use of DNS in decentralized systems.
- There was also a contingent interested in “Decentralized DNS” or, more correctly, decentralized blockchain name services (using, for example, ERC 721). References:

- Web3 Domain Alliance (W3DA): <https://www.web3domainalliance.com/>

Central player/instigator: Unstoppable Domains: <https://www.todaynftnews.com/web3-alliance-launched-by-unstoppable-domains-seeks-self-regulating-boards/>



## ***Mapping our non-technical problems***

**Session Convener:** Adrian Doerk

**Session Notes Taker:** Kalyan Kulkarni, Sabastian

**(optional) List of Session Attendees:**

Adrian, Michael Shea, [Kalyan Kulkarni](#), Andreas Abraham,

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

Mural:

<https://app.mural.co/t/mainincubator8485/m/mainincubator8485/1686212566933/6f450a7af44fc0838024e1029d5224ef673125b1?sender=adriandoerk7527>

**Few of the problems stated are -**

#1

#2 Education for people on trust in the solution - For example, there is a myth that names and PII gets stored on the chain which is not the case.

#3 How to put a use case and software into production

#4 Biggest problem faced is for non-technical people to use the wallet

#5 Legal aspects are the biggest problems

#6 This SSI field is filled with difficult and scary jargons

#6b Don't re-invent the wheel - use existing terminology and schemas for respective subject areas, e.g. schema.org, FHIR in healthcare, ...

#7 What's the balance of growing awareness for the non-techies

#8 Finding credentials in the mess of credentials? How do we manage the updates of wallets?

#9 Inclusion of elderly and handicapped

#10 Government issued certificates and claims are still paper based - bound by the legal and regulatory requirements

#11 How can offline verification take place

#12 Interaction between Humans and AI

#13 What's in it for the government - monetary value is important?

#14 Interoperability requires Standards (including implementation!)

#15 Connecting wallets and payments, e.g. used in KYC processes

#16 Enabling cross border information exchange and sharing - for better interoperability

#17 Identifiers of individuals vs. legal entities (LEI)

#18 Backups are necessary but not really user friendly

#19 Creation of honeypots

- Revocation of wallets

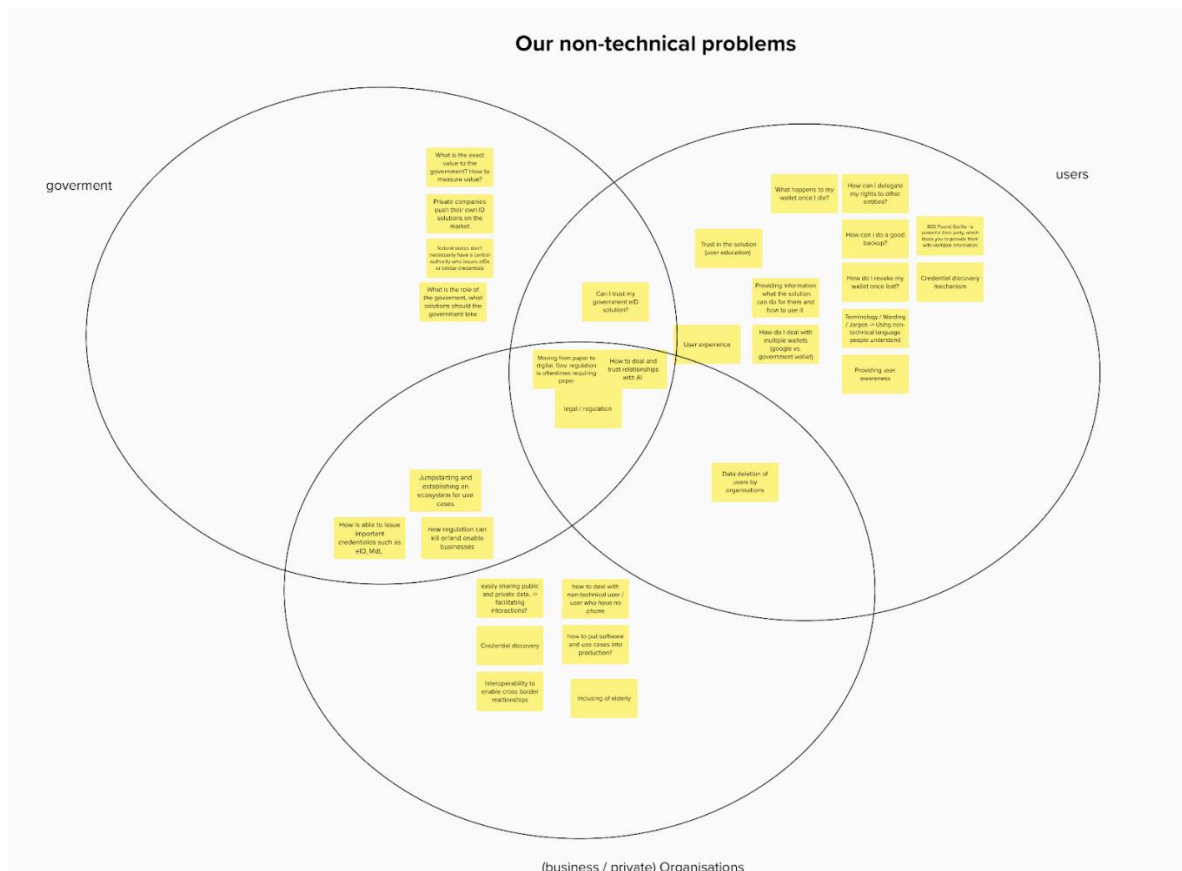
#20 What happens with my wallet when I die?

#21 How do we deal with Guardianship (long term or temporary)?

#22 Wallets on the mobile. When we cross the border into another country - border security asks to surrender the phone - how am I protected (or not protected) in such situations?

#23 Discovery mechanisms

#24 Data deletion of users by organisations



## *Does GDPR Need to be Part of the SSI Solution?*

**Session Convener:** Katrin @provicisAG

**Session Notes Taker:**

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

### **GDPR and consent**

- Each party involved in the process of credential handling (issuer, holder, verifier) needs consent from the end user if no law exists that governs the handling of data
- So for credentials issued and verified by states this might not be required, for private companies it is
- Should there be a standard to get the consent or is the existing process through a website acceptable?
  - The wallet is the UI the user is using, how can accepting the GDPR agreement for the issuer and verifier be moved to the wallet?
    - Currently done for existing ID providers e.g. for login with Amazon, the same concepts could be applied to wallets
    - Problem of non compliant wallets and bugs
      - Leads to legal links between issuer and wallet and verifier and wallet because the verifier needs to be sure that the user consented in the wallet
    - Agreement between wallet providers and verifiers and issuers is required
      - Reduces compatibility from a legal perspective
    - Differences between laws of EU member states
      - probably a single standard can not be created
    - How can non-repudiation be ensured?
    - Agreement on the issuers and verifiers web ui might be the way to go

### **Problem of fraudulent verifiers**

- Give the user the power to invoke the GDPR guarantees through the wallet
- Verifiers might ask for more data than required
  - Clear display of the asked data in the wallet
    - Again legal link between the parties because the verifier does not control the wallet
  - Selective disclosure and ZKPs for data minimization
  - They still may ask for more data, the user will probably just accept that because he has no other choice to use the service
    - Common problem in other technical systems as well
- GDPR only implies fines for fraudulent issuers but does not by itself prevent fraud
  - Technical means to reduce the risks should be considered if possible
- Verifiers might share and use the data for other purposes
  - Assignment of a trustworthiness predicate to verifiers

## *How to evaluate Tech-Stacks for Future Ecosystems?*

**Session Convener:** Jonas Niestroj & Andreas Frey Sang

**Session Notes Taker:** Andreas Frey Sang

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

Given the current developments regarding multiple technological solutions and standards developing in the SSI-Space, future infrastructure providers are confronted with making hard decisions regarding evaluations for the future ecosystems they might operate (be that as a whole or single components). The session was driven by the Swiss federal government's openness to collaborate regarding the technological future of the Swiss ecosystem and had the goal of brainstorming criteria and advice with/from the community. Given the international participants the discussion also involved the state of play in the EU and further needs arising through open questions in the EIDAS 2.0 ARF and other initiatives.

Important work done already by the community was also mentioned and listed (see attached photo 2).

The group gathered the following points:

Communication:

- DIDCOMM vs OID - Do they replace each other or are complementing solutions

Ecosystem:

- In general design should be done for multiple stacks
- EIDAS should not be the only driver in the decision, next to various other international initiatives
- Ecosystems “providers” should try to keep final or absolute decisions open for as long as possible
- Architecture which supports multiple stacks as well as modularity should be preferred

Issuer:

- The capability to issue in multiple formats can be preferable or a criteria for “issuing-solution” evaluation
- What cryptographic primitives are used should be evaluated as well as which crypto agility in the field

Registry-Level:

- Solutions which minimise requests/look-ups to the registry are favourable (privacy preservation)
- What “parsing solution” is offered by the system?
- The effects and needs regarding (non)immutability should be considered
- Decentralisation of trust lists is a further aspect to consider

- Additionally chained credentials rooted on the same “trust anchor” were mentioned (comment: Notekeeper: not sure this is placed at the correct spot or more a credential topic -> potentially related to linked credentials rooted on the same trust anchor)
- Potential for mapping existing global systems (e.g. LEI) to identifiers -> (comment notekeeper: similar comment about placement)

Non Functional Requirements/further advice:

- Roadmap based technology - is there a clear path for evolution/further development available within the potential standards/technological solutions
- Agile through & through -> more as an hint for ecosystem implementers, that agile mindset is to be had “through & through”
- There might be not “one right” solution - it is beneficial to test various pieces/combinations in a sandbox
- Simplicity of the technical solution -> is it clear and comprehensible to developers what is going on under the hood
- Non correlation
- Layer based decisions and modular architecture

Comment notekeeper:

While the mention of a sole role of the “ecosystem” provider might be weird in the context of decentralised networks this can be viewed as a placeholder for any organisation providing the core infrastructure to run a “trust ecosystem”. It is nonetheless driven from a public service infrastructure provider perspective. The session organiser would like to thank all participants for their effort and ideas regarding this topic.

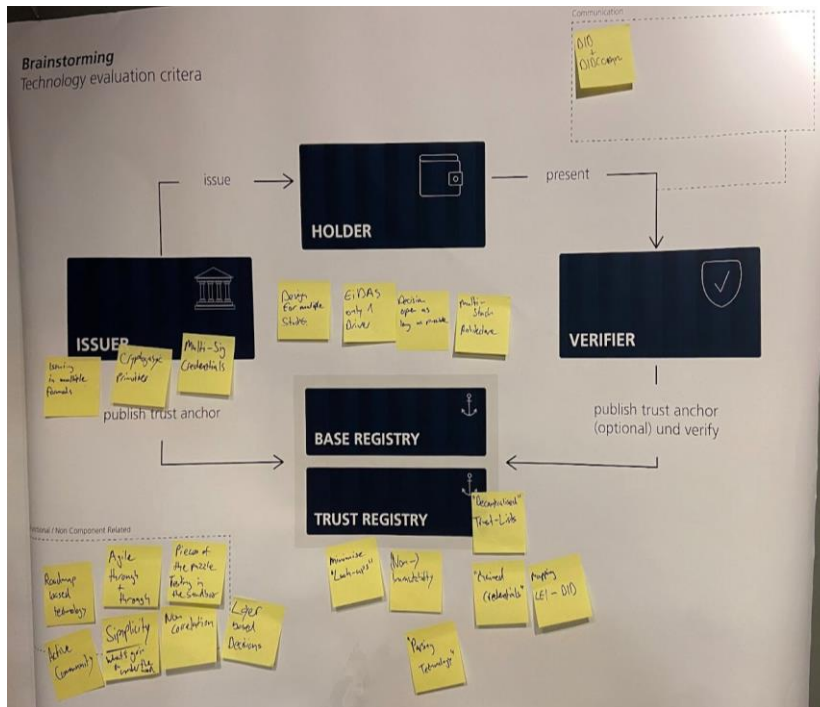
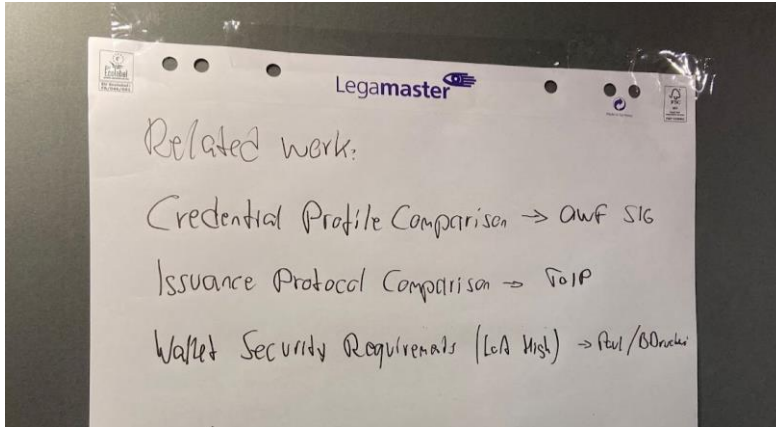


Photo 1 (Brainstroming)

Photo 2 (Other related Work)



Further criteria brainstormed by individual participants independent of the session

- Open source?
- Open Core vs Company Open Source vs Community Open Source
- License?
- Developer/integrator support? Commercial? Community?
- Issuer/verifier support? Commercial? Community?
- End-user support? Commercial? Community?
- SDK?
- Implementation project?
- Cloud/On-premise?
- Programming languages?
- Existing usage - how many users?

## ***Collaborative Identity Proofing***

**Session Convener:** Max

**Session Notes Taker:** Max

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

Proofing the identity of digital ID holders is one of the harder parts in the identity management game. Can we do that collaboratively?

Yes, we could. Although maybe we do not reach the quality and Identity Assurance Level (IAL) that an official government office can reach, that level of quality is not needed in every situation. Also, we might be faster than the official track that depends on legislation and government processes to

be put in place, and we might build upon identity proofings that have already taken place, such as companies enrolling their partners to their extranet.

What I propose is to create an association of companies that conduct individual identity proofings for their own stakeholders in an agreed-upon standardized manner, and then share the results among each other. There are many more thoughts.

The presentation given in the session was based on notes created on the train ride to the unConference, and presenting this to the interested parties was a decision taken the night before. So this is in boot mode.

Also there were remarks that some of these topics have been addressed as part of the organisational and governance subjects in the DID dokumentation. Building upon that is of course sensible.

For further information, please refer to <https://www.metakey.ch/> project “A Collaborative Effort for Proofing Identities (ACEPI)” and be sure to leave a note so that your interest is visible, or subscribe to the mailing list that should be available within a couple of days after the conference.

## ***Digital Ethics - How to balance value tensions in Digital Identity***

**Session Convener:** 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.**

- “Digital Ethics concerns the continuous moral evaluation and calibration of choices surrounding the design, organisational implementation, and oversight (governance) of digital solutions.
- Digital Ethics aims to ensure the values of all the digital solutions’ relevant stakeholders are mapped against each other, and tensions are carefully considered to ensure the solution is aligned with the intended values and acts in accordance with predetermined moral guidelines as set out by the designer, society, or governmental institutions.”
- Digital Identity solutions are complex, dynamic and networked -> there are no clear solutions to the problems, due to a wide array of solutions and perspectives
- Values are principles, standards, and qualities that guide actions. Values are what one holds important and prioritises, and guide people in how they choose to live their lives.
- Definition of trust: a confident relationship with the unknown

- There is tension between values of various stakeholders, as seen in for example Swisspass. This very popular solution will most likely be replaced with the new Swiss eID solution. What will then happen to the current business models? What will the stakeholders of Swisspass think of the new solution?
- Technology is taking over characteristics of the system it is trying to replace (e.g., cryptocurrency now becoming more centralized again on trading/wallet platforms)
- There are a lot of assumptions about the values of the people we are designing the solution for -> we need to ensure people understand the incentives behind all decisions to get the right things done
- Incentives can be used to do the right things, if used in the right way. E.g., stimulating issuers to issue credentials
- Credentials need to be commoditized, so they can be priced accordingly
- If you ask people what they want, they say privacy. At what point do you communicate to them what the consequences are of privacy. If you build it according to their values, they won't adopt it.
- DI systems are not about privacy, they are about agency
- Can we align incentives to replace the business models that will disappear?
- If you want to introduce new paradigms, you need to find the right incentives
- Just because we can monetise data, does not mean that we should
- Designers of digital identity solutions hold immense power of shaping the technology that will influence our daily interactions. They need to ensure they have the values in mind of the people they are designing it for. Ethical design is nothing more than a reflection of the values of the intended audience.
- The debate around ethics should be more structured and should have more practical outcomes, as it is currently not widely discussed due to lack of relevant outcomes. Due to a rise of relativism, concrete and tangible recommendations are usually missing from discussions on digital ethics.



## SESSION #2

### *Open ID for Verifiable Credentials / OpenID for VC - Interop - Profiles & Experiences*

**Session Convener:** Paul Bastian, Victor Martinez, Markus Kreuzsch, Micha Kraus

**Session Notes Taker:** Markus Kreuzsch

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

- Presentation of the IDUnion 2.0 TechStack
  - EU Regulation eIDAS contains W3C VC, OpenID4VC, ISO mdoc and ISO 23220
  - Shift from Hyperledger Indy / Aries / AnonCreds to OpenID Interop Profile
  - see Session 3 C on Hyperledger Indy Stack
- OID4VC Profile in the Netherlands DDIP (Dutch D? Interoperability Profile)
  - Reasoning for work on this: no good interop profile available, happy to drop this when a standard becomes available.
  - Involved: Animo Solutions (SSI development), Sphereon (SSI development), TNO (research institution),
  - OID4VCI + OID4VCP
  - DID Web + DID Key
  - JWT credentials
- OpenID4VC High Assurance Interoperability Profile with SD-JWT VC
  - Current draft presented  
<https://vcstuff.github.io/oid4vc-haip-sd-jwt-vc/draft-oid4vc-haip-sd-jwt-vc.html>
  - Tradeoff between features and stuff in the spec and simplicity of implementation
  - Question to the audience: What is your experience when using OpenID4VC?
    - Interoperability between providers is hard, lots of discussions to ensure compatibility
    - Idea of a plugfest for OID4VC
    - OpenID foundation planning to provide a conformance test fo OID4VC
    - OpenID4VC is a lot simple than the AnonCreds/DIDComm stack  
Loss of some privacy properties but in most cases it is probably enough
    - Simple issuer written during a hackathon in Nuremberg in 1,5 days
    - Rooms for improvement in terms of modularity (for example no way of doing error reports and strong reliance on properties of HTTP)
  - Missing part: trust and trust lists, this has been left open in eIDAS  
In general there are several choices
    - OpenID connect federation
    - X509 registries
  - SIOPv2
    - Authentication mechanism similar to FIDO
    - Overlap with OID4VP

- Plan: Merging of JWT VC and SD-JWT VC spec
- Use case for OID4VCI: Identity Management in Distribution project
  - VC issuance to travel agencies
  - Protocols and standards
    - did:web
    - OpenID4VCI
    - open to DIDComm
    - JSON-LD
    - plan to support JWT
  - Discovery of cloud wallet credential offer endpoint through DID service  
Reasoning: compatibility of the two approaches OID4VCI and DIDComm while keeping the choice transparent to the user
  - Prevents nascar problem of cloud wallets
    - nascar problem of cloud wallets:  
An issuer needs to display the user a choice of ALL possible wallets the user might want to use to send the credential offer to the correct wallet
  - Insights into a discussion at IIW: How can a wallet be invoked?
    - Several sessions spent on that topic. Google wants to deprecate deep links although it is used widely and everybody is focusing on it to invoke wallets currently. Proposition on an API that is browser / OS provided and can be called to invoke a wallet.
  - Privacy concerns: Using the same DID to receive multiple credentials  
This is not a problem in the presented usecase because it is only concerned with organisational wallets

## ***Explaining and Communicating E-ID***

**Session Convener:** Rolf Rauschenbach [rolf.rauschenbach@bj.admin.ch](mailto:rolf.rauschenbach@bj.admin.ch), Communication Officer E-ID, Federal Office of Justice, Switzerland

**Session Notes Taker:** Rolf Rauschenbach

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

### **Topics**

#### **General remarks**

- [Douwe] What target groups we need to engage to bootstrap to ecosystem to become the well adopted digital infrastructure in the coming 10 years ? First angles: consumers: youth, working age, old, children, disabled etc Business: the ones who can be instrumental in distribution and onboarding (banks, telco, insurers), companies offering 'acceptance' services (to be a verifier).
- [Douwe] Which message towards each target group? to C messages, to B message, to C-suite messaging for decision making
- [Douwe] Common communication across all stakeholders is crucial and therefore the coordinated governance of messages, media and planning
- Culture of digital transformation
- How much effort is this going to take?
- How can we make citizens care about E-ID
- Communication to issuers and verifiers
- Relationships with similar groups in other countries - share resources
- Consider how other have solved it:
  - Adoption of biometric passport
  - Adoption of TWINT/wireless banking cards (NFC)
- What story/stories are going to tell to the public (priorities):
  - E-ID
  - Credentials in general
  - Convenience
  - Privacy
  - Security

#### **Onboarding & life-cycle management**

- Initial identification process to get an E-ID (remote)
- How complex is enrollment?
- Is getting the E-ID a point of no return? Like once I get it I cannot get rid of it anymore?
- Who will help me, if it does not work? (holder)
- What is the relationship between foundational ID and digital ID?
- How to get the VC?
- How to use the VC?
- How to back-up VC?
- How to onboard?

- How to back-up?
- How to revoke?
- What if I lose my phone?
- What happens when I get in the hospital (coma) or die?
- What happens with my E-ID when I die? When I cannot use it anymore?
- How is the E-ID updated - lets say i wanted to change any attribute. How does that happen on a process level (non-tech)?
- What all my information (personal) be used to issue an E-ID?
- Recovery possibilities
- I have no mobile phone or internet connection. What should I do? (from private person)

#### **Children etc.**

- Should my car have an ID too? (holder)
- Can I have a trusted person use my ID? I am not good at using digital tech.
- How can I use VCs on behalf of my parents I take care of?
- What do I do with the ID of my small children? When do the ID go to them? 18?, 16? 12? (from private persons)
- Can I also hold the E-ID of my children and share them?

#### **International questions**

- Interoperability with the EU?
- Does it work when I am on vacation? Holder
- I have international customers. Does it work as well? (issuer)
- I have international partners. Does it work as well (verifier)

#### **Devices**

- Can I obtain/use it without a smartphone?
- Will there be possibilities to go full digital and just have digital credentials?
- Do I need a smartphone to hold my credentials and E-ID or is there a web-interface?
- Can I get an E-ID on a "smart-card"? Why not? (for a private person)

#### **Benefits and use cases**

- How do I benefit from this system?
- What are my benefits and risks? (for private persons and companies)
- Ease of life of citizens and companies in their interaction with digital services
- How do I benefit from this system? (verifier)
- How do I benefit from this system (holder)
- What is there in it for me?
- Why should I get an E-ID? Use-cases?
- Which use-cases are available= Where can I find a list? Which organisations are contributing?
- What is in it for me as a citizen? How does it make life easier?
- [Douwe] Appealing use cases, consumers like ease of use, so improvement of existing services at government, banks, telco's, insurance, education => so notably (usually complex) services which involve paper and/or physical displacement. Government / public

use cases have big potential for mass adoption, eg. tax filing, drivers licences, public transport, health care .

- [Douwe] How can providers 'use' the infrastructure to realise data sharing use case, so even beyond PII / SSI data sharing
- [Douwe] Figuring out the incentives for each target group to participate in this effort to 'created the next infrastructure for our digital economy'
- which are the sexy usecases

### **Security and trust**

- How can I trust my data is secure? (citizens and companies)
- Who protects my data? (holder)
- How can I trust this E-ID?
- Why can the holder/user trust the solution?
- Is it reliable?
- How do you keep it private?
- Improve security (ex. no more upload of scan IDs)
- How secure is my information?
- Is it safe?

### **Please no E-ID**

- But we voted against an E-ID!
- What happens if I do not sign up for the E-ID?
- Am I forced to use this? (holder)
- Can my E-ID be limited or completely blocked?

### **Ethics and money**

- How will you ensure the right values are reflected in the design?
- How will you balance incentives to ensure an ethical and user-centric design?
- What does it cost?
- Business case: Who is paying for what?
- Can I make money with this? (issuer/verifier)
- Can I monetize my data?
- Ethics: around data and what the ecosystem allows/prevents (Google pays 1 CHF for my data)

### **Technical questions**

- Why do I have an ID from my bank, insurance, employer? (holder)
- Self-sovereign means responsibility (Selbstverantwortung)
- How is this better than the first E-ID?
- How can I share my identities and certifications in a proper and safe way?
- I have a private wallet and act for a company. How do I separate both? (private person)
- Explaining what is on the registry (users, population)
- Verifiable Credentials: Understandable concept and use?

### **Media**

- Teach the teachers

- Coiffeur
- Small business
- post office
- use potential ecosystem to talk to issuers and verifiers
- well defined communication strategy and sensitive art (no propaganda)
- Different sorts of media according to type of population, official (e.g. social network, TV, etc.)
- Video with sexy use case to explain the usage
- Statistics and numbers of user groups and communication behaviours (demographics)
- Schools, universities, continuing education
- Communicate along use cases, e.g. through banks for account opening
- Instagram
- Youtube
- Discord (discussion)
- TikTok
- Globi-Book (happy to support tim weingärtner, hslu)
- pol.is, ongoing community conversations, online so viral, neighbourhood gatherings, citizen assemblies ([cb@lovevolv.org](mailto:cb@lovevolv.org), please contact)
- Have a mobile info-vaan with hands-on use-cases
- “letter from the future” from citizens on microsite
- tiktok is risky as it could end (?) the discussion. Message: e-id ist for the young.
- Pro Senectute
- Pro Juventute
- Medien-Partnerschaft (aligned information set)
- Swiss Telcos (reach)

#### Existing Resources

- <https://www.eid.admin.ch/eid/de/home.html>
- How the standard bill with QR-code was introduced in Switzerland
- Polling tools pol.is
- Don't re-invent, use existing definitions, schemas (e.g. schema, org, FHIR, content , not technology)
- DIDAS (intro videos, yotube, HSLU)
- WEF paper
- SSI (Reed Drummel)
- Digital Switzerland Whitepaper

#### Happy to join a working group

- [rolf@rauschenbach.ch](mailto:rolf@rauschenbach.ch), Information Officer E-ID, Federal Office of Justice, Switzerland
- [catherine.fankhauser@sicpa.com](mailto:catherine.fankhauser@sicpa.com)
- [tom@lyons.ch](mailto:tom@lyons.ch)
- [tim.weingaertner@hslu.ch](mailto:tim.weingaertner@hslu.ch)
- [patrick.brouwer@kinegram.com](mailto:patrick.brouwer@kinegram.com), OVD Kinegram
- [peter.janes@abdagon.com](mailto:peter.janes@abdagon.com)
- [michael.shea@thedinglegroup.com](mailto:michael.shea@thedinglegroup.com)

- [allison@proofspace.id](mailto:allison@proofspace.id), Allison Fromm, proof space
- [jeroen.vanderhoeven@innopay.com](mailto:jeroen.vanderhoeven@innopay.com)
- [luethi@procivis.ch](mailto:luethi@procivis.ch)
- [weisgerber@procivis.ch](mailto:weisgerber@procivis.ch)
- kalyan (Ayanworks)
- [e.prosperetti@studioprosperetti.it](mailto:e.prosperetti@studioprosperetti.it), Eugenio Prospeetti, italian e-id expert (lawyer)
- [silvano.tari@abraxas.ch](mailto:silvano.tari@abraxas.ch)
- [cb@lovevolv.org](mailto:cb@lovevolv.org), charles blass, link.bar/cb, nao.is, greencheck.world
- [stephan.hofstetter@secoia-excon.com](mailto:stephan.hofstetter@secoia-excon.com) , Managing Partner / Senior Consultant SECOIA Executive Consultants AG
- [vladimir.simjanoski@blokverse.com](mailto:vladimir.simjanoski@blokverse.com), Blokverse
- [igor.simjanoski@blokverse.com](mailto:igor.simjanoski@blokverse.com), Blokverse

## ***Making Verifiable Credentials SPEAK! VC-based voting/ polling/survey***

**Session Convener:** Nicolas Gimenez, Co-Founder & CTO @ZKorum ([LinkedIn](#))

**Session Notes Taker:** Nicolas Gimenez

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

**ZKorum is an Open Startup, and all our work is open-source. Feel free to join the conversation by contacting me on LinkedIn or by creating an "issue" on one of our GitHub repositories!**

We're working on the first MVP.

ZKorum primarily focuses on social polling, and while the MVP will support electronic voting, it will only be recommended for non-critical votes for a long time. This is due to the need to meet specific compliance requirements for high-stake voting, as well as the ongoing need for the protocol to mature, be thoroughly tested, and undergo audits. Therefore, until both the legal considerations are resolved and the protocol reaches a higher level of maturity, high-stake voting cannot be recommended. There are plans to support high-stake voting in the future, once these crucial aspects are addressed.

Voting, polling, forms, and surveys can utilize the same underlying protocol, which can be found at: <https://github.com/zkorum/poc/blob/main/vc-flow/README.md>.

The presented slides can be accessed here:

[https://docs.google.com/presentation/d/1BjQYW17qs3WsBSb4n1f04ChCZ\\_EyldTw6GOTq48Vks/e/dit?usp=sharing](https://docs.google.com/presentation/d/1BjQYW17qs3WsBSb4n1f04ChCZ_EyldTw6GOTq48Vks/e/dit?usp=sharing).

Regarding conversations:

- In the EU, it may be legally acceptable to use an anonymized version of an ID attribute from an official VC (such as a passport) for registration in a vote/survey/poll, as long as it is explicitly communicated to the user. Certain unique numbers, like the SSN, found in passports or social security cards are heavily regulated and can only be used by authorized agencies or companies. To the best of my knowledge, there is no workaround to conduct voting/polling without utilizing such numbers. However, this usage is limited to the registration process and not the voting/polling itself, which helps mitigate the issue.
- When it comes to data transparency, the choice between a blockchain and an off-chain peer-to-peer network was considered. Immutability is important, but having all data available at all times is not necessary, making a blockchain unnecessary. The data itself contains sufficient information to self-validate its own eligibility and the associated response. Individuals who are concerned can run their own node, and specialized companies can verify that ZKorum is not manipulating or deleting data. The frontend can be configured to connect to different backends (federated servers), including those from opposing political parties and a trusted neutral third-party. Additionally, the frontend can



also listen to votes/polls from a peer-to-peer network, minimizing the required level of trust and maximizing censorship-resistance.

- During the registration process, there is a minimum level of trust required in ZKorum. Theoretically, ZKorum could register a specific user multiple times with multiple secrets if it were corrupted. However, if such a situation were to occur, ZKorum would need to have a personal relationship with the user in order to give more voting power, as ZKorum only receives an anonymized ID from the official VC during registration. In the future, this aspect could also be decentralized.
- The adoption of BBS+ VC is crucial because it provides the privacy and zero-knowledge proof required for our purposes. We hope to see its adoption grow in the future.

## The Big Mountain Behind the SSI Hill (part 2) (How to use “OCA” & “KERI” in Healthcare)

Session Convener: Philippe Page - Human Colossus Foundation

Session Notes Taker: Philippe Page

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

The title of this session refers to a session we made in a previous IIW un-conference. SSI brings decentralised authentication to a new level and opens a new playing field for digital innovations. But despite this great progress, it is just a “hill” compared to the “mountain” of additional considerations that have to be taken into account for adoption at scale.

Governance and Context are the two additional domains decentralised authentication has to grasp with to deploy scalable solutions and sustainable business models.

In today’s session we want to report an update on the progress made since then through practical examples. The session mixes a non-technical presentation and a demo.

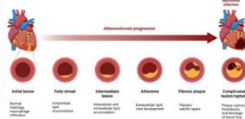
We started with a presentation of the work done in preparation for a EU Horizon project in the domain of accessing sensitive data held in different biobanks themselves located in different

From eSSIF-Lab to NextGen - a mini Health data space in cardiology

Scenario #6 Myocardial Infarction risk prediction



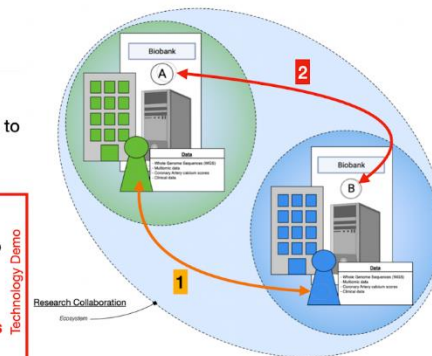
The Barrier to innovation  
lawfull access to data for deep  
phenotyping of atherosclerosis  
plaques



Accredited Researchers are empowered by the Research Collaboration to provide access to specific data located in their respective biobanks

1. Researchers issue & exchange authentication credentials providing access to the data for a documented purpose

2. Researcher B authenticates on Biobank A



countries.

**Key Discussion point:** Decentralised semantics (OCA) provides the architecture to a) structure the meta-data surrounding the context of the access request and b) ensure the integrity of the the meta data and other data object involved in the transaction. (no decentralised authentication required !)

Then we reported the work done as part of the eSSIF-LAB project DKMS-4-SSI the development of libraries to introduce a KERI architecture in SSI solutions.

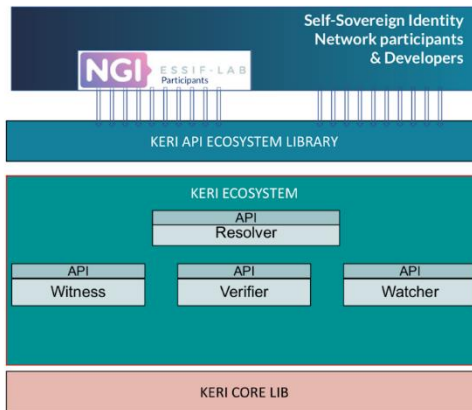
**No magic** - Face the complexities under the hood  
Users remains unaware of the ambient infrastructure intricacies

**Accredited Researchers** are empowered by the Research Collaboration to provide access to specific data located in their respective biobanks

1. Researchers issue & exchange authentication credentials providing access to the data for a documented purpose

2. Researcher B authenticates on Biobank A

Infrastructure



**Key Discussion Point:**

KERI offers a truly decentralised key management infrastructure

Our project builds libraries on top of the KERI core libraries to support SSI applications developers. The libraries developed can be used across multiple root of trust. Centralised (i.e. DNS), Oracle (i.e. DLT) or KERI.

The eSSIF-Lab EU Horizon 2020 project terminated with the proof of concept as per above slide. Works on this topic continues with an enterprise version of these libraries developed by MeDDEa Solution.

The work done was displayed through a short demo including:

- Credential Issuance by Researcher A including an OCA bundle

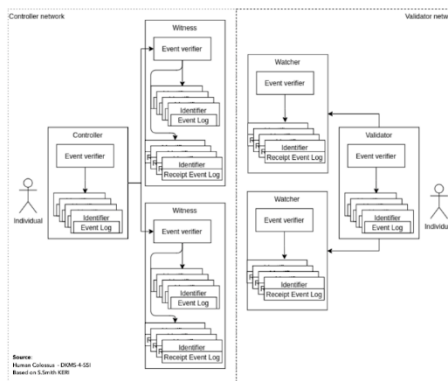
**No magic** - Face the complexities under the hood  
Users remains unaware of the ambient infrastructure intricacies

**Accredited Researchers** are empowered by the Research Collaboration to provide access to specific data located in their respective biobanks

Demo using

OCA Architecture  
KERI Architecture

Infrastructure



- Credential usage by Researcher B to access a virtual machine via an SSH connection

## W3C VC-Edu Task Force: Verifiable Credentials for Education

Session Convener: Dmitri Zagidulin

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 from the intro session:

<https://docs.google.com/presentation/d/1iTVPEYOAn6XxNAVEYvBHTXJYi-5Mz3jLao2XB-TFTXI/>



**Danube Tech** @DanubeTechNews · Jun 8

🌐 Live from **#DICE2023** in Zürich a session from our CEO @peacekeeper and Azeem about **#DIDs**, the Universal Resolver and Universal Registrar **#DIDResolution** **#DIDRegistrar** **#DICE2023**



## Universal DID Operations (resolve, create, update, deactivate)

Session Convener: Markus Sabadello, Azeem Ahamed

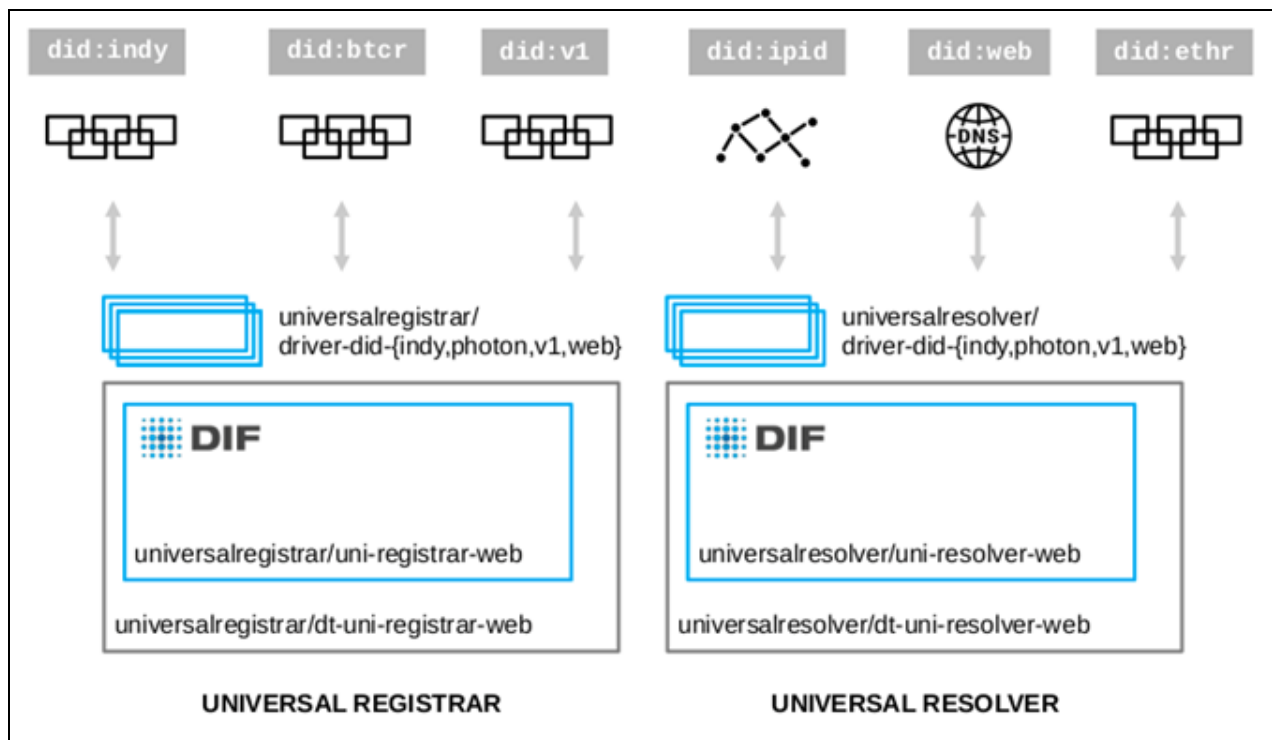
Session Notes Taker: Markus Sabadello

(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.

Links:

- <https://w3c-ccg.github.io/did-resolution/>
- <https://identity.foundation/did-registration/>
- <https://dev.uniresolver.io/>
- <https://uniregistrar.io/>
- <https://godiddy.com/>



## SESSION #3

### *US SVIP - Digital Wallets & Verifiers Solicitations / SVIP Program Info.*

Session Convener: Anil John  
Session Notes Taker: Charles Blass

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

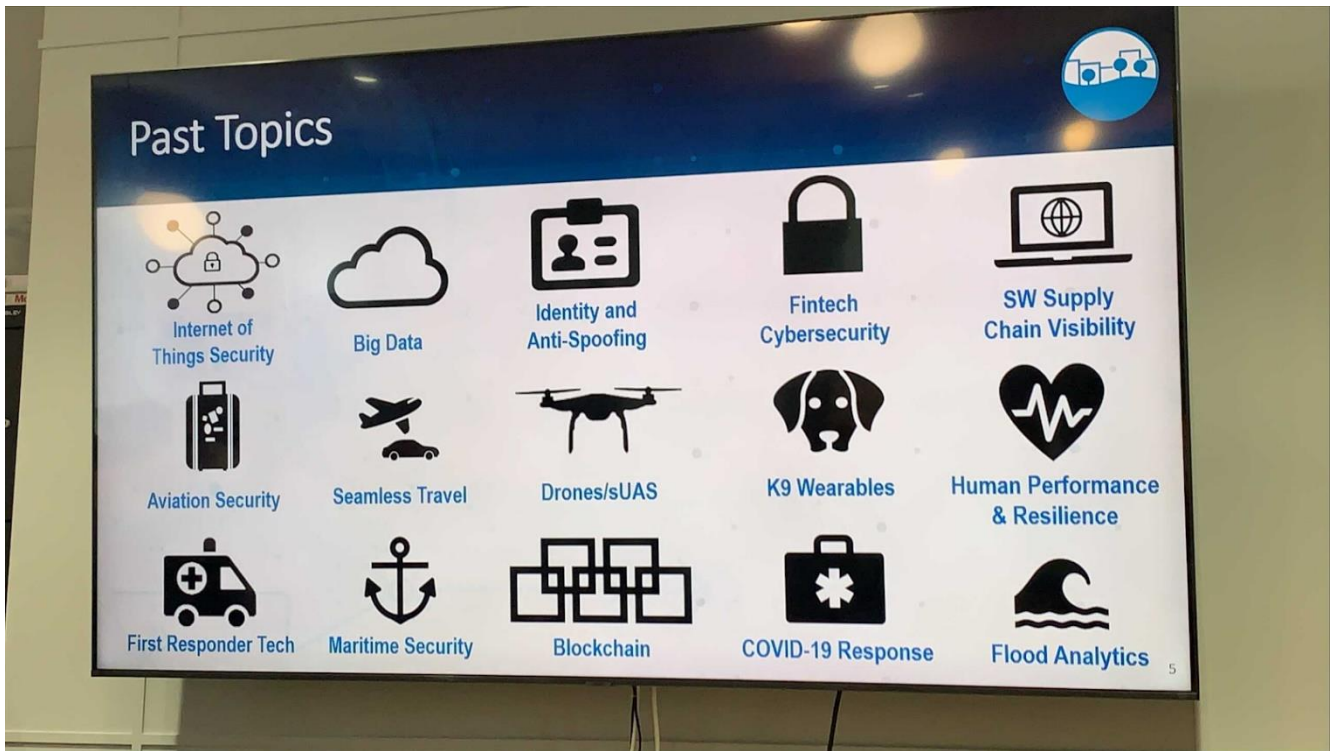




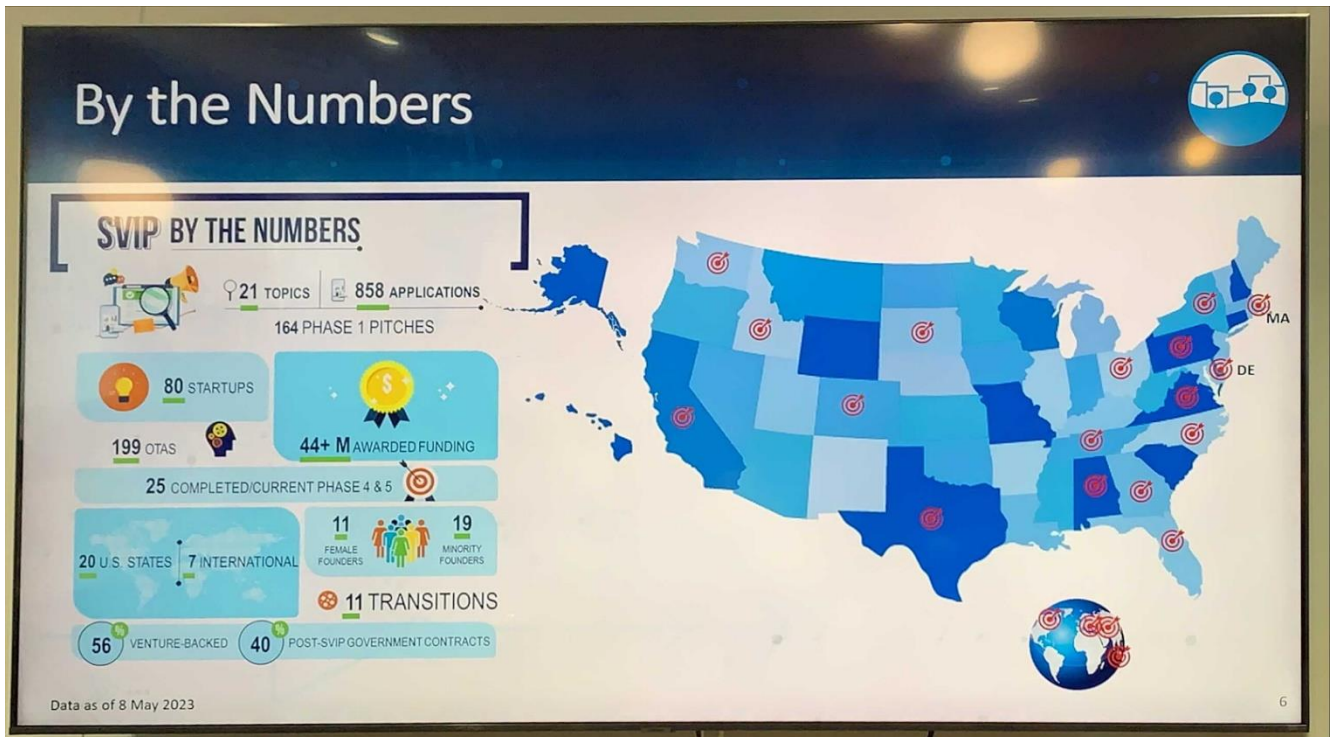
"technical arms buyer"  
 30-45 days to contract  
 no IP taken from startups  
 IP remains with you and not with the government  
 we want to empower companies



"multitracking"  
 funding multiple companies  
 up to 2mil per company  
  
 program is completely unclassified



eg fitbit for dogs (at airports, borders etc) - health monitoring



"SV" branding but really international  
 "talents knows no borders"



# Eligibility to Participate in SVIP

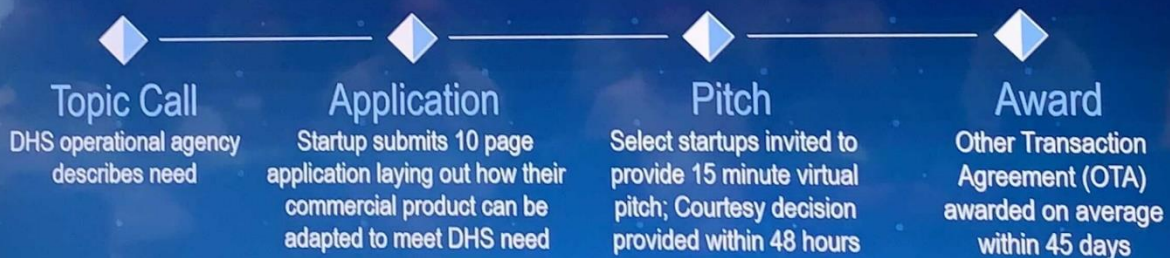


- Have a Unique Entity ID from SAM.gov. DUNS numbers no longer required as of 4/4/22.
- Have less than 200 employees. This must take into account and include affiliated businesses, such as parent companies and subsidiaries, that are either in or outside of the USA.
- Have not been a party to any U.S. Federal Acquisition Regulation- (FAR) based contracts and/or federally awarded grants totaling more than \$1,000,000 in the past 12 months, whether as a prime contractor or subcontractor. This total includes SBIRs.
- Do NOT have any Cost Accounting Standards Contracts with the U.S. federal government

7

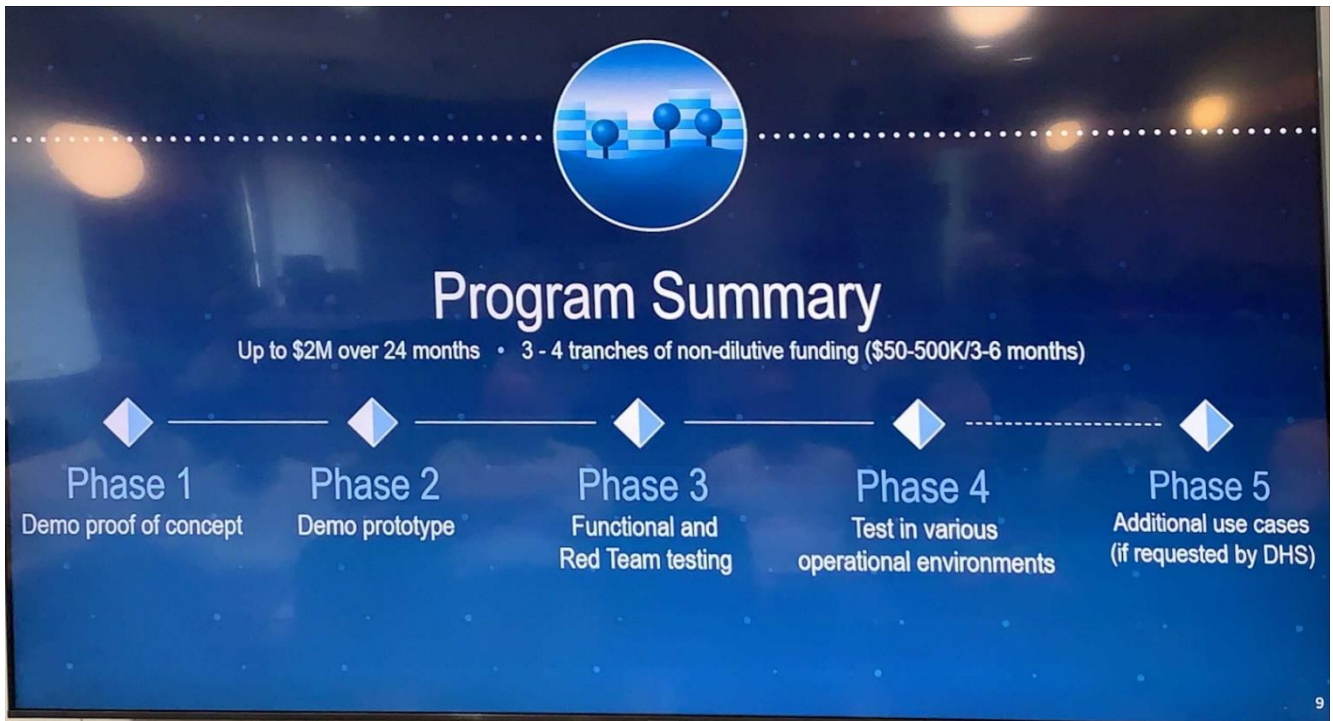


## Application Summary



8

decision within 24 hours



"red team"  
 Untrusting scenarios...  
 Under NDA  
 Operational testing

End of phase 4, expectation to have commercial product, roadmap - product to be bought outright




# Privacy Preserving Digital Credential Wallets & Verifiers

TTA 1 – Digital Wallet  
SHALL incorporate one or more OSL(s)

TTA 2 – Mobile Verifier  
SHALL incorporate one or more OSL(s)

Open-Source Libraries (OSLs)

- OSL (A) – Cryptographic Tools SDK
- OSL (B) – Sealed Storage SDK
- OSL (C) – Metadata Management SDK
- OSL (D) – Confidentiality and Integrity Protected Computing SDK



PRIVACY PRESERVING DIGITAL CREDENTIAL WALLETS & VERIFIERS

- Open Global Solicitation
- Application Information @ [sam.gov](https://sam.gov)
- Application Deadline is 15 September 2023 12:00 PM PT

11

- want to support building products, plus broader ecosystem
- Need to deliver open source sdk + closed source/ commercial product
- Incentivizing building, patching, improving over time
- bake in incentive to maintain codebase over time
- Operational agency, without the luxury NSF has, eg to advance science
- Not R&D like NSF
- Teaming up to apply? Every single company need to comply - don't want to deal w/ drama
- Operate at speed of startup, not speed of government

## PRIVACY PRESERVING DIGITAL CREDENTIAL WALLETS & VERIFIERS

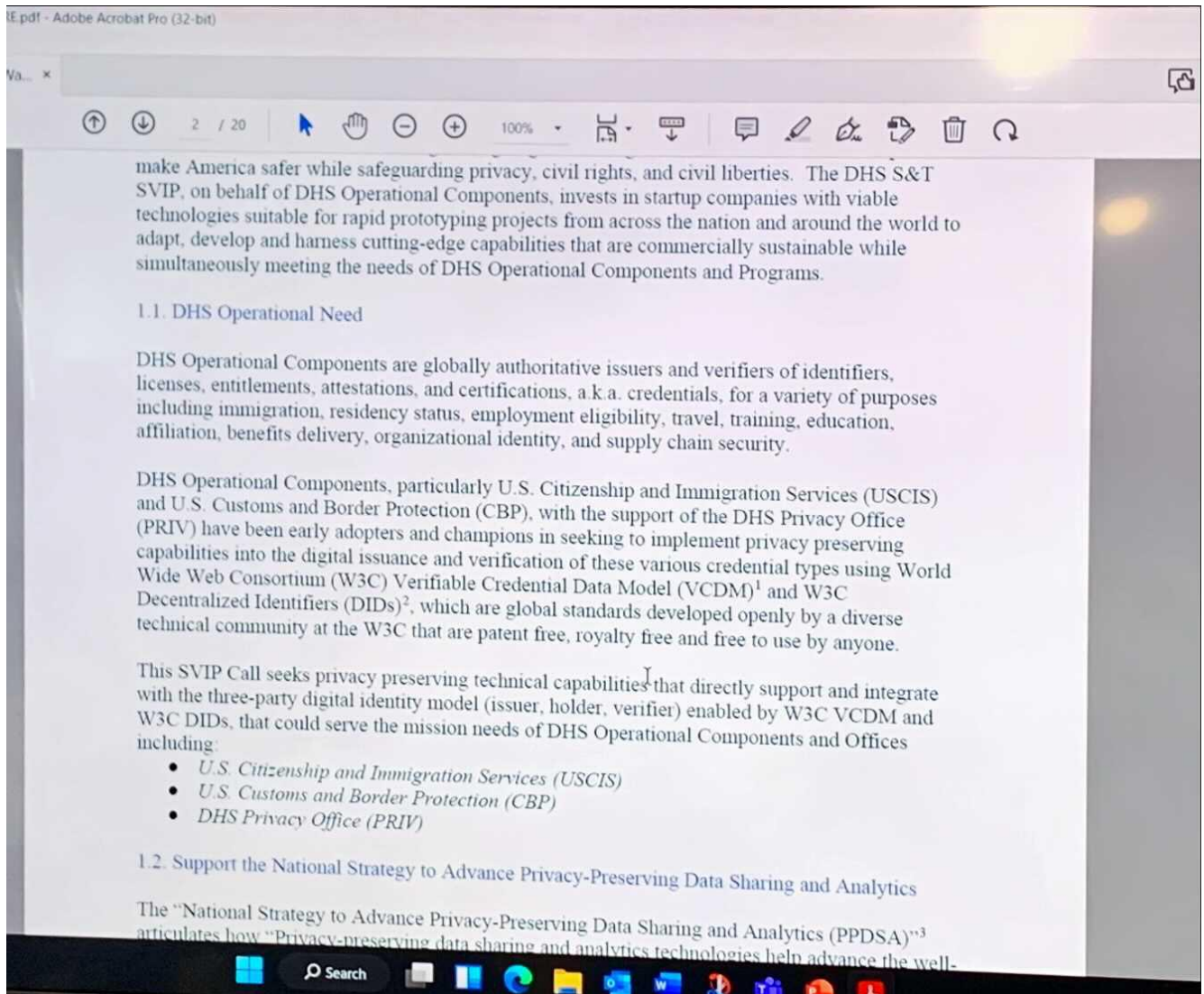
Other Transaction Solicitation Call  
70RSAT23R00000034

INDUSTRY DAY  
Privacy Preserving Digital Credential Wallets and Verifiers  
August 18, 2023 | 10:00 A.M. to 12:00 P.M. CT

Application Forms @ [SAM.gov](https://sam.gov)  
Application Deadline  
15 September 2023, 12:00 PM PT

<https://www.dhs.gov/science-and-technology/svip>

pay attention to main sponsors



see "Support the National Strategy..."

discusses value of open source and collaboration

not R&D,

-> shaping product

"scenario wording" giving themselves maximum leeway in future scenarios

expected that an applicant will use one or more of these solutions in their application.

### 1.3.1. Scenario I: DHS Issuing Credentials to a Digital Wallet Holder

USCIS administers the nation's lawful immigration system and is responsible for the issuance of documentary evidence of citizenship, immigration, and employment authorization.

The application of technologies sought in this Topic Call could potentially enhance USCIS capabilities to:

- Issue digital immigration credentials to a CBP Mobile Digital Wallet e.g., CBP One Mobile Application, to meet the needs of the Western Hemisphere Travel Initiative (WHTI);
- Issue digital immigration credentials to State Partner Government Digital Wallets e.g., California DMV Open-Source Digital Wallet, for use by their residents in online and in-person interactions;
- Issue digital immigration credentials to Digital Wallets assessed and approved by our International Partner Governments e.g., Government of Canada, the European Union Member States etc., such that the holder can assert U.S. immigration status, residency, and employment eligibility with both public and private sector verifiers; and/or
- Issue digital immigration credentials to Digital Wallets that meet DHS requirements for security, privacy, and interoperability, such that the holder can assert U.S. immigration status, residency, and employment eligibility with both public and private sector verifiers.

CBP, as the United States' first unified border entity, takes a comprehensive approach to border management and control, combining customs, immigration, border security, and agricultural protection into one coordinated and supportive activity.

Intense signaling, "we will have a digital wallet in play, not sitting on the sidelines"

"requirements for security, privacy, and interoperability"

- Verify DHS issued W3C VCDM/DID credentials and other authoritative documentation at web, kiosk and in-person infrastructure, stored in Digital Wallets assessed and approved by our International Partner Governments e.g., Government of Canada, the European Union Member States etc., in support of relevant online and in-person interactions; and/or
- Verify DHS issued W3C VCDM/DID credentials and other authoritative documentation at web, kiosk and in-person infrastructure, stored in Digital Wallets that meet DHS requirements for security, privacy, and interoperability, in support of relevant online and in-person interactions.

## 2. Topic Description

### 2.1 Topic Call Conventions

The International Organization for Standardization (ISO) uses specific verbal forms to convey clarity on what is a requirement and what is a recommendation or other type of statement. This Topic Call adopts and uses the following ISO document conventions:

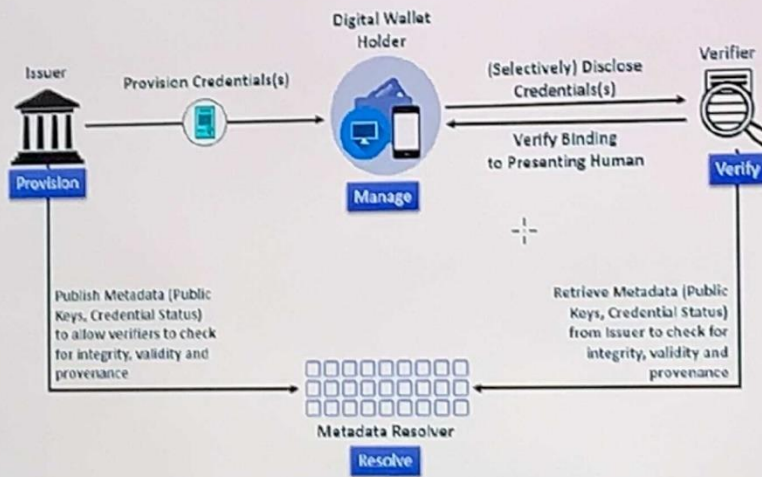
- Requirements - SHALL, SHALL NOT
- Recommendations - SHOULD, SHOULD NOT
- Permission - MAY, MAY NOT
- Possibility and Capability - CAN, CANNOT

# PRIVACY PRESERVING DIGITAL CREDENTIAL WALLETS & VERIFIERS

SVIP OTS Call 70RSAT23R00000034

## 2.2 Assumptions and Constraints

Applicants are assumed to know the concepts and terms presented in W3C VCDM and W3C DID global standards.



NOTE: The W3C VCDM Standard identifies an abstract component called a “Verifiable Data Registry” which in DHS implementations is referred to as a “Metadata (or Public Key) Resolver”

DHS implementation of digital credentials using the W3C VCDM and W3C DID standards have the following principles that we consider critical in meeting the expectations and needs of our global customer base, that must be part of any proposed solution:

- Support for selective disclosure capabilities to provide the holder of the credential granular

JSON-LD - linked data, valid json-ld

o W3C JSON-LD SHALL define all types using @type

o W3C JSON-LD SHOULD leverage objects instead of strings to refer to Issuers and Holders

o W3C JSON-LD MAY rely on @vocab to automatically define terminology

Credential Data Model Proof Format

- Verifiable Credentials, as defined in W3C VCDM, SHALL be secured using the Data Integrity Proof format
  - o Data Integrity Proof format SHALL implement mandatory U.S. Federal Information Processing Standards (FIPS) Compliant Cryptography
  - o Data Integrity Proof format SHALL implement interoperable security engineering best practices
  - o Data Integrity Proof format SHALL implement interoperable privacy engineering best practices
- Verifiable Credentials, as defined in W3C VCDM, MAY be secured using the JSON Web Token Proof format
  - o JSON Web Token Proof format SHALL implement mandatory U.S. FIPS Compliant Cryptography
  - o JSON Web Token Proof format SHALL implement interoperable security engineering best practices
  - o JSON Web Token Proof format SHALL implement interoperable privacy engineering best practices

Providing Credential Provisioning and Credential Presentation APIs that are publicly documented, patent free, royalty free, non-discriminatory, and available to all mitigates technology and vendor risk to Issuers, Holders and Verifiers while simultaneously providing technology providers the ability to build innovative and value-added solutions behind the API.

To that end, the following are specific items to be incorporated into each Technical Topic Area (TTA) listed below to ensure that solutions are secure, privacy respecting, scalable and interoperable:

data integrity proofs required which supports parallel signatures

Require DIDWeb support

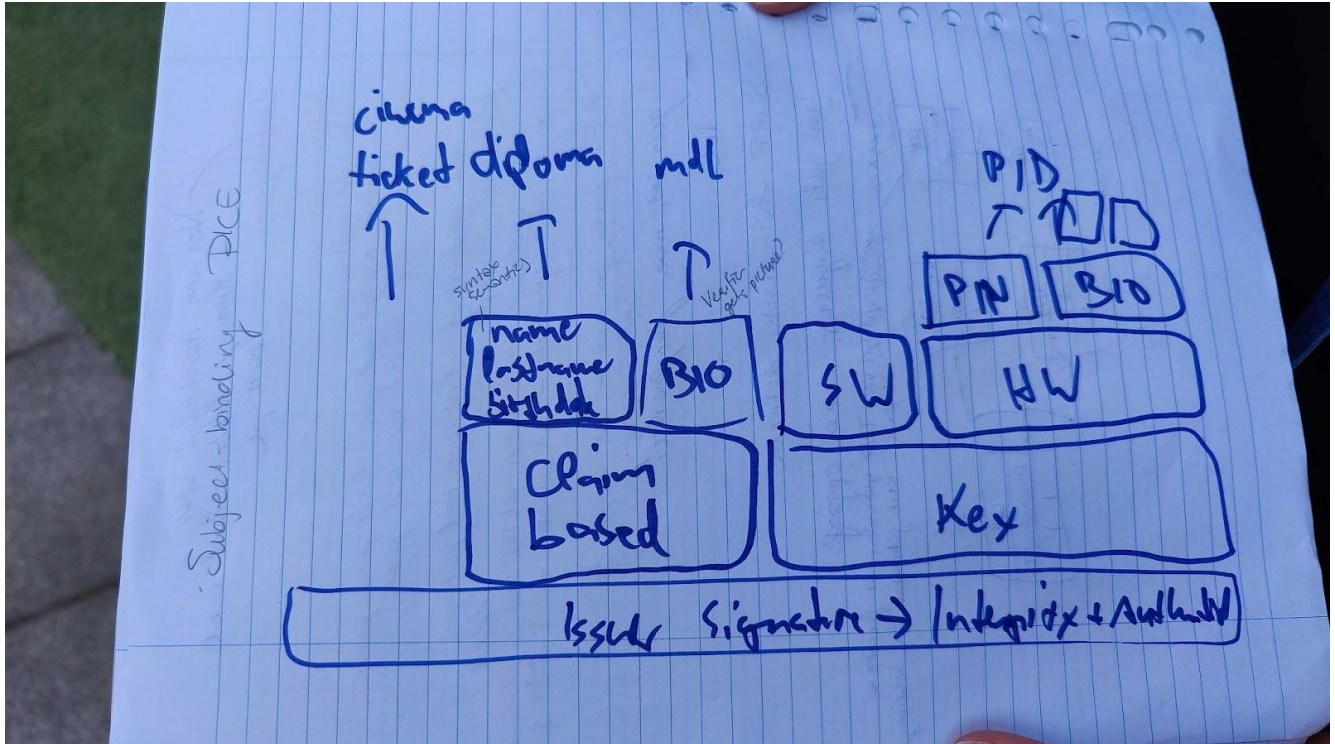
## How to solve subject binding?

Session Convener: Maaike v. Leuker

Session Notes Taker:

(optional) List of Session Attendees: Paul

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





## *Does INDY Have a Future? / @ Giorgio Zinetti CTO Procivis AG*

**Session Convener:** Giorgio Zinetti

**Session Notes Taker:** Giorgio Zinetti

**(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.**

[Indy future](#)

### **Findings**

The audience agreed that indy (referencing the whole stack (indy, aries, didcomm, anoncreds etc..)) is harshly judged sometimes, being one of the most used stack it has been under more scrutiny compared to other solutions.

It makes much more sense to pick the individual layer technologies and discuss them separately

It makes sense to separate the protocols from the implementations.

Indy as a whole remains the best privacy preserving stack

We agreed tha indy 1.0 including all tech elements is probably not going to make it. however some parts of it in a 2.0 version could make it in the mid term.

Didcomm is the most feature reach protocol and enables many more use cases compared to other protocols

Anoncreds in the current form are not viable

- they can't be stored securely in hardware
- computationally expensive

## *Hopepunk Futures: What are our stories*

**Session Convener:** Will Abramson

**Session Notes Taker:**

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

This was a broad discussion about the concept of hopepunk fiction as a powerful tool for exploring alternative, positive possible futures for digital ID.

More information about hopepunk can be found here: <https://beforewegoblog.com/purity-and-futures-of-hard-work-by-ada-palmer/>

Then an example of a hopepunk anthology containing a collection of short stories focused on the broad theme of digital identity in times of crisis can be found here:

[Stories from \(un\)Identified Worlds](#)

If anyone is interested in writing hopepunk fiction around digital identity, I would love to start a casual writing group to play around with this. Contact me if you are interested at [wip.abramson@gmail.com](mailto:wip.abramson@gmail.com).

## *VC lifecycle, especially recovery in face of the national E-ID*

Session Convener: Mike and Sven

Session Notes Taker: [Mike](#) and [Sven](#)

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

Notes from the session: (slides below)

- Pseudonym feature is only required with type 1 wallet. Type 2 wallet does not require it, since backup restore of keys is possible
  - this is correct, but then you still cannot rollover keys for type 2 or recover from key compromise or change keys or algorithms.
- How does the Pseudonym VC concept compare to cloud wallet.
  - cloud wallets use same key regardless of the device that is involved in the SSI exchange with an issuer or verifier.
  - To rollover keys or cryptographic algorithms forces all the VCs in the wallet to become unusable so that they have to be reissued.
  - If the credentials for accessing the keys are lost, there are two options:
    - The keys cannot be recovered
    - The keys can be recovered meaning that the cloud wallet provider has a method of establishing access to the keys without the holder being involved
  - If the keys are compromised in the cloud wallet, all the keys must be revoked and all the VCs in the wallet become unusable
- Trust in the E-ID is on same level as PP
  - There is no need for the E-ID issuer to operate the PP issuer. They can be operated by separate organizations.
  - The attack vector on the PP is somewhat more difficult. It is correct that the PP could issue a Pseudonym VC for a 3rd party. The third party still would need gain access to the VC associated with this Pseudonym VC to abuse the VC.
  - It is probably desirable to have the PP operate on the same trust level as the E-ID issuer.
  - Follow-up questions that have not been discussed during the session:
    - is it useful to have multiple PP?
    - Is it useful to have PP of different trust levels?
- PP is only involved during the issuance of the Pseudonym VC.
  - The PP is not involved in the transactions with issuers or verifiers
  - The PP at no time gains access to any claims stored in VCs
  - The PP must identify the holder during a registration process. This can be achieved using an E-ID or another process of the same quality.

- Where is the data?
  - The data is at the issuer
  - The data is in the VCs in the holder wallet
  - The data may be in a VC Backup (local, cloud)
  - The data may be shared with verifiers if the holder consents.
- Would it help if the usability of Pseudonym VCs is somehow limited
  - This was suggested but not discussed in depth during the session:
  - Could we impose a time limitation on the Pseudonym VC to prevent abuse of the recovery function?
- Is a self-managed PP possible?
  - 
  - technically yes.
  - Are there vulnerabilities or undesired side effects with self-managed PPs?
    - A potential attack was discussed:
    - The holder of a VC can generate Pseudonym VCs for other holders to share a VC.
    - Example: a holder shares a concert ticket.
- How does revocation work?
  - The revocation mechanism itself has no special requirements.
  - Partial revocation is possible i.e. revoke all pseudonym VC associated with the keys in a single device

## IdP Assisted Recovery

### Recovery is challenging in SSI context

- Life cycle management is a strong requirement for national E-ID
  - Onboarding
  - **Replacement**
  - **Loss/Recovery**
  - **Parallel use of multiple devices**
  - **Compromise of keys**
  - Retirement

# Problem Statement

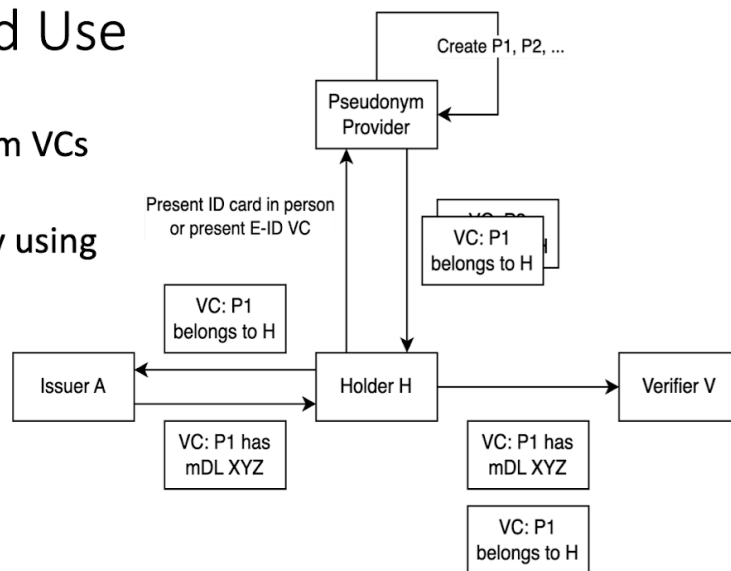
- **Master Secret Issue**
  - Requires backup/restore for management
  - Hardly acceptable for a national E-ID solution (e.g. ARF Type 1 wallet)
- **Privacy**
  - Cannot share Holder DID or reveal Link Secrets
    - Loss of correlation resistance
    - No multi key DID methods easily possible
- **Ease-of-use**
  - Recovery requires restore of each credential individually
  - Effort required by holder, automation hardly possible

# Different Approach

- Can holders use multiple DIDs?
- Use individual DID for every issuer (pseudonym DID)
  - Unique identifier for the holder
  - Correlation resistant identifier for issuers
  - Inject Pseudonym DID in every VC issued by this issuer
- Pseudonym DID are issued as VCs by a Pseudonym Provider
  - Lifecycle management operations need only be solved by the Pseudonym Provider
  - Recovery: Pseudonym Provider issues a VC that links a new Pseudonym DID with its predecessor.

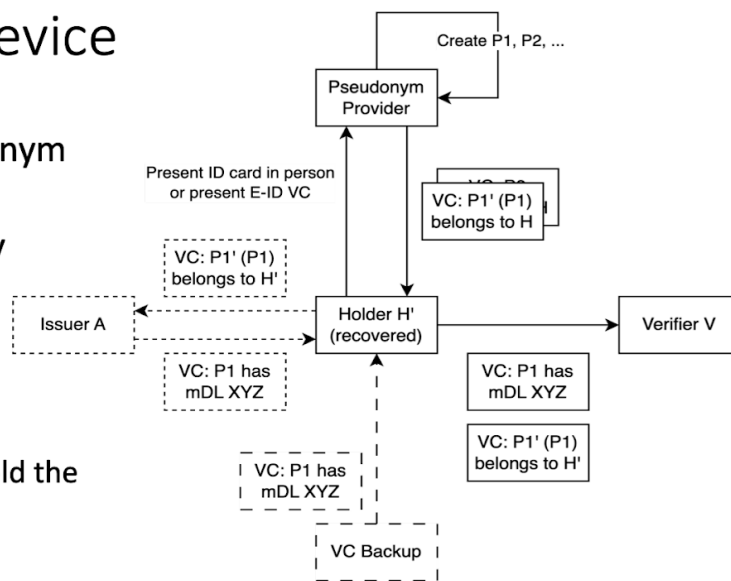
## Initial issuance and Use

- Holder acquires pseudonym VCs from provider
- Provider can verify identity using any method
  - In-person check
  - Present national E-ID VC
  - ...
- Holder supplies selected pseudonym VC in every interaction



## Recovery / New Device

- Holder re-acquires pseudonym VCs from provider
- Provider can verify identity using any method (as before)
- Holder recovers VCs from backup or issuers
  - Can re-use them as they hold the same pseudonym VCs



## *Get an Overview of Technologies to Implement SSI*

**Session Convener:** Richard Zbinden

**Session Notes Taker:** Richard Zbinden

**(optional) List of Session Attendees:** unfortunately no software developers showed up to help to build an overview. Fortunately two people were tech savvy.

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

Georg Greve and Vasily Suvorov gave some insight into their views on the subject.

At the core level I understood that SSI enhances the traditional authentication and authorization technologies with at least one challenge / response check with VC in order to make sure that both parties can trust the other party.

As a happy guy I was approached by Maaïke van Leuken who kindly provided a reference where to find an overview: <https://www.tno.nl/en/newsroom/insights/2023/05/what-those-ssi-standards/>

## ***Kicking off an SSI Agent Comparison Task Force***

**Session Convener:** [Samuel Rinnetmäki](#) / Findynet

**Session Notes Taker:** Samuel

**(optional) List of Session Attendees:**

- Douwe / Innopay
- Michael / Curity
- Cat
- Nicola
- Isaac Henderson
- Jacques / Bhutan
- Rob Schwartz
- Kaliya
- some others whose names the notes taker missed (add yourself if you were present)

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

If there was a curated list of agents (issuer, holder, and verifier wallets) including the technologies and capabilities they support, ..

- organizations (or consultants supporting those organizations) could use the list to shortlist/select the technologies suitable for their use case and environment (weather buy or build) and contact the potential solution providers
- organizations who have already chosen their technologies could use the list when benchmarking their choices with other organizations
- an issuer or verifier could use the list when finding out which wallets to support or seeing how much support there is for a certain credential format, issuance protocol, etc.
- an ecosystem could choose their methods and technologies for trust registries and revocation based on what wallet's are supporting
- an ecosystem could endorse wallets to their members and users based on whether the wallets support the methods and technologies for trust registries and revocation based that are selected for the ecosystem
- Interoperability between wallets could improve when there's more visibility on what's supported by whom

In the next phase, the list could be enhanced to include information of the kinds of interoperability profiles, requirement sets, etc. the agents/wallets conform to. That would be very useful as a support for decision-making. At some point of time, the list could also contain information about which solutions are trusted, vetted, certified, etc.

We discussed about the capabilities and information that should be collected. In the list below, the properties that were added during the session or discussed particularly, are bolded.

- **Wallet**
- **Provider**



- Holder wallet
- Issuer agent
- Verifier agent
- API/SDK
- License/Pricing
- Credential formats
- Signature formats
- DID methods
- Protocols
- **Verifiable Data Registry**
- **Trust list mechanisms**
- **Revocation methods**
- **Transferability**
- Comments
- E-mail (commercial contact)
- Support address (e-mail)
- Website
- App Store
- Google Play
- Web
- Source code

*After the session, Samuel was introduced (by [Maaike](#)) to the Github resource <https://github.com/tno-ssi-lab/wallet-overview> and the associated website <https://tno-ssi-lab.github.io/wallet-overview/> which contains a lot of the content for above, but only about holder wallets. Samuel and Maaike will collaborate to combine the efforts and to extend the current wallet overview to include information about issuer and verifier agents.*

We had a discussion about transferability (import/export or backup/restore). We concluded that in some cases it is desirable or OK that the holder can copy a certificate to multiple wallets (requires also copying the attached private key). In some cases that should be strictly forbidden. (Some tickets shouldn't be duplicated. Copying keys creates new attack vectors.) The Bhutanese wallet allows very sophisticated backup/restore system which only allows one instance of the wallet to be active at a time.

There was also an off-topic discussion about the relationship between Findy Cooperative (provider of Finnish trust ecosystem infrastructure) and Findy Agency (Aries-based open-source identity agency project). Findy Agency is developed by OP bank who is a member of Findynet Coop. The cooperative and the project share the same name and even the same logo and are linked through OP, but don't have a direct connection at the moment.

## SESSION #4

### *A Framework for Wallet Security - device binding - holder binding - wallet authentication - DEMO /*

**Session Convener:** Paul Bastian, Micha Kraus, Markus Kreusch, Sebastian Bickerle  
**Session Notes Taker:** Markus Kreusch

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

#### **Presentation**

- Motivation & eIDAS 2.0
  - Trust triangle of issuer, holder and verifier
    - Much attention on trust relationship between verifier and issuer
    - Less attention to a trust relationship between issuer and holder and verifier and holder
    - Special attention required for governmental VCs
  - eIDAS 2.0 Architecture Reference Framework
    - Covers regulated and non-regulated issuers
    - Type 1 and 2 configuration for different security levels
      - Type 1: high assurance, hardware bound
      - Type 2: other credentials
    - Several protocols and
  - Binding types for PID & EAAs
    - Simple issuer signature
      - bearer token
      - e.g. cinema ticket
    - claim based binding
      - biometric & PII claim
      - e.g. diploma, on-site mDL
    - exportable software keys
      -
    - non-exportable keys
      - PIN / password
      - e.g.
- Wallet Architectures
  - Cloud vs. local wallets
  - Focus on local wallets
- The Journey
  - 2021
    - prototyping proprietary wallet attestation in the ID wallet
    - project provided valuable learnings
  - 2022
    - starting the DIF wallet security working group

- prototype with Lissi based on DIDComm & AnonCreds
  - 2023
    -
- Regulations and Tools
  - Regulatory requirements
    - protection against
      - credential duplication/theft (extraction)
      - online/offline guessing (impersonation)
      - others... (not wallet relevant)
    - wallet enables issuer to achieve a certain level of assurance (LoA)
  - Mobile market
    - several mechanisms available but fragmented market
    - software and whitebox crypto not really secure
    - a<zTEE, strongbox and secure enclave in the middle range of security. combined a high market share
    - secure elements, eUICC, eSIM: high level of security but a low market share
- Three Pillars
  - Device binding: authentication factor possession
    - hardware backed crypto very restrained
    - no ZKP support (long time till support is available)
    - NIST P256 as the smallest common denominator
    - no backup / recovery possible
  - User binding: authentication factor (knowledge/biometry)
    - local on-device
    - Biometric have many challenges and security issues
    - Regulators are still in favour of PINs
  - Wallet authentication (integrity and authenticity of the wallet)
    - mobile OS with less-trusted, complex layer in front of trusted, high secure hardware key storage
    - iOS device check, Android SafetyNet/Integrity API
    - Key attestation (not available on iOS)
- Attestation Process
  - Holder wallet will create a hardware key for device binding
  - It will contact the attestation service and present a wallet authentication proof
  - The attestation service can be run by the wallet publisher or a trusted third party
  - The attestation service issues a device attestation vc
  - This vs is later presented to an issuer that wants to issue a credential into a trusted wallet
  - The issuer checks the attestation vc and can bind the hardware key to bind the issued credential to the wallet
  - The issuer issues a credential
- Summary
  - End to end demonstration of a wallet attestation and issuance has been done
  - Enabling eIDAS (Type 1) configurations
  - Next steps

- IETF Draft for “Attestation based client authentication for OAuth 2”
- Incorporation of the concept into OID4VCI
- Trust list management
- ...

### **Sidenote on Level of Assurance (LoA)**

Only the issuer can reach a certain level of assurance because he is the only party that has control over all the security choices (user authentication, wallet security, revocation, ...). Wallet security is only a part of this.

### **Questions and discussion**

- Is there a benefit for putting more logic into secure components of a smartphone?
  - It is good to put as less logic in there as possible. It is really complicated to put and update logic inside of the secure components. As long as there is not a secure display it does not make sense to put more logic in there because in case of a rooted phone everything shown to the user could be faked.
- How do you handle wallet updates?
  - The attestation VC has an expiration date. Depending on the validity duration of this VC it must be renewed regularly.
- How would something like this work for web wallets?
  - In general this would work the same way for web wallets. As long as there is an attestation VC issued by the web wallet it should work there as well.
  - Backend enabled web wallets store private keys probably in an HSM etc. So a comparable security level is possible.
  - Open question: How do we authorise the usage of the HSM in the backend? If the level of security of this method is lower than the one provided by the HSM the actual level of security is lower than provided by the HSM.
- In order to leverage iOS and Android, were you able to do a modern business relationship permission by the parties?
  - No special agreement in addition to the standard app developer setup required
  - Quota of 10k requests per day exists, request for more (paid) possible
  - If the APIs change: Issuer and verifier do not need to change anything because of the way the attestation VC is used
- How is this related to common criteria certification?
  - Doing a common criteria certification on apps is not possible
  - Secure element and eSIM are common criteria certified
  - Secure enclave is in between, did part of the process but did not complete it
  - TEEs are not certified and not that strong

## ***Trust Registries for global Interoperability & The Role of Trust Frameworks in two-sided Markets***

**Session Convener:** Isaac Henderson (Fraunhofer) & Douwe Lycklama (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.**

Introduction Douwe:

- How to make (horizontal) infrastructure attractive for everybody in society (that it works for everybody, like roads, sewage, GSM) without discrimination
- It is all held together by a trust framework -> technical, legal, business,
- Unified expectations for a trust framework (speed limits, wheels, steering wheel on the right) -> made possible by a range of coherent technologies
- Where is this concept of trust frameworks in the conversation we have right now for SSI/ID
- What are our minimum expectations
- It can start local but grow global based on best practices. So scope is irrelevant right now

Introduction Isaac:

- How to create an approach for trust registries that is globally interoperable
- How do we make trust registries globally interoperable?
- eIDAS trust lists should be open

Discussion:

- "Path of least resistance is the best way to get adoption" -> it has to be something we want rather than something that is pushed
  - However, some things are pushed on us, like payment methods
- "Ethics should be at the forefront of our discussions"
- Even though certain companies might try the path of least resistance, most of the times the relevant trust model is missing (e.g., EU citizens cannot use mDL because it is not issued by the governments)
- Trust frameworks should be built around permissionless access, where parties that want to join the framework simply follow the steps that should be taken (e.g., downloading relevant stacks)
- "Governments can usually overcome the game theory to create the right governance and 'force' incentives on the right party, and initiate a governing role to ensure a trust framework is created"
- "What governance do we currently already have, what is already working well?"
- "Governments shouldn't provide the trust, only the accountability models that ensure the right trust and governance"
- "Governance should be extended beyond what we currently have as regular methods to solve the trust problem, e.g., using decentralised DNS or DAOs"
- "Regardless of which technology should be used, there are many moving components right now in the market, so we need to determine on what is important now"

- "Decentralising the onboarding component: but who then determines who can be trusted?"
- "Common communication should be developed that signals shared expectations (e.g., EUDI Wallet is accepted here in this store)"
- "How do you create an ecosystem in which trust and governance is built from the bottom-up"
- "At one point, people will just trust the system, like we now trust telephone calls to be secure"
- "Technology doesn't dictate, it enables"
- "People need to experience these solutions first, before they will start to question the current practices (e.g., experience SSI and being able to see your data)"
- "Trust frameworks could be go back to individuals actually choosing themselves who to trust"

*Ask the Swiss eID team everything ;)*

**Session Convener:** Andreas Frey Sang

**Session Notes Taker:** Zoé Blanchard / Christian Heimann

**(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.**

Public Sandbox, is there an API we need to connect to?

Transactions can be sent via an endorser connection (based on the protocol). This is based on the endorsement protocol from aca-py.

Why do we need an internet connection for the public sandbox?

One of the public sandboxes goals is to emulate the functionality mentioned in the law draft referencing the "base-registry".

A main aspect of that is a public identifier look-up, that is why you need to be connected to the internet. Additionally in order to write things on the registry, you need an internet connection. You could combine that with an issuing solution and people can verify your credentials while connecting to the sandbox and check your published information (identifier/public key).

Why a certain tech stack? Why Indy?

At the beginning, starting from scratch, the point was to get hands-on experience to understand SSI and so be able to write a law that makes sense and allows the technology to progress. Indy is quite a mature stack which can cover a lot of aspects of the trust diamond - so it was a good starting point.

Distributed aspect (ledger/registry) will be the choice of the final technology?

We do not know at the moment, since we are in the process of making a technology evaluation, but our current gut feeling is rather no.

Opinion and challenges with trust registries for the Swiss eID Team?

Difficult topic because no dominant design patterns or global standards are available yet. plan so far: verified DIDs for the public organisations, and then later the wider ecosystem relationship model based on the type of credentials (designated issuers, designated verifiers, potentially also on the claim basis)

Can I have multiple wallets and therefore eIDs issued by you?

In the first law proposition we were thinking of only one eID at once. Through the consultation we gathered a lot of questions and feedback regarding the need to possess multiple credentials.

How will the issuing of the electronic identity be done?

Most likely there will be 2 ways of receiving an eID.

Biometric verification online as well as an in person process at the passport office for the ones who might wish this.

What wallet to use for the eID?

The Law proposal says the eID as well as other credentials can be stored by the user in their means of choice.

The issuing (the biometric verification) will happen in the governmental wallet and then there should be a step to deliver the credential to third party wallets.

Certification for wallet necessary?

The law proposal is not suggesting such currently. If someone wishes to build his own wallet, he would be able to use it. The ordonnance will be written in a following step. It is possible that the ordonnance will give a certain set of requirements which need to be fulfilled.

Public consultation process?

Two phases in the lawmaking process. Parliament first gave us the task to come up with a new law. Informal consultation was set up, to know in which direction to go. A majority of the feedback went in the direction of SSI and an open trust ecosystem. After that, last summer the first law proposal was put online for two months for every citizen and organisation to give their opinion/feedback on the proposal (117 responses). Questions, good hints and criticism were taken into account and the proposal was revised. Now the law proposal is under internal consultation in the government and in the summer the federal council could accept it and give it to the parliament to debate and hopefully come into force.

Could we know what is in the law that will be debated in the parliament?

The report of the feedback gathered during the public consultation, stated there were no major issues revealed, so you can expect no huge changes. We cannot say more at the moment.

But what about forcing the cantons to use the eID?

There was never mention of using eID only but of obligating to use eID along their own other solutions. Here we can think about the AGOV (Authentication Service of Swiss Authorities) project which has been recently advertised as a supporting solution for the cantons and local municipalities.

AGOV for whom and for what?

For citizens to authenticate themselves to governmental institutions.

AGOV is:

- Identity Provider (classic)
- Identity federation
- eID verifier to connect the old world to the new ssi world.

Communication between AGOV and eID will have to be made very sensitively for the wider audience to understand. Bringing two products at the “same” time can be complicated. It is a very dynamic domain we are facing and we will have to see how the architecture of the solutions will evolve.

Requirements for issuing in the Swiss gov ecosystem?

One goal we follow to let the ecosystem flourish is to keep the barriers low enough for many actors to be able to issue their credentials.

Backup system for the swiss wallet, is there an update on that yet?

The law proposal was tried to be kept tech agnostic, we just say that the government has the right to provide something, giving the possibility. We had a lot of feedback to transform the “could” provide a backup into a “must”. In which way we included those feedbacks in the second version of the law cannot be disclosed yet.

Further points discussed but not listed in detail:

- Competition with other potential Wallet providers
- Decentralised Identity vs Centralised Backups



## ***Biometrics, Credentials & Privacy***

**Session Convener:** Sebastian Zickau, Iain Corby

**Session Notes Taker:** Sebastian Zickau, Iain Corby

**(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.**

### **IDunion results for a proximity use case**

(presented by Sebastian Zickau)

#### **Scenario: Age verification for club access**

Bouncer

- check authenticity of DOB typically from ID
- shall check binding between visitor and ID (face check)
- might not be trustworthy
- 

Club visitor

- must provide ID (incl. irrelevant data, e.g., address, ...)
- has no control for what the data is used for (gets even worse with automated ID checkers)

#### **Objectives**

- Enable the verifier to check the binding between the user and the legitimate holder of a credential with a biometric portrait image.
- Protect the user's privacy by preventing the leakage of the portrait to the verifier, i.e., copying of high-quality image.

#### **Properties**

- Biometric reference: transfer? which quality? authenticity check?
- Biometric comparison: automatically or manually?

#### **Device engagement**

- Each variant needs an established (peer-to-peer) connection between the user's and the verifier's wallet. This could usually be established by the user scanning a QR code.

#### **Variant Overview**

- Variant 1: Transmission of full biometric reference to verifier
- Variant 2: Disclosure of biometric reference on holder's screen
- Variant 3: Holder device verifies biometrics

Prerequisite

- Used credential format and signature scheme may support

Selective disclosure

Age attestation in zero knowledge fashion (>18?, >21?, >67?)

### Detail Variant 1 and Subvariants

V1.1 (manual verification, no verifier wallet attestation)

- Low cost
- Manual (human) biometric verification
- No verifier device check
- mDL variant

V1.2 (manual verification, attested verifier wallet)

- Middle cost
- Manual (human) biometric verification
- Attested verifier device check (attestation)
- Could be an mDL variant

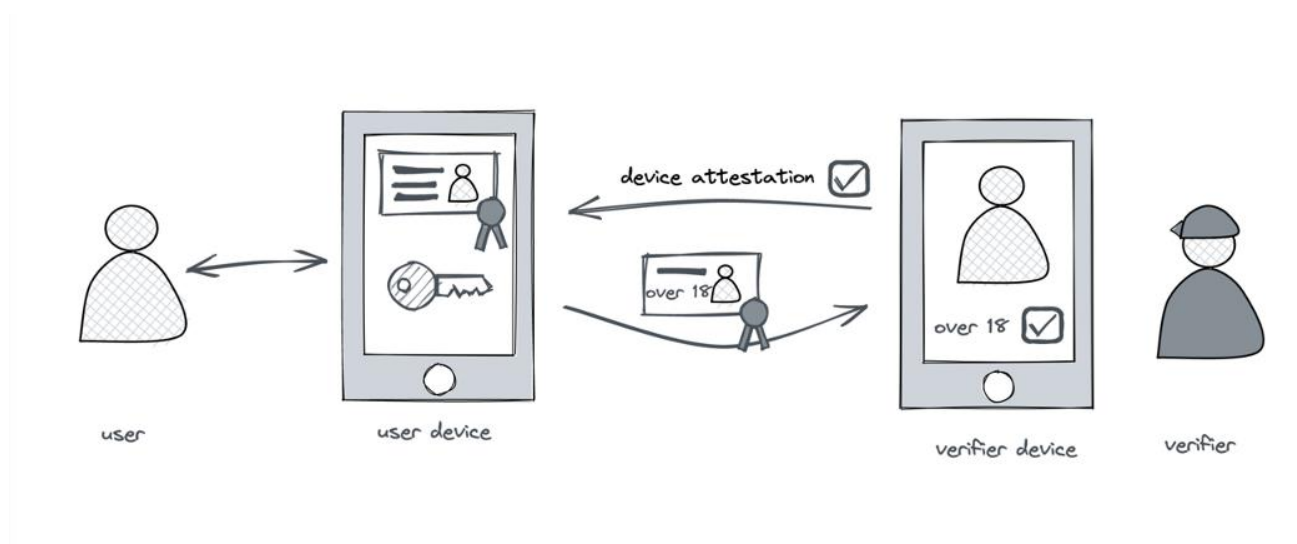
V1.3 (automatic verification, attested verifier wallet)

- High cost
  - Automatic (technical) biometric verification
- Automatic verification also be possible on holder device
- Attested verifier device check (attestation)

Privacy issues

No protection against copying or saving the image including additional data, such as DOB, time and place

Variants 2 and 3 address this



### Detail Variant 2 and Subvariants

Variant 2.1

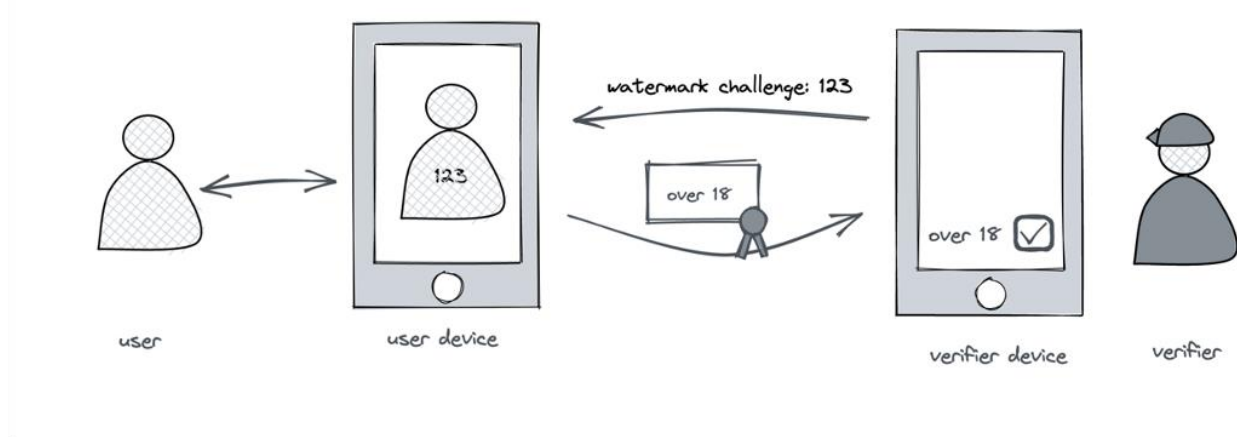
- Low cost
- No holder attested device/wallet check

Variant 2.2

- Middle cost
- Holder attested device/wallet check

## Consideration

- User does not transfer any biometric data to the verifier
  - Shows a portrait on his own device
  - This variant excludes all biometric modalities that need algorithm support, e.g., iris, fingerprint, and therefore applies for manual face control only
  - This variant's challenge lies in the verification of the authenticity of the user's portrait
  - Unlike variant 1, the portrait is not part of the transferred proof and the user's display cannot be trusted by default
  - So a malicious user could present a portrait of another person which is not the subject of the age proof
  - Challenge is: How can the age verification be bound to the portrait?
- Idea also used in Yoti Age Check for retailers.



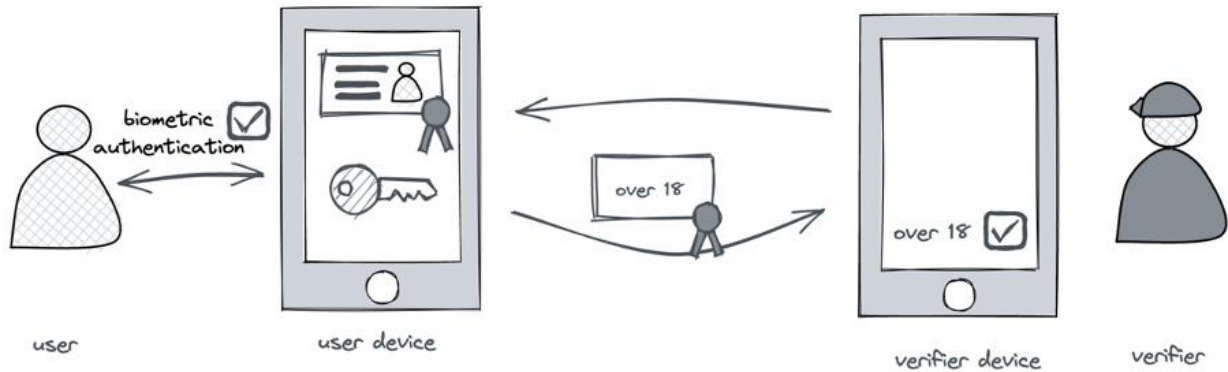
## Detail Variant 3 and Subvariants

### Variant 3

- Holder Wallet attestation
- Verification of biometric verification result

### Considerations

- Indirect automatic biometric verification on user's device (on-site identity credential with biometric)
- The verifier gets biometric verification result from trusted user wallet
- Uncertain binding, unsupervised, uncontrolled enrolment on user's device when using Android/iOS system components → biometric attributes from other persons could be used?!
- Idea: private/public key pair is generated and stored on device. User proves via challenge, that biometric unlocking has happened
- → make sure, that biometric attribute for access cannot be changed for accessing key pair. Prevent biometric user authentication fallbacks, e.g., user PIN.
- Best solution from a privacy perspective, but user binding is difficult to achieve.



### Iain Corby's use case and solution approach

In the United Kingdom, the proof of age standard scheme (PASS) which is already recognised in law as an authority which can issue plastic identity cards is developing digital proof of age. The main challenge is that it licenses a number of independent issuers so there needed to be one common method for validating, the credential and ensuring that the correct user had authenticated before it is used.

Through an open procurement process where both the proposal and the selection were managed through consensus of all the stakeholders, we selected a PKI based solution where each issuer is able to create a encrypted QR code with their app in response to the phone, reading a challenge QR code displayed, either statically or dynamically by the till in a shop, or next to the door staff for a pub, club or casino. The challenge QR code includes some details about the venue which are then played back to the verifier within the encrypted response QR code to minimise the possibility of using a code created remotely for somebody else of a different age. A reader app or software within a point of sale is able to decrypt the response QR code which confirms the users eligibility as over, or under, a particular age.

The user will have the option to display their name and date of birth on the screen alongside the response QR code if they wish to do so, but no personal data will be transmitted from the user device to the receiver device. It can only be recorded visually. With this exception we are otherwise following the ISO 18013-5 mDL standard.

Each of the digital proof of age apps will need to be audited and certified to ensure that the mechanism for authentication is sufficiently robust, for example, it cannot rely on phone based authentication, where more than one face or fingerprint can be stored to unlock the phone.

## ***POC for Wallet Based EHR & Being Part of a SSI Use Case Implementation project on health data.***

Session Convener: [Peter Janes](#) (Piet), [Dominik Geller](#)

Session Notes Taker: Peter Janes

(optional) List of Session Attendees: [Michael Doujak](#) (Mike), [Stefano Limonta](#), [Andreas Abraham](#), [Will Abramson](#), [Leonardo Staffolani](#) (Leo), [Fabian Vollrath](#)

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

### **How shall we proceed?**

- Short intro of group members?
- Idea presentation - Dominik, Peter
- Collaborative brain dump
- Clustering, wrap up

### **Being part of SSI use case implementation on health data**

**Dominik Geller**

#### **Idea**

Building a citizen controlled health data store with focus on EU. Several projects at EU and member state level are ongoing to build use cases and infrastructure related to the ambition of a European Health Data Space. Hygiaso (Dominik Geller) is participating in two: a Horizon Europe IHI consortium project to build this (platform and tools for health data access) across several EU member states, and a German effort on a national hub (Health-X dataloft), which ties to the GAIA-X infrastructure.

Infrastructure and applications are pointless if they are not used, which depends on the value offered to those users to create engagement, reach and critical mass.

We therefore suggest to

- gather those parties, who are willing to connect and offer their service to be included in such an open and interoperable platform (e.g. wallet, id service, patient or citizen offering, healthcare professional offering)
- Gather any of parties who are willing to collaborate to bring and create a GAIA-X health hub to Switzerland

[dominik@hygiaso.ch](mailto:dominik@hygiaso.ch) if interested to participate

### **PoC for wallet-based EHR**

*Peter Janes*

#### **Current Situation**

Various national electronic health record (EHR) initiatives are based on plain text documents («expensive dropbox»):

- Switzerland (opt-in) - Elektronisches Patientendossier (EPD)
- Germany (opt-in) - Elektronische Patientenakte (EPA)
- Austria (opt-out) - Elektronische Gesundheitsakte (EIGA)

National EHRs based on opt-in have almost no content due to serious adoption problems. Instead, personal health data is spread over many siloed platforms in a non-interoperable manner.

Based on increasing practical experiences, there is now wide agreement about a need for **standardized structured personal health data** (both administrative and clinical).

While DACH countries typically have a quite restrictive approach for personal health data (driven by data protection representatives), nordic countries are much more pragmatic (see [webinar](#)). Respective standards would be readily available ([FHIR](#), [SNOMED](#)).

### Existing First Prototype

To move towards structured clinical health data, a first prototype was built («EPD 2.0»). Use cases were chosen along the highest «pain levels», based on workshops with representatives of health providers (hospitals, general practitioners) and a resulting roadmap:

- Medication plan
- Vaccination record
- International patient summary
- Simulated access the EPD

Using existing standards and technologies (e.g. a centralized FHIR-Server), the very first version of the prototype was completed in two months time, also implementing a clean backend and app architecture to address data protection requirements from the beginning.

See the «OnceHealth» [positioning document](#) for more information about the envisaged ehealth ecosystem and a pragmatic approach to get results quickly.

### Idea

As outlined in the [positioning document](#), the **main objective** is to provide a **citizen centric** (vs. siloed) approach for personal health data.

To address the shortcomings of centralized data stores, a proof of concept (prototype) of a **wallet-based personal health record** (PHR) shall be implemented («EPD 3.0»), based on existing standards and the Swiss E-ID sandbox (i.e. Hyperledger Indy, aca-py). To focus on relevant elements, the PoC is time-boxed by purpose and shall be completed by end of 2023, as time is a factor.

A subset of the [international patient summary](#) is envisaged as scope, as specifications already exist.

The main purpose of the PoC is to demonstrate an implementation based on SSI principles to showcase tangible results to potential users and investors for further refinement and funding.

## References

- FHIR standards - <http://www.hl7.org/fhir/>
- International patient summary - <https://international-patient-summary.net/>
- Swiss FHIR definitions - <https://fhir.ch/>
- SNOMED CT - clinical standards - <https://www.snomed.org/>
- [Positioning document](#), ehealth ecosystem «OnceHealth»
- E-ID sandbox - <https://www.eid.admin.ch/eid/de/home/sandbox/sandbox.html>
- Swiss E-ID Github - <https://github.com/e-id-admin>
- Webinar health data and cultures - [https://youtu.be/8\\_oLi-a4Lck](https://youtu.be/8_oLi-a4Lck) (see Youtube channel for more webinars)

## Team's Braindump

- (Dominik) Who is going to pay for it > (Peter) currently a pre-investment up to prototype, which should be a tangible deliverable
- (Mike) Where to get the data from? Where does the structured data come from? ...chicken / egg problem
- (Dominik) Schemas are continuously evolving - using graph databases for flexibility?
- (Mike) EPD - has good core components, e.g. Master Patient Index, emergency access, ...
- (Fabian) Objective - the solution must serve the citizen (citizens don't care about the underlying technology)
- EPD is currently not used
  - no incentive for health both providers and citizens to provide content, hence nothing usable around
  - doesn't solve any problems
- (Peter) Implement use case by use case (see «pizza chart» of positioning document «OnceHealth»)
- (Dominik) Offering services in Europe - with compatible data
  - Finland, Denmark, France

## Contributions

### Potential activities to address

- GAIA-X Hub Switzerland - [GAIA-X](#) > following up with [Georg Greve](#) and [Felix Greve](#)
- [European Health Data Space](#)
- Use cases
  - Lung cancer
  - Long covid
  - Medication plan
  - Vaccination record
  - Long xy (chronic diseases with high burden on patients and health system)

## «Alliance of the Willing»

Interested in follow-up and regular discussion and exchange. Peter will invite based on LinkedIn contacts - interested persons can contact Peter ([Peter Janes](#) on LinkedIn or to [peter.janes@abdagon.com](mailto:peter.janes@abdagon.com)).

### *How can we connect SSI with supply chain?*

**Session Convener:** Pascal Gottret

**Session Notes Taker:** Pascal Gottret

**(optional) List of Session Attendees:** Francois, Nikola Cutura,

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

Interoperable supply chain is all about speaking the same business language. Therefore, there was a focus in this session about the GS1 standard EPCIS 2.0, allowing companies to record their business events in a machine-readable and standardized format. The standard seeks to answer the important questions:

-**What** (Object) was proceeded?

-**Where** was it proceeded?

-**When** was it proceeded?

-**How** (under which circumstances like temperature) was it proceeded?

-**Why** (under which business context like commissioning) was it proceeded?

Concepts about signing, storing and sharing event data were discussed. As EPCIS 2.0 also defines the way of sharing data ("Core query operations"), companies are able to store data in a decentralized and public manner, such as an own web server, where other relying parties can query data. In order to check data integrity and authenticity **hashes of data** would be signed with public resolvable DIDs and stored in a (permissionless) blockchain.

Sharing these kind of data is important in order companies are able to provide traceability of their supply chain and providing carbon footprint information in a **digital product passport**.

Further, we discussed concepts of how products can be **protected with a seal**, such as a tamper proof QR Code. Each product can be tested for counterfeits on site. The QR Code could link to three different URIs:

- A **data integrity check** of the manufacturer itself.
- a **verifiable credential** issued from the manufacturer to the product itself.

An **NFT** with an ownership history as possible extension.



## SESSION #5

### *AI (ML etc) and SSI / Identity in the age of Generative AI*

Session Convener: Dmitri Zagidulin & Tom Lyons

Session Notes Taker: Charles Blass

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

[slides by Dmitri]

# A.I. (ML etc) *and* SSI

Dmitri Z [dzagidulin@gmail.com](mailto:dzagidulin@gmail.com), MIT / DCC  
Tom Lyons

## Summary (TL;DR)

- AI is *here*, and moving fast.
- If you're not following the developments, you may be surprised at what it can do now
- Serious opportunities and dangers (potential for harm)
  
- AI runs on **data**
- The more personal/vulnerable the data, the more powerful the AI. And more dangerous.
- This is where we come in.

## Terminology / Acronym Soup

"If it works, it's not AI" - old AI industry joke

AI - general buzzword, largely for marketing

ALI - Limited AI ("business as usual" / "please do not be alarmed")

AGI - Artificial *General* Intelligence (uh-oh. human-level intelligence). Not here yet.

ASI - Artificial *Super* Intelligence (self-improving / runaway AI). Common fear.

ML - Machine Learning. (main current direction in AI, as opposed to symbolic AI)

LLMs - Large Language Models. Neural networks trained on *large* scraped datasets.

GPT - General Pre-trained Transformer (a neural network / ML method), ca 2018

suggestion to add the word "intelligence" to the jargon list

## Brief History

**1956** - John McCarthy coined the term 'artificial intelligence' and had the first AI conference.

**1969** - Shakey was the first general-purpose mobile robot built. It is now able to do things with a purpose vs. just a list of instructions

**1974-1980, late 1980s to mid-90s** - "AI Winter".

**1997** - IBM's "Deep Blue" defeats world chess champion.

**2011** - Big data / deep learning revolution

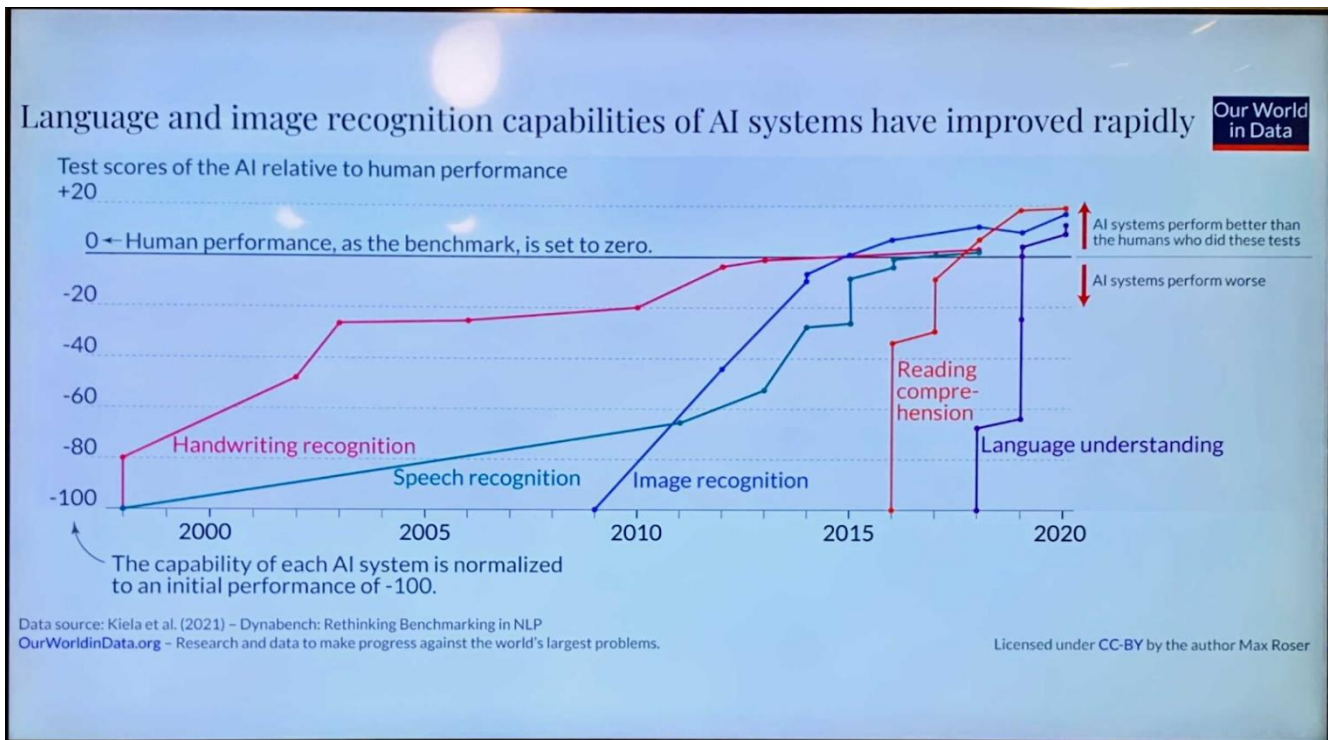
**2017** - **Transformers** paper by Vaswani et. al

**2018** - OpenAI "Improving Language Understanding by Generative Pre-Training", introduces GPT

**2019** - GPT2, **2020** - GPT3 / ChatGPT

**2024** - GPT-4 released

notice how late reading comprehension comes along



- ## What can it (AI / LLMs) do?
- Generate text, images, video (deep fakes)
  - Text: write essays, posts, pass SATs / law entrance exams
  - Writes code (complete software, fragments)
  - Make phone calls, schedule and organize events
  - Make scientific discoveries
  - Generate new protein structures (medicine, bio-warfare agents, etc)
  - Much much more

artists/ creators hard feelings...

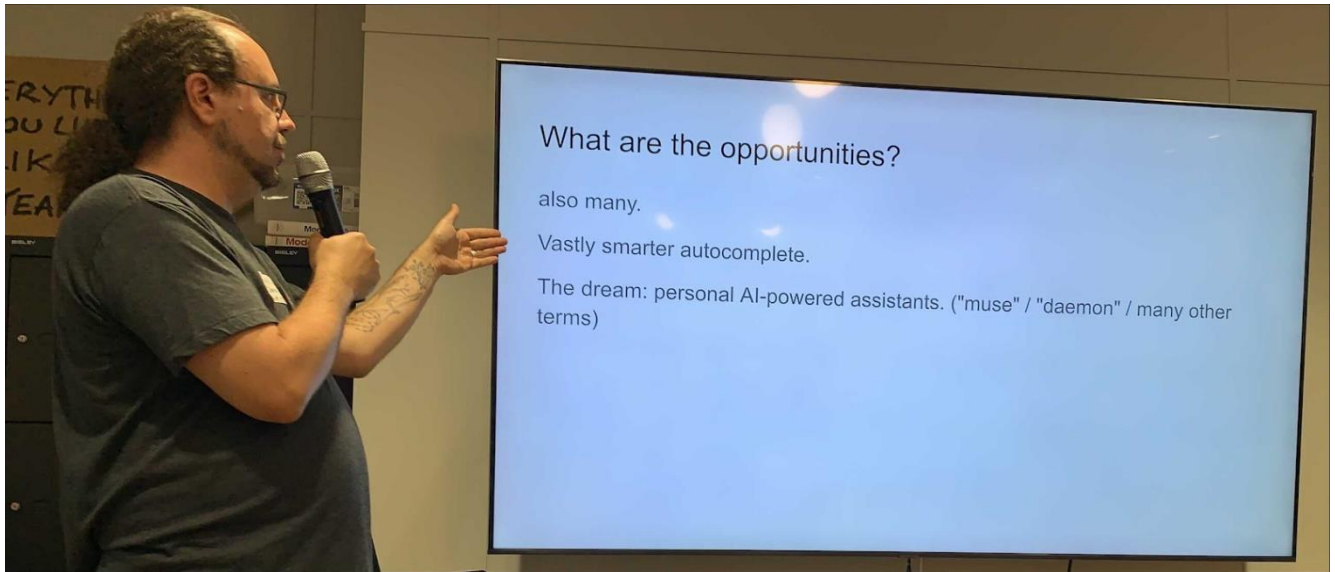
entering the age of deep fakes

acing law entrance exams ...

generating code, training from github

microsoft bought to have massive data sets

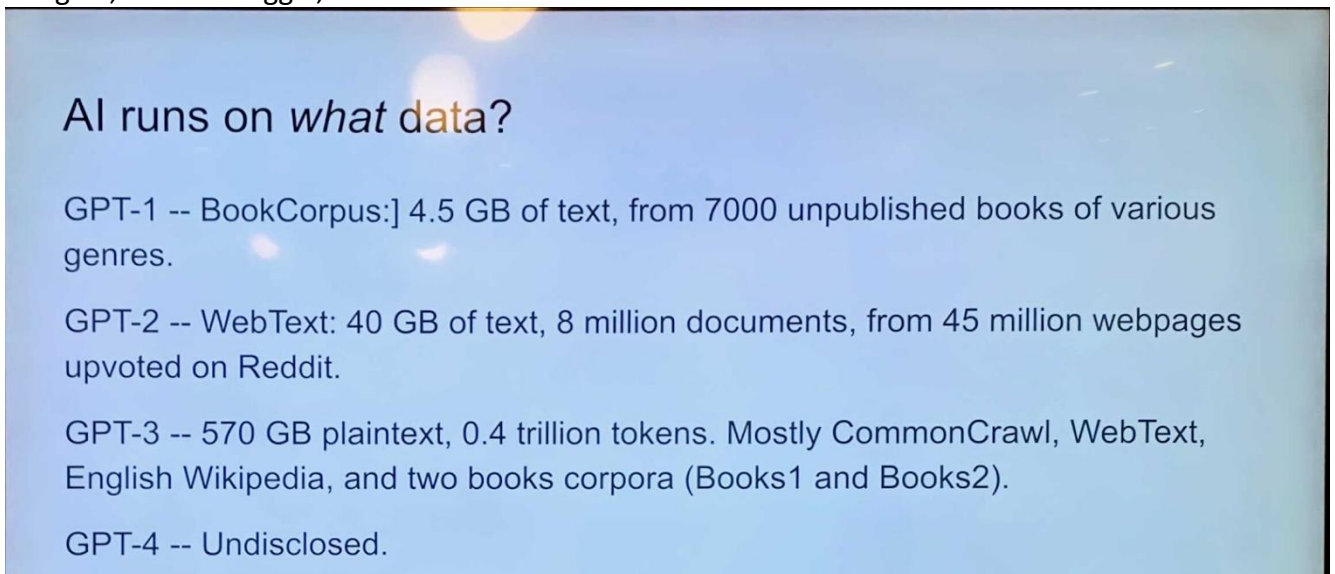
hookup to scientific discoveries



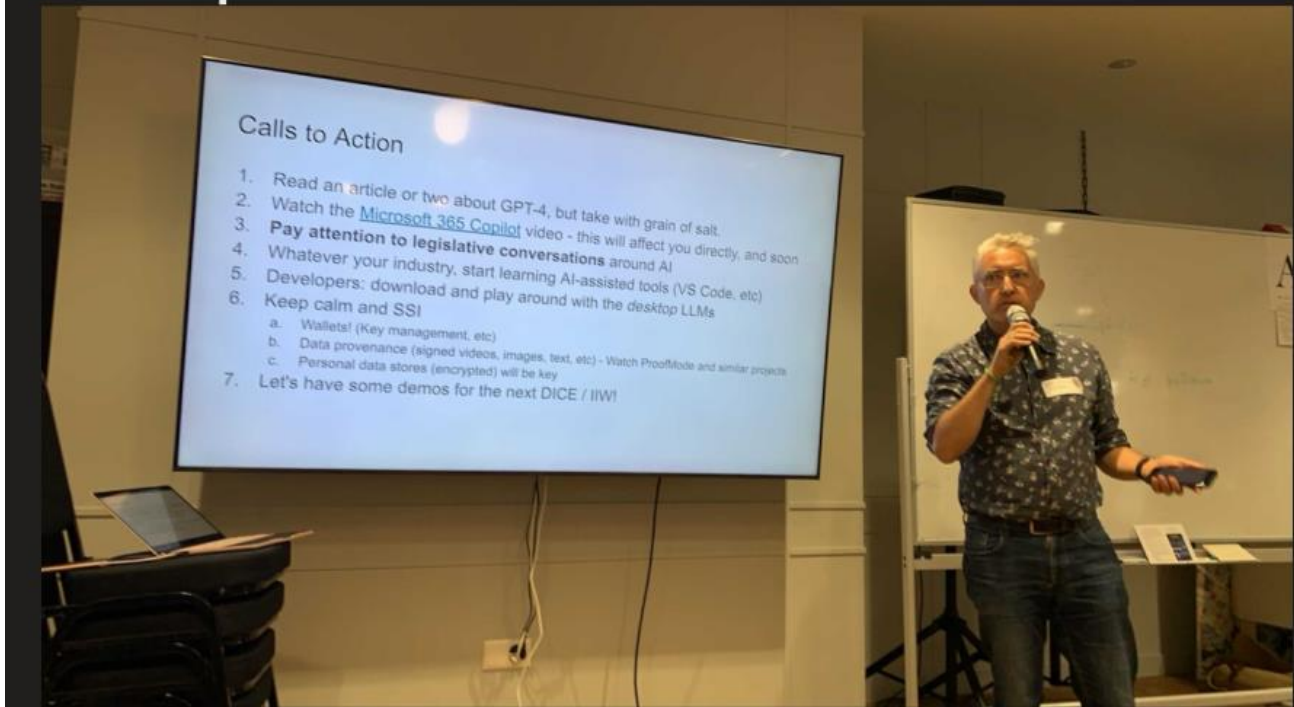
really smart autocomplete

many promises, many hard conversations

dangers, "hoooo doggie, what to do?!"



# GPT4, undisclosed Cb Not "OpenAI"



## Calls to Action

1. Read an article or two about GPT-4, but take with grain of salt.
2. Watch the [Microsoft 365 Copilot](#) video - this will affect you directly, and soon
3. **Pay attention to legislative conversations** around AI
4. Whatever your industry, start learning AI-assisted tools (VS Code, etc)
5. Developers: download and play around with the *desktop* LLMs
6. Keep calm and SSI
  - a. Wallets! (Key management, etc)
  - b. Data provenance (signed videos, images, text, etc) - Watch ProofMode and similar projects
  - c. Personal data stores (encrypted) will be key
7. Let's have some demos for the next DICE / IIW!

Tom bullets/ questions:

There seems to be several main questions here:

- data sovereignty: how can we ensure data sovereignty with a technology that depends on our collective data? Human society has always depended on collective wisdom, so why not allow it to the AI? If an LLM is trained on your content, but does not recreate it one to one, has it really stolen from you? Does the right to be forgotten apply? What if LLMs were based not on data scraping but

on federated learning - sending the compute to the data - would that be on? If you post on the public internet, is not the assumption then that this information is public?

- distinguishing human from machine identities: now that machines can create an almost perfect illusion of human output on their own, how can we distinguish between them? what systems do we need for this? and what rights, if any, does the machine have to an identity?
- Security: how can we prevent AI being used for identity theft? What are the risks?
- regulation: how does this get regulated? also the identity part

CIP.org (Collective Intelligence Project) collab w/ OpenAI et al on citizen assemblies around governance of generative model data

legislative convos, across the globe, participate  
"raise your hand"

some self sovereign data modeling/ machine learning  
very cool, play around with it

can keep model on your device  
or, federate, pass on model to community, becomes more powerful

we need nutritional labels, data provenance

be careful  
confident hallucinations

play w/ lamas (?), wonderful experience to have data sovereignty and play with the modeling/  
training

q. re using synthetic data for training, compared to personal data eg from onedrive etc....

data watermarking  
tamper free guarantee  
no one else is injecting data into your dataset

tom  
chatgpt already biased, based on pre training  
bias is built in  
richard  
with windows 11, there is no local data  
dmitri: can disable...

cb  
licensing for writers/ creators, related to data provenance

algorithmic bias cant be solved technically

human is the weak link  
boils down to self responsibility  
parents, children,, upbringing

robots getting citizenship?

corporate personhood

identity of things

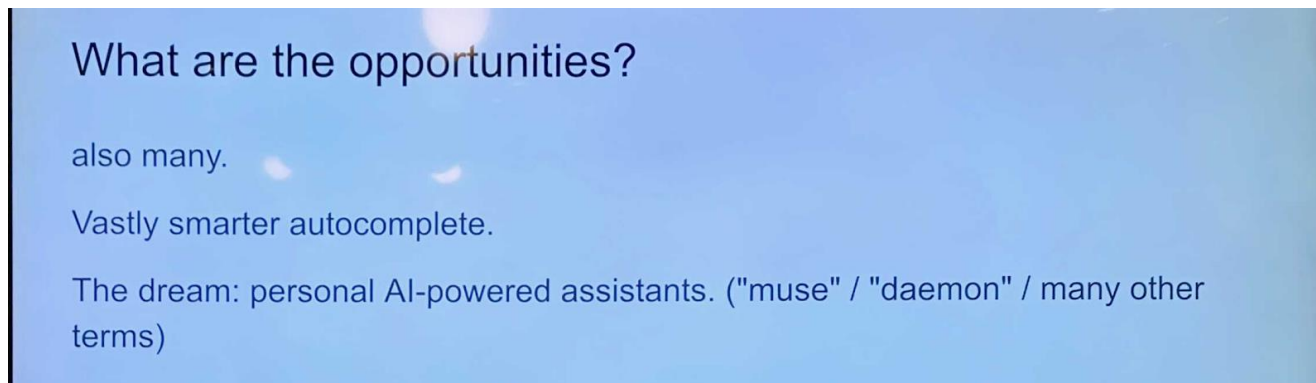
learning unexpectedly, beyond/ outside intentions

legal issues  
incl.cant find out source of bugs

dmitri read recent paper  
“moral crumplezone” car analogy applied to responsibility  
companies currently abusing the notion of self responsibility

next door at mit, automotive intelligence lab  
shutting down research on decisionmaking, companies dont want to disclose thinking processes

tom  
prompting upside, we all become geniuses



dmitri recap

generative ai causing a trust crisis  
so, we need everything signed, using ssi, vcs etc  
interdepartmental conversation

trust crisis means the death of the internet  
cf. google search results from bots etc

## Human experience within SSI

Session Convener: Zoé Blanchard and Marco

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

How to design a wallet for my 60 years old parents?

—> “boring” will to focus on other types of population

How to deal with the conflict btw service expectations and user’s responsibility?

How to mitigate the gap btw usability and control?

How to best involve and to what amount the citizens / user groups to a participatory design porcess?

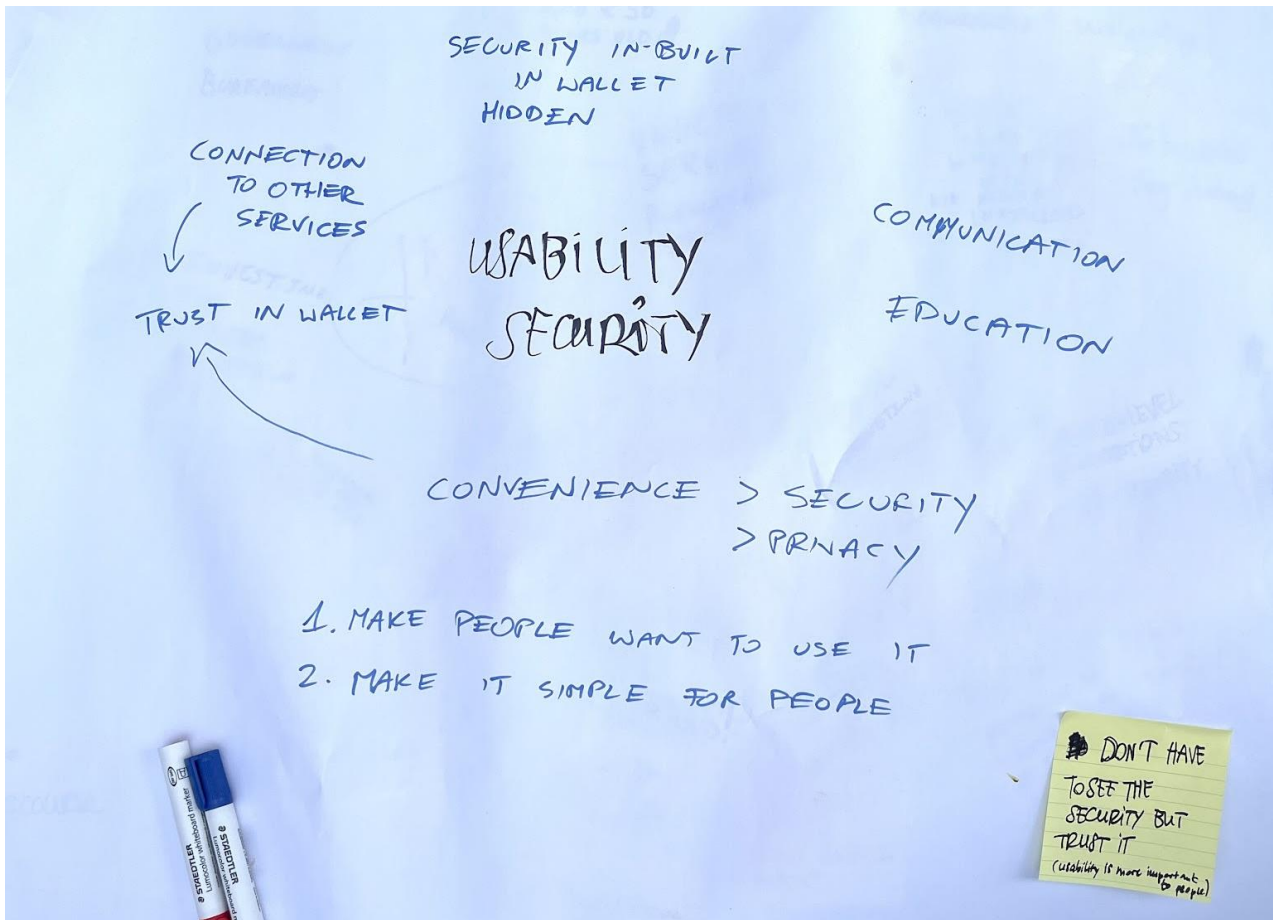
...

First collection of topics and voting to those

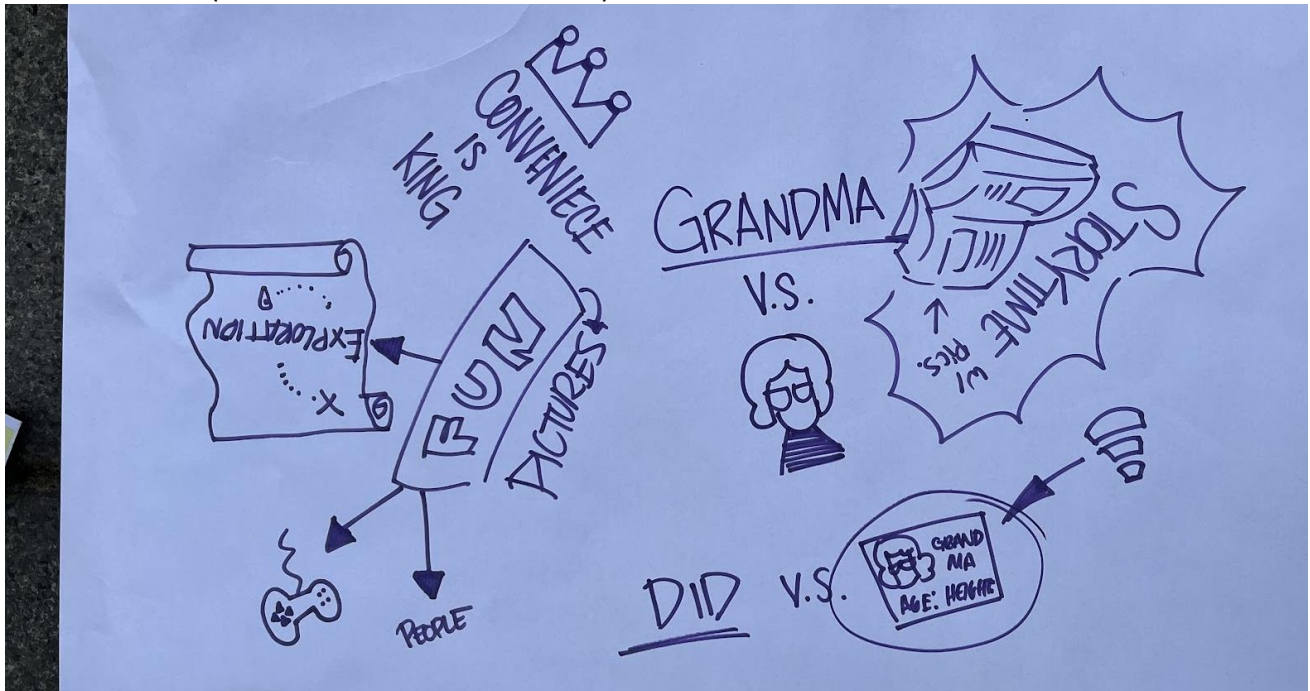


Break-out groups discussions:  
Usability versus security (or “over” security)



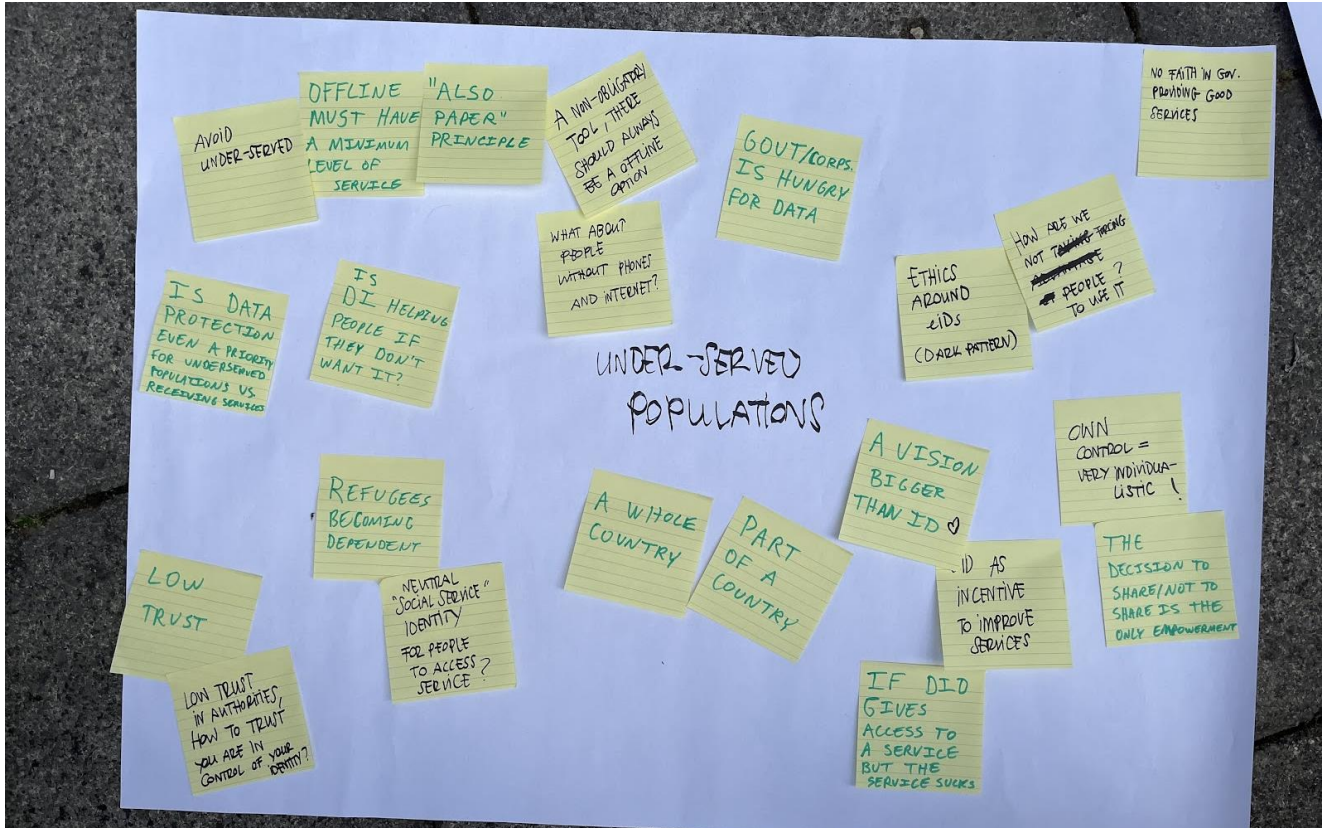


People do not want to directly deal or be confronted with security features but they want to feel or trust the service through built-in security by design.  
Stories and fun (desirable and less serious eID)



Pictures and visual stories to reduce complexity, lower the threshold and illustrate benefits

## Underserved population



Offline processes are to be enforced and supported as well and it is the mission of a state (offer access to all)

Low trust in gov and its services can be a big barrier → how to lower this threshold? Is a digital product around eID the solution?

Any person living in a country (Switzerland case) having an official accreditation from the authorities is entitled to the eID. → What about the undocumented? Is there gonna be a "neutral" identity (like there has been during covid to access to tests)?

eID as an incentive to improve services

To give the whole control to users is a very individualistic view. One, especially the state, should not expect for everyone to navigate safely around this new technology.

Alerting mechanisms are an appreciated idea. Better would be prevention mechanisms. (Forbiddance)

## ***Requirements for Org Wallets***

**Session Convener:** Andre Kudra

**Session Notes Taker:** Andre Kudra

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

US:

Cross-border trade context

Wallet vs vaults

Certificates of origin, supply chain settings

Org-to-org transfers - org is issuer, holder, verifier at the same time

Org validation in public bidding scenarios

Quality, security, etc. certifications of orgs

Some individual has triggered the org action

Natural person acting on behalf of organization

The legal entity might not be acting on itself, always representative of org

Enterprise wallet always issuer, holder

Has to work across jurisdictions, multi-jurisdiction

E-receipt, proof of purchase, also recurring

Noone is involved (person), can be totally automated process

Automated process vs person invoked

Delegate authority to person from wallet

Somekind of interface required to org wallet for person/user to drive it

Can be integrated in an ERP system (or similar)

Persons are sometimes inclined to lying - truth is flexible

Analytics required to detect anomalies

System-to-system transaction

Entities behind it can be very diverse, from different industries

Trading documents in global trade are usually piles of pdfs handled over ODI

Every single hub in supply chain should be able to run their own stack

US Customs could have imposed their blockchain of choice

Layer of abstraction is VCs and standardized APIs  
Data model and APIs need to be agreed

Leveraging standardized data models, e.g. from GS1 and GLEIF  
Different representations of schemas are helpful  
No vLEI at US DHS but WebLEI  
Organizational identity  
It's better data but it cannot be considered absolute truth (factoring in residual uncertainty)

Org Wallet is much more than an SSL certificate  
Business trust on top of the level of security

Industries living of the inefficiencies of paper will not want a VC based world

Inclusion requirements may demand still physical (paper) credentials - this is also an opportunity

Financial industry: Lots of systems which required understanding who in fact did an action or transaction

Who's authoritative to what? Qualified issuers list in EU would not be available in the US  
How can that scale?

Strive to have also a flexible way without the trust list approach to facilitate more broad adoption, avoiding overhead, use trust lists / QEAA only when needed

Fix liability of the transaction

Differentiation between an enterprise wallet and employee wallet?

Looks like a portal infrastructure, it's implemented in the existing enterprise IT systems with existing mechanisms

Depends on the size of the systems - IAM systems within large organizations are usually very complex

Trust lists: Can be coming from the governance body but can also be self-managed lists of eligible actors

Country, enterprise, person, IoT device can be issuers

What's the org wallet?  
Enterprise standing behind certain attestations  
Enterprise assessing attestations from other organizations

One entity may not be accurate because a large corporate may have hundreds of legal entities somehow associated or (partly) owned

Depends on the business use case / process

One process may need consuming/issuing VCs, many others not

Existing, working, useful systems in enterprise orgs are hard to change - they want to protect their investments and are reluctant to change / replace them

Replacing physical stamps and paper with VCs

Basic layer of security: Strong authentication to internal systems with SSO and federation - not reinvent that

Managing relationships between organizations, e.g. Bosch manages a huge amount of suppliers, keeping masterdata up to date is a challenge, could be pushed to them by suppliers via an existing relationships

Most people in the room feel end user wallets are something substantially different than the organization wallet (system implementation) - by raise of hands

Org wallet might be just some portal or online (cloud) hosted service that multiple users can log in to

## ***How to kick off the E-ID-ecosystem?***

**Session Convener:** Vitus Ammann  
**Session Notes Taker:** Vitus Ammann

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

In order to gain fast and broad adoption the group came to the conclusion that there might be three routes to be followed with priority:

1. Credentials which are often/daily used by citizens such as credentials in the area of transport, tourism and payments.
2. Credentials used in high value processes where currently original documents and wet ink signatures are required (e.g. opening bank accounts or governmental confirmations).
3. Credentials used in cross-organizational B2B-processes such as employee-, educational-, health- or access-credentials.

It was suggested to get potential issuers of above mentioned credentials in the pre-launch-phase on board to either pilot potential use cases in advance of or have a set of interesting credentials ready for the launch of the E-ID.

Key to adoption will be the provisioning of issuing- and verifying services with no/low barriers to entry by private companies or the government. In case of the highly federated government structures in Switzerland the federal government should provide both cantons and municipalities with these services. It might even be a chance since smaller cantons and municipalities so far did not have the means to develop their own digital IAM-infrastructures.

## ***Sustainable business models without a dominant party. How does the marketplace look?***

**Session Convener:** Jan Vereecken  
**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**

## Notes Day 2 / Friday June 9 / Sessions 6 - 10

### SESSION #6

did:web 2.0?

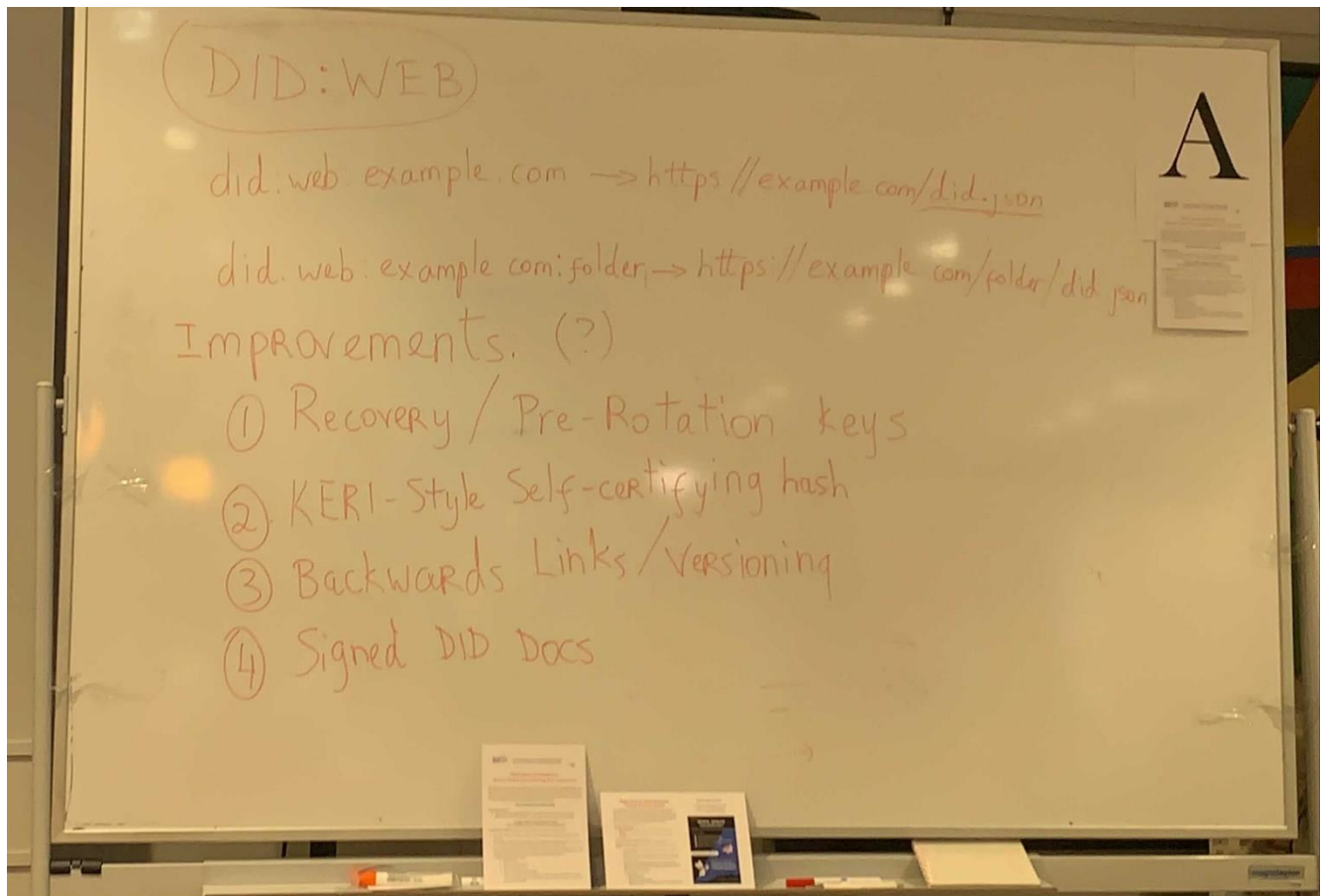
Session Convener: Dmitri Zagidulin

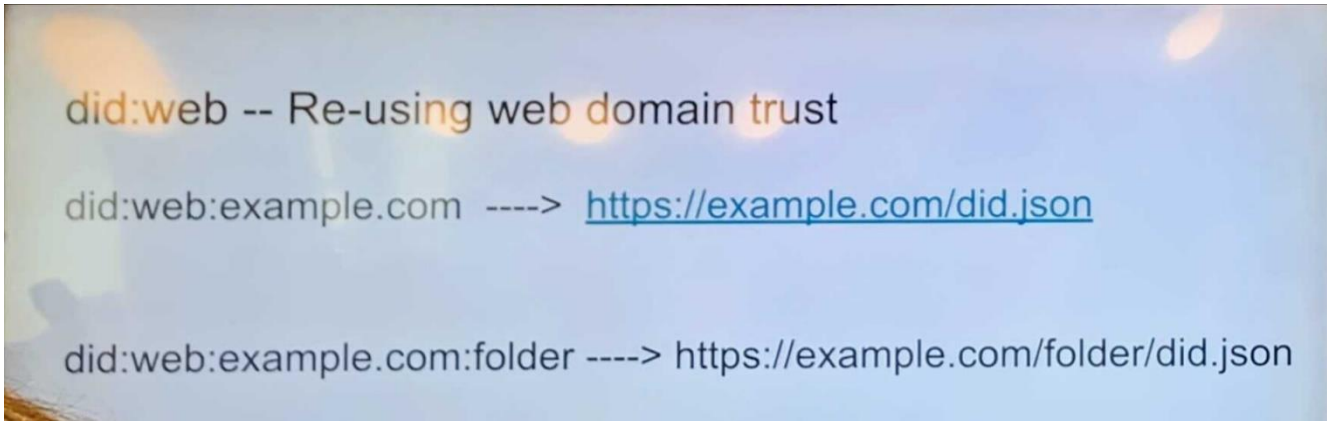
Session Notes Taker:

(optional) List of Session Attendees:

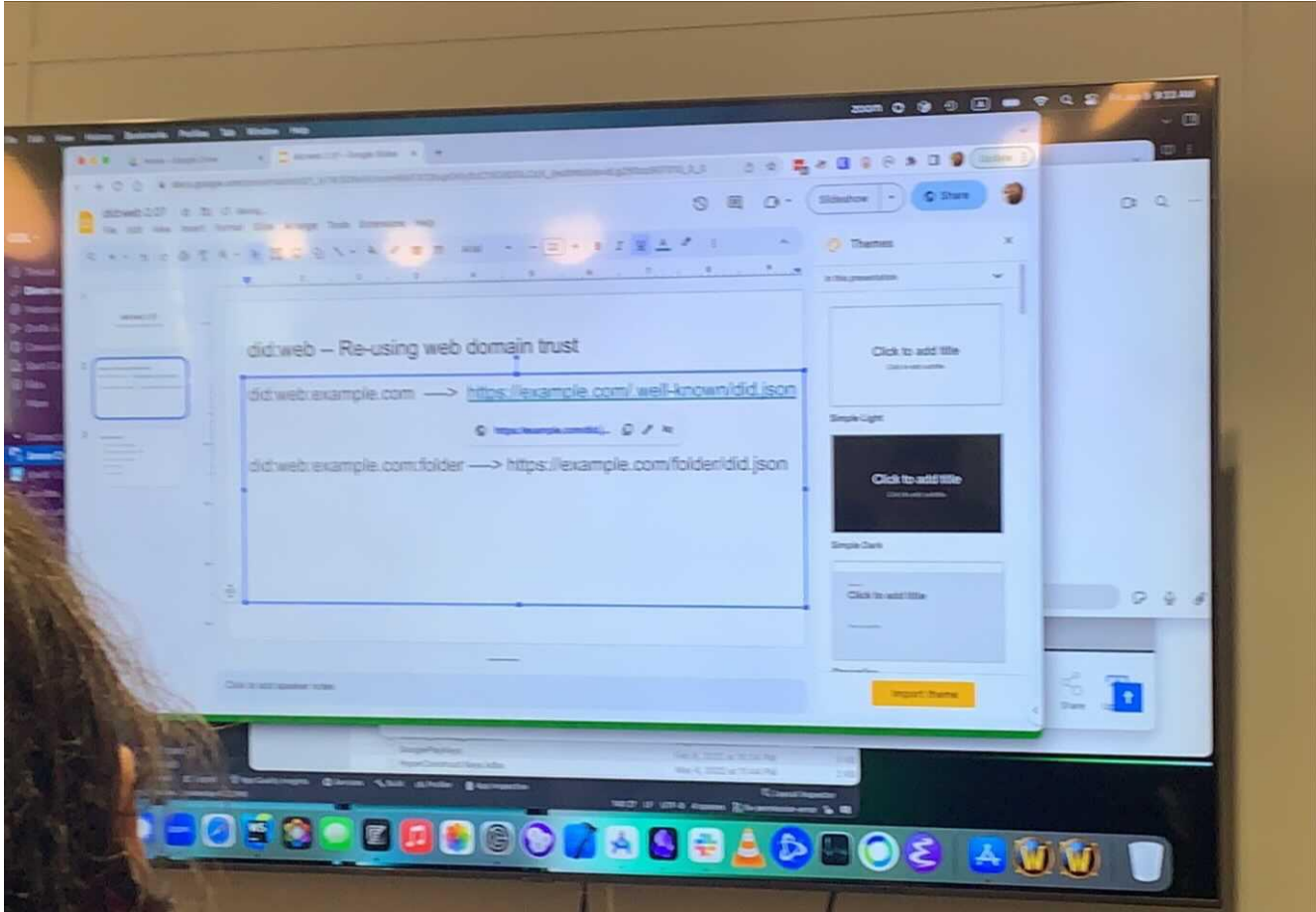
Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

Dmitri is a co-author of did:web standard

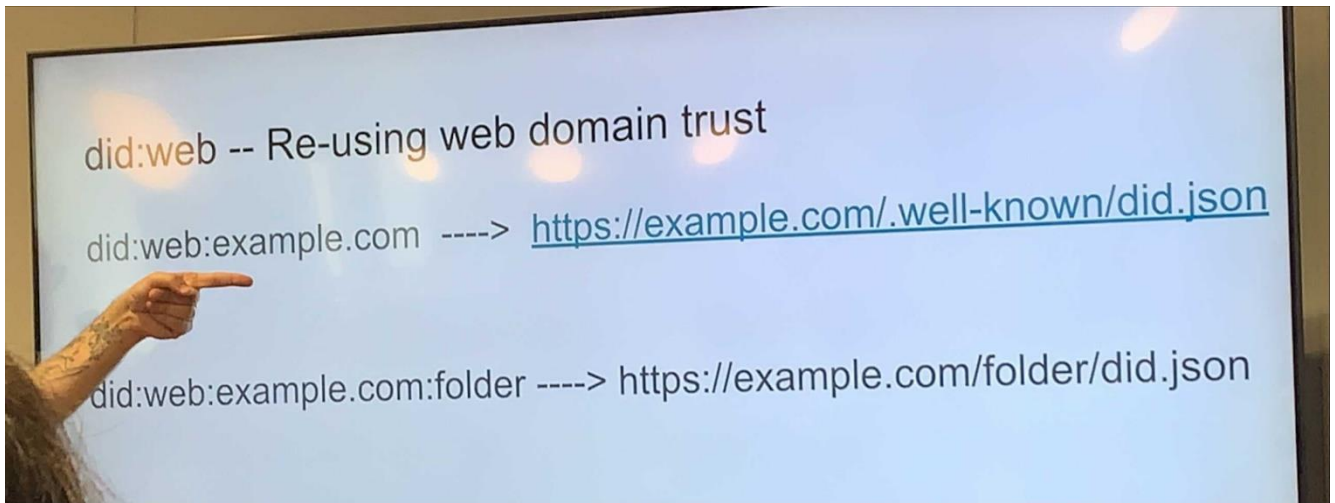




controversy re: “well-known”

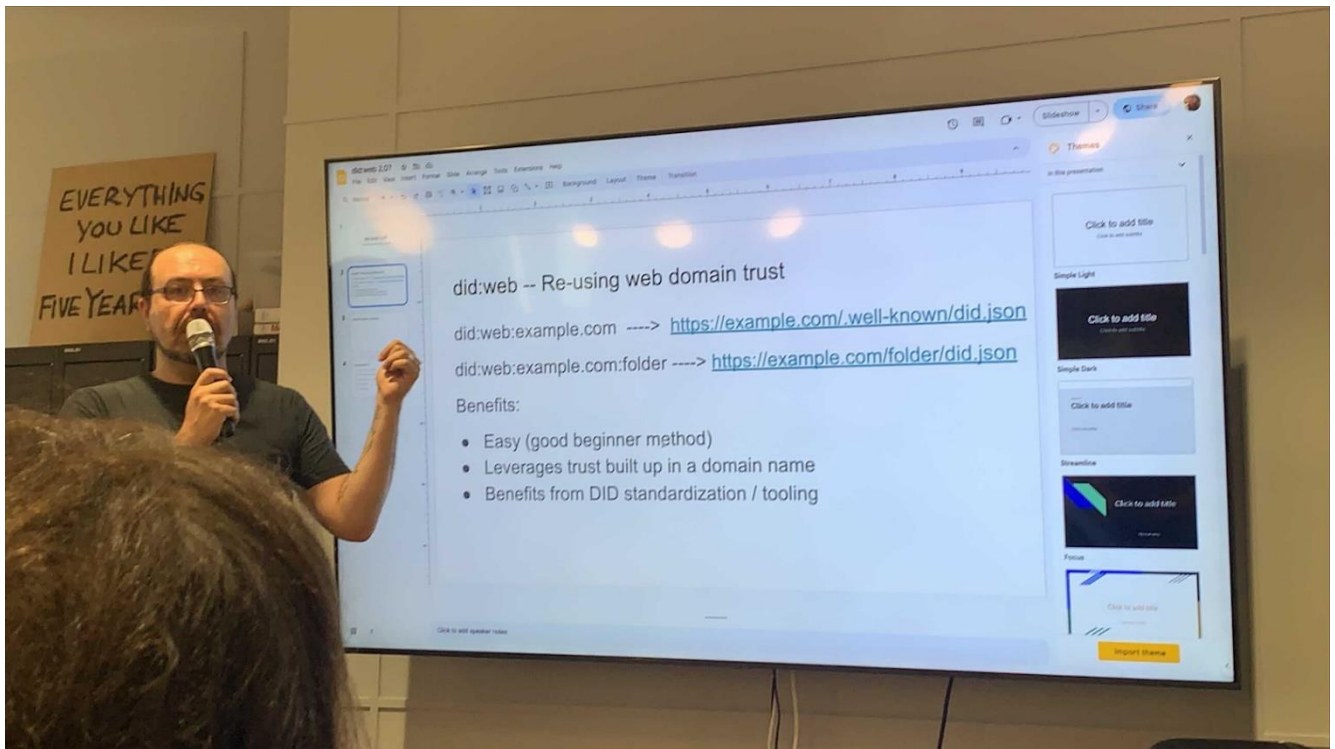






DID standard funded by Anil/SVIP w/ Manu Sporny et al

DNS security, verifying integrity of DID document, SSL turned on, various other considerations



offline methods bring risks, across all did methods, blockchain etc

caching takes care of offline use  
as long as caching and rotation policy is explicit...

did key cant be deleted = both benefit and downside

key rotation...

there are observers, within an ecosystem....

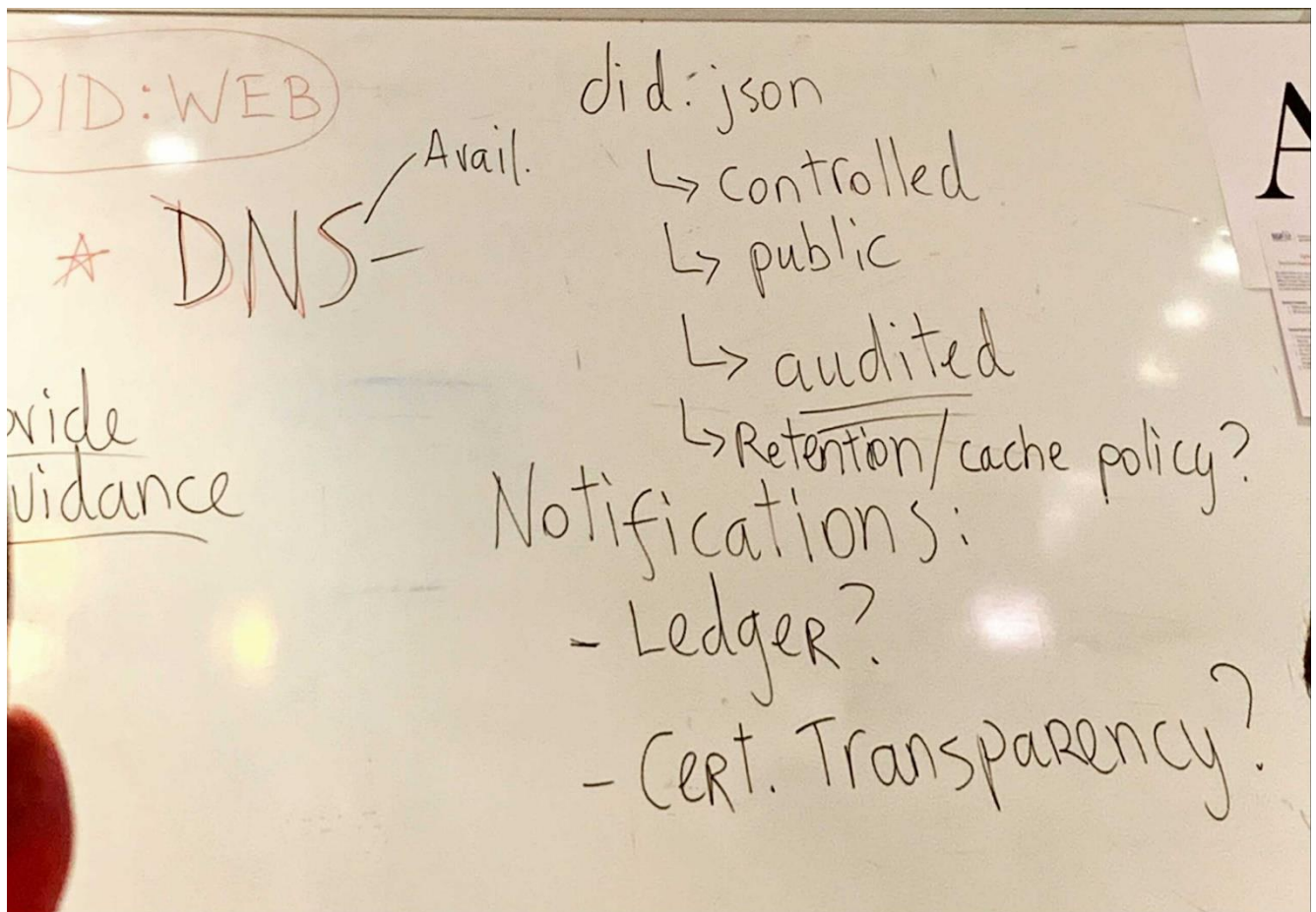
anil: did document is fundamental, needs to be controlled, significant governance, incl. auditing changes, eg 'bump in the night'...

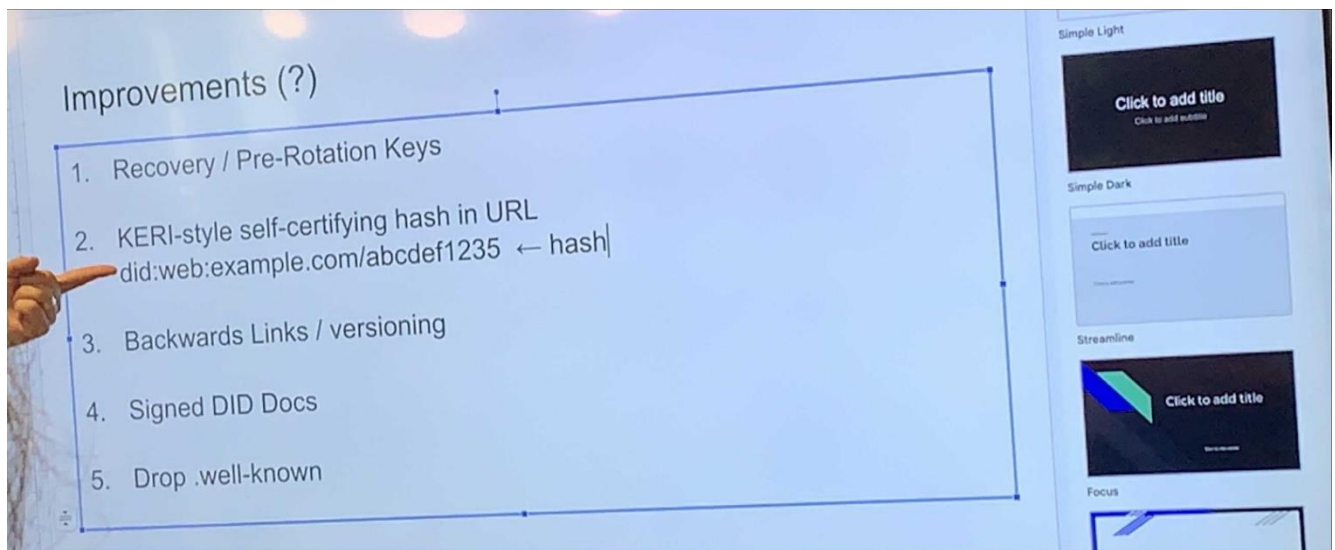
- not usu. a fan of "blockchain it" - but, here, distributed ledger could be useful, need a process in place to notify of changes in the did document, bake in ways to prevent people who manually update websites from stepping in and changing the did document - need to provide more guidance in the did doc itself
- need to start with control over did document

dmitri

DNS provides powerful tools for us

- use for carryover and availability





anil concerns

developer centric hash process

happy to provide a perspective on this

system gets broken when adding these types of complexities

depends on organizational mix, and process

would ask developer to provide ....

(exchange re: devs needed anyway; plus, can solve with the tooling...)

bluesky

trying to reinvent twitter using open protocol/ standards

quickly became one of the largest did providers

did:plc (did placeholder) - own did method created, in conversation with community

added backwards links field

allowing backwards links,,, makes it easier for verifiers, and makes did docs a little more resilient and long lived

specify keys, eg recovery...

additional signing provides more security

more eyes/ four eyes...

bc anyone can change the did document ....

anil re dot gov, "level of confidence"

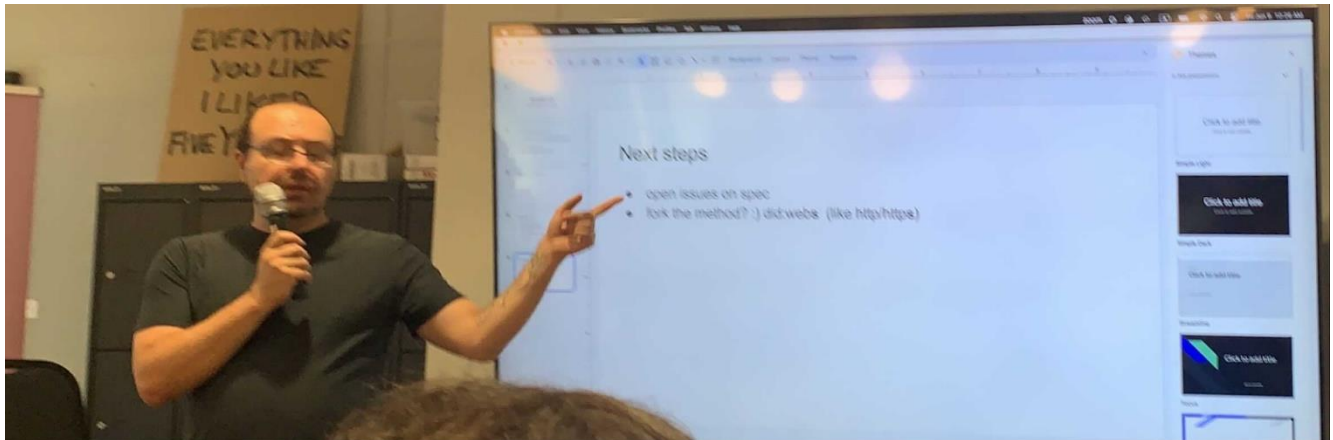
exchange w/ andreas re dont make addl signing mandatory

dot gov domain controllers are in a privileged position...

dmitri: ftp access + access to signing doc

anil-dmitri exchange re dropping well-known...

dmitri: out of practicality, some institutions literally cant upload



There was a discussion around the naming of the spec. The changes could be implemented to the a new version of the did:web specification. Another option would be for the did:web method and call the updated method something else.

It was pointed out that forking could be beneficial not only to “keep everyone happy” but to also keep a simple did:web method simple and allow more complex stuff (like versioning, signed did docs) using a different did method.

## *.ZKDID Decentralised DNS Web3 TLD protocol*

“A sybil resistant DAO and dedicated decentralised DNS identity protocol to work in harmony with Zero Knowledge DID credentials intended to empower humanity and improve democracy”

**Session Convener:** Toby Bolton (.ZKDID / Vibration Servers) id@zkdid.io

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

Introduction Toby:

The conversation was initiated by introducing the concept, which employs zero-knowledge identity along with a decentralised Domain Name System (dDNS) Top-Level Domain (TLD) .zkdid, aimed to serve as a dedicated DNS identity protocol and mark of trust. The proposal is to incorporate a dedicated TLD .zkdid into Iden3 PolygonID technology and construct a DAO (Decentralised Autonomous Organization) that is resistant to Sybil attacks through the use of ERC-721 token gating and the dDNS. The goal here is to empower the public by facilitating a fair, private and trustless decentralised governance system (DeSoc) that works in harmony with ZK DID technologies.

- **.zkdid™:** is a Web3 decentralised DNS Top Level Domain, it uses blockchain technology. It can be used for identity and resolve decentralised websites, send emails, provide access control, interoperate with other network resources, protect privacy, block unwanted content, improve online security and is blockchain agnostic.
- **.zkdid™:** The ".zkdid™" TLD is an acronym for Zero Knowledge Decentralised Identity and refers to the fact that the registry will complement the Iden3 zero knowledge identity toolset. It is essential that users can differentiate between other TLD's. ZK Proofs are a cryptographic technique that allows users to prove their ownership of a piece of data without revealing the data itself.
- **Decentralised DNS registry:** A decentralised DNS registry is a DNS registry on the blockchain that is not controlled by any single entity. This means that no one can censor or control the domain names that are registered on the registry.
- **DAO:** A DAO is a decentralised autonomous organisation. A DAO is a type of organisation that is run by code, rather than by people. This makes it possible to create an organisation that is transparent, accountable, and resistant to corruption.
- **DeSoc:** Decentralised Society (DeSoc) is an umbrella term for a new web3 ecosystem that aims to create a tamper-proof record of web3 users identity and social relations paving the way for a co-determined society with diverse ideals and fair governance.
- **Sybil resistance:** A system's ability to resist "Sybil attacks", where a single entity creates many identities (or nodes in a network) to gain disproportionate influence or manipulate the system.
- **Complement the Iden3 Zero Knowledge DID toolset:** The .zkdid™ registry can complement the Iden3 zero knowledge DID toolset. The Iden3 toolset allows users to create and

manage zero knowledge decentralised identities/wallets. The .zkdid™ registry can provide a way to interact with the Iden3 protocol using clearly readable domain names.

- **Blockchain name service (BNS):** A blockchain name service is a type of DNS that is based on a blockchain. BNS and dDNS are synonymous. A blockchain is a distributed database that is secure and tamper-proof. This makes it possible to create a BNS that is secure and reliable.
- **Intended as a global mark of trust:** The .zkdid™ registry is intended to be a global mark of trust. This means that company and user domain names registered on the registry will be seen as being trustworthy by businesses and individuals around the world. Intended to help encourage the adoption of Zero Knowledge decentralised Identity.
- **Dedicated DNS resolution protocol using the ERC-721 Ethereum smart contract standard:** The .zkdid™ protocol is based on the ERC-721 Ethereum smart contract standard. The ERC-721 standard is a standard for creating non-fungible tokens (NFTs). NFTs are unique tokens that cannot be replaced by another token. This makes them ideal for representing domain names and identity with powerful programmability.

Discussion:

The group consisted of varied backgrounds, from online payments, bank note inks and printing, security, blockchain, identity solutions, IT consultancy, security, government advisors, and science in stories.

Feedback was generally positive and inquisitive, the consensus was that systems that can improve governance are crucial to the future of society, especially with the advent of powerful identity technologies and Ai systems.

Taking a step back and looking ahead is essential, protecting our children and future generations. It is important to build solutions to mitigate mistakes that can be made during this technological shift into digital identity technologies.

The group agreed systems need to be built to empower the public, the presentation was focused on DeSoC using ZK tech and dDNS which can prevent abuse of identity systems, biometrics and personal data.

Most attendees were not familiar with many of the terms and technologies such as sybil resistance, dDNS, blockchain resolution patents, Iden3, W3DA, and much of what is ongoing in the web3 DNS space. The decentralised DNS space is in its infancy, though it looks to disrupt the traditional DNS space due to the enhanced functionality and smart contract capability.

Integrating a dedicated TLD into Zero Knowledge wallets could build trust and may speed up voluntary adoption of DID.

Zero Knowledge technology is cutting edge and abstract, it has the potential to become the DID standard in the near future due to its unique privacy and encryption methods.

The group agreed they would like to talk more. Gave important feedback on scaling, and discussed proving the concept worked in smaller settings, while increasing the size of the registrar over time. The best way forward was to demonstrate its efficiency in a small community first. The meeting was very inspiring and with luck may have sparked some future collaboration.

### ***Introducing the Use Case Canvas for VC use-cases***

**Session Convener:** Adrian Doerk

**Session Notes Taker:** Sebastian

**(optional) List of Session Attendees:** Frank, Allison, Laurent, Zoe, Carsten, Frederic, Andreas, Sebastian, Jan, Peter

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

Find the canvas here:

<https://app.mural.co/t/mainincubator8485/m/mainincubator8485/1686295084789/8f5032abe99dde16dafceb759bb63526f51206cd?sender=adriandoerk7527>

*The road to hell is paved with identity. Designing and building for humans.*

**Session Convener:** Bart Suiches and Andrew Slack

**Session Notes Taker:** Andrew Slack

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

Slides: [The road to hell is paved with identity](#)

We talk a lot about digital identity systems in terms of technology. That is a highly limiting view and we're on our way to building towards very bad outcomes, where every single thing needs to be verified. Do we want to live in such a zero-trust environment?

Trust is a confident relationship with the unknown. The tech around the SSI is mostly focusing on making the unknown known, not about increasing our confidence. We need to pay more attention to how our systems increase people's confidence with the unknown. This might require changing our perspective. It's not just the identity system you are building, it's also the system around it.

The problem with ANY identity system is typically not related to the tech it's using, but rather the inability to live our lives in freedom, to have agency, without an identity. Without an ability to be anonymous in your identity system, basically it reduces to a hierarchical registry.

How can we build better identity systems? It's not better technology, it's about developing from society centric and human centric principles.

Degrade gracefully - can we ensure that services are still available without identities?  
Resilience is an important attribute, as evidenced by COVID

We are not designing the system for the system to exist, it is to provide positive outcomes for people.

The better your infrastructure the harder the fall when it breaks.

There should be a downgrade path out of SSI systems

The problem of "over-identification" -  
with all technological progress there is a pressure to adopt and use.

Opt-out vectors can act as fallback vectors.



## *Sam Smith's tech-stack explained (KERI and other buzzwords)*

Session Convener: Michal Pietrus

Session Notes Taker: -

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

- Discuss the role of the basic components from the Sam Smith's tech-stack, including:
  - KERI
  - ACDC
  - TEL
  - CESR
  - SAID
  - OOBI

Technical specifications for the above: <https://github.com/weboftrust/keri>

- Clarify components applicability, how they are related to each other and how they are used in practice.
  - KERI (primary root of trust)
  - ACDC (data container for anything)
  - TEL (simple yet powerful revocation list)
  - CESR (how to combine data, i.e. an ACDC, with metadata, i.e., digital signatures in the most compact form)
  - SAID (content-addressable identifier that includes its type, a digital fingerprint)
  - OOBI (discoverability mechanism)
- Explain the basic building blocks of KERI, including Witnesses, Watchers, type of identifiers, KEL's, KERL's.

## *OID4VCI & SD-JWT deep dive*

**Session Convener:** Paul Bastian, Micha Kraus, Markus Kreusch

**Session Notes Taker:** Markus Kreusch

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

The session consisted of a presentation of an OID4VC issuer. The issuer was shown together with the Lissi wallet to issue an SD-JWT credential using the pre-authorized code flow. Details about the involved data and requests were discussed and questions clarified.

Several standards were explained:

- OpenID4VC High Assurance Interoperability Profile  
A profile choosing and demanding several features from the other specs to be implemented by issuers, wallets and verifiers to have a compatible basis to operate together. Using the high assurance profile leads to more secure choices concerning the options from the other standards.
- OpenID for Verifiable Credential Issuance  
The issuance protocol that transfers credentials from the issuer to the wallet. For issuance two basic flows are defined, the standard oauth authorization code flow and the pre authorized code flow. The main difference is, that for the authorization code flow, user interaction with the issuer happens after the wallet first contacted the issuer. For the pre authorization code flow user interaction with the issuer happens upfront.
- SD-JWT VC Specification  
Defines a VC format based on SD-JWTs. The main thing in this spec is the definition of some custom claims that can or need to be in a VC SD-JWT.
- SD-JWT Specification  
Defines the SD-JWT format, a JWT with the feature of selective disclosure. This is independent of VCs. SD-JWTs do not support non correlation.

Learnings from our implementation:

- The whole protocol stack was known to a team of 3 people who then implemented an issuer prototype including UI from scratch in two days.
- Implementing a the pre authorized code flow is easy and should be possible by a single person without any upfront knowledge besides good HTTP and programming skills in two weeks.
- The overall complexity of the protocols is much lower than the Aries stack.
- Implementing the full high assurance interop profile in an issuer requires more work because more requirements exist.

Relevant links

- OpenID4VC High Assurance Interoperability Profile  
<https://vcstuff.github.io/oid4vc-haip-sd-jwt-vc/draft-oid4vc-haip-sd-jwt-vc.html>
- OpenID for Verifiable Credential Issuance Spec  
[https://openid.net/specs/openid-4-verifiable-credential-issuance-1\\_0.html](https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html)

- SD-JWT VC Specification  
<https://datatracker.ietf.org/doc/html/draft-terbu-sd-jwt-vc-02>
- SD-JWT Specification  
<https://datatracker.ietf.org/doc/html/draft-ietf-oauth-selective-disclosure-jwt-04>
- SD-JWT overview  
[https://self-issued.info/presentations/EIC\\_2023\\_Selective\\_Disclosure.pdf](https://self-issued.info/presentations/EIC_2023_Selective_Disclosure.pdf) (presentation starts with SD-JWTs but contains other formats as well)
- SD-JWT libraries  
Kotlin library  
<https://github.com/openwallet-foundation-labs/SD-JWT-Kotlin>  
Reference implementation (not intended for production use)  
<https://github.com/christianpaquin/sd-jwt>

## AMA about the Polygon ID Solution

Session Convener: [Silvia Aran](#)

Session Notes Taker: Silvia Aran

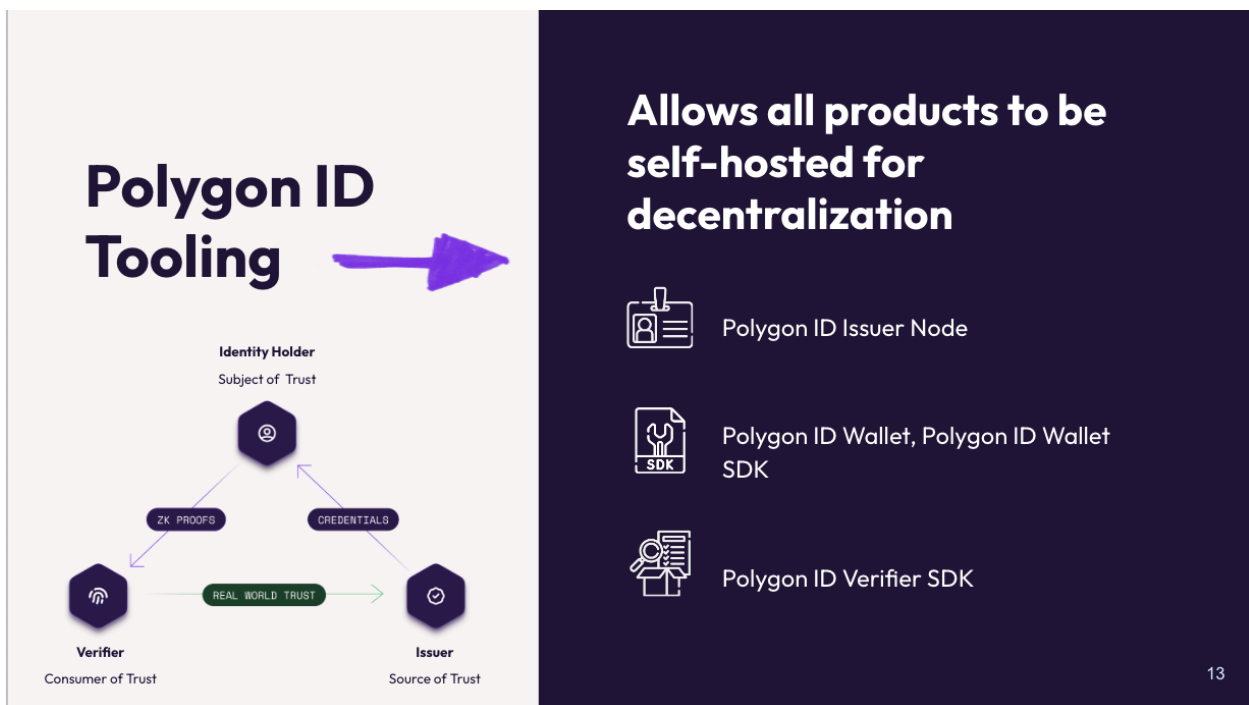
Please list the key points of your conversation, what you would like to share with your colleagues and/or next steps.

The session covered the following topics

### High Level Overview of the Polygon ID product stack

PolygonID provides identity infrastructure that enables secure and trusted relationships between users and apps based on the principles of self-sovereign identity. It allows individuals to securely interact with off-chain applications and smart contracts without revealing personal information, utilizing verifiable credentials and zero-knowledge proofs.

[Polygon ID verifiable credentials are issued according to the W3C standards](#) and signed cryptographically to guarantee they are tamper-proof.



**For the Issuers**, Polygon ID includes [the Issuer Node](#), a self hosted API capable of creating these credentials.

**For the identity holders** Polygon ID has developed a reference Wallet application. Polygon ID makes available a [Wallet SDK](#) in Flutter and Kotlin (now working on wrappers for React Native) that can be used by wallet providers to develop mobile wallets that request, store and present credentials or proof of credentials (using zero-knowledge proofs). Polygon ID also includes a JavaScript SDK for developing web-based wallets, browser extensions and dApps.

And last but not least, these credentials are meant to give the identity holder the possibility to prove something about him/herself to an App, or a dApp -or SmartContract- (the Verifier of the credential); or to selectively disclose some information contained in the credentials to the App or dApp.

The process is like a “question-answer” dialog. The App / dApp needs to verify that I’m older than 18 to give me access to some content, or a SmartContract needs to verify that I’m human and unique before giving me an airdrop. These Verifiers can “ask” my wallet these questions and my wallet will generate a valid answer using my credentials.

The entire process is highly resistant to tampering - thanks to the use of PKI (public key infrastructure) and blockchain, is also privacy preserving - thanks to the use of zero knowledge proofs.

**For the verifiers**, Polygon ID includes the [Verifier SDK](#) and smart contracts for off-chain and on-chain verification. These libraries allow the Verifier to compose different queries (questions) using the zkQuery language without having to deal with the complexity of reconfiguring the underlying cryptography.

### **Introducing the polygonid:did method**

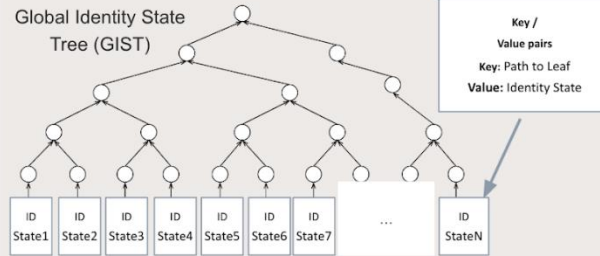
Polygon ID is an identity protocol which aims to maximize the privacy of the identity holder by leveraging Zero Knowledge Proofs (ZKP) technology. The protocol enables users to generate ZK proof responses on Verifier requests using the [ZK query language](#). [did:PolygonID](#) - is an implementation of the [iden3 protocol](#). Some of the key features are the following:

- Key rotation, private revocation with YK
- DID profiles
- zkQuery language to create verification criteria for Apps and dApps
- Multiple credential issuance methods: SIG method (does not require the use of a blockchain) and MTP method (enables on-chain use cases and revocation)
- Leverage Babz Jub Jub (BJJ) keys for optimized generation of zkProofs in mobile devices
- Compatible with any Ethereum Virtual Machine (EVM) blockchain
- Fully Open Source with MIT / Apache license

# did:PolygonID - Identity State

## Identity State Contract:

- Initially identities are in genesis state, where their state can be proven directly with the identifier.
- The identity states are all published in a "global identity state tree" (sparse merkle tree) on chain. Proofs can be provided to demonstrate that one of the identities is being used without revealing which one.
- A smart contract is kept up to date with the information of the identity state (more on this later). The smart contract also has check of state transition function, needed to update the identity state and verify correctness of the transition.



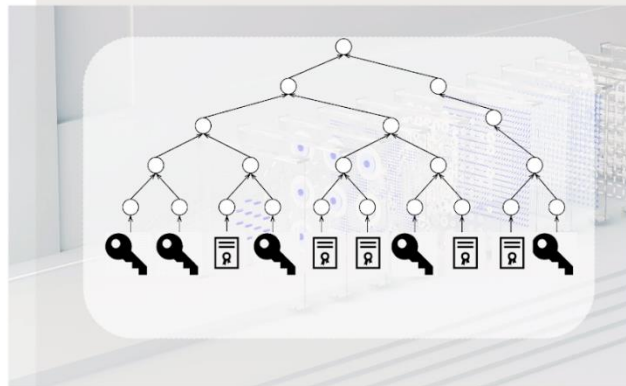
# did:PolygonID - Claims tree

## Claims Tree:

- Claims can be issued by the identity holder (and added to the claims tree when issued using the MTP method, more on this later)
- Each claim has a unique "revocation nonce" which can be used to revoke the claim (more on revocation later).

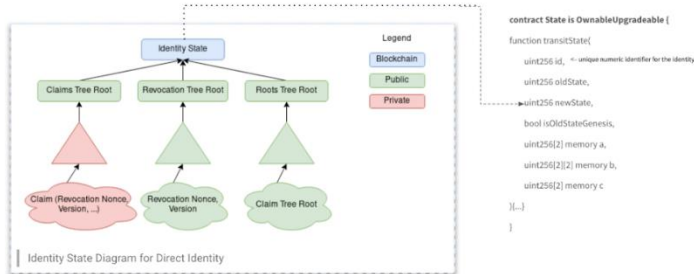
## Claims Tree may hold:

- Keys
- Credentials issued



# The Identity State

Polygon ID Identity State stored on-chain

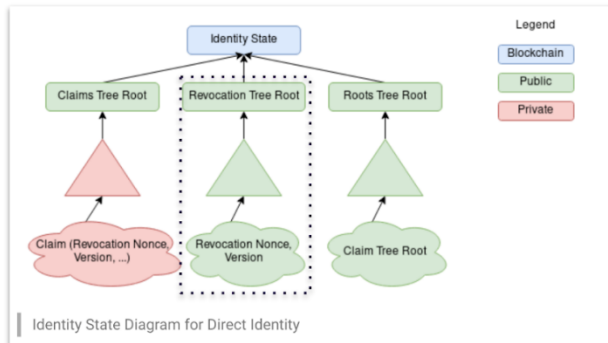


The identity state is a hash of the three merkle trees, which themselves are a hash of:

- 1 the claim tree
- 2 the revocation tree
- 3 the roots tree

# Revocation

Revocation data stored publicly



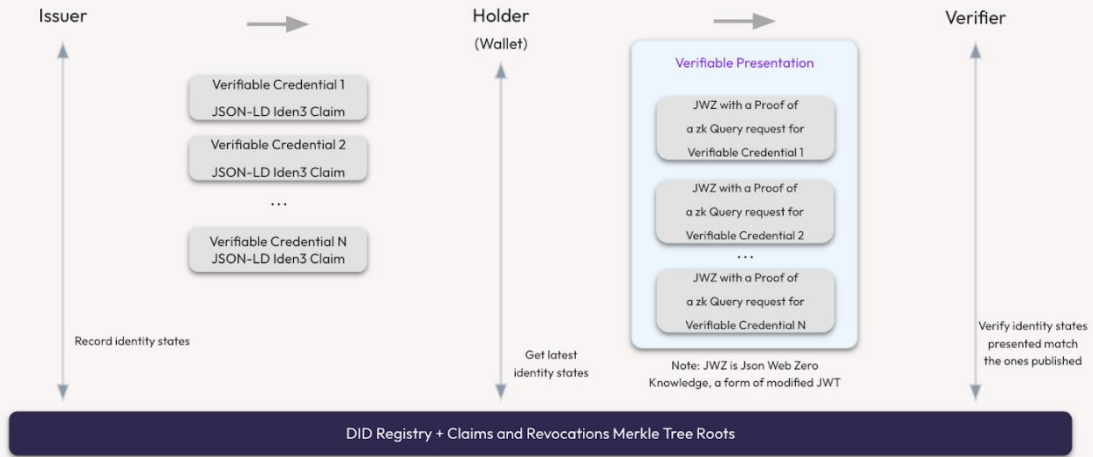
The revocation tree specifies which claims have been revoked

The information revealed is only the unique identifier of which claims have been revoked.

The revocation tree is composed of the revocation nonces (unique revocation numeric identifier for the claims) and is stored in a public file storage such as Amazon S3, IPFS, Filecoin or similar).

## Support for Verifiable Credentials

did:polygonid - Privacy preserving verifiable credentials method, *selective and private disclosure* of specific data attributes without revealing the user's main identifier.



30

**Are Polygon ID ZK proofs stored on-chain?**

**No!**



**Can polygon ID ZK proofs be verified on-chain?**

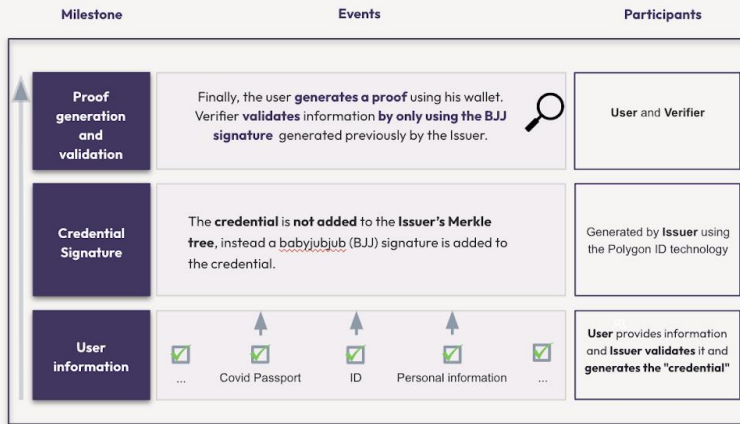
**Yes!**



29



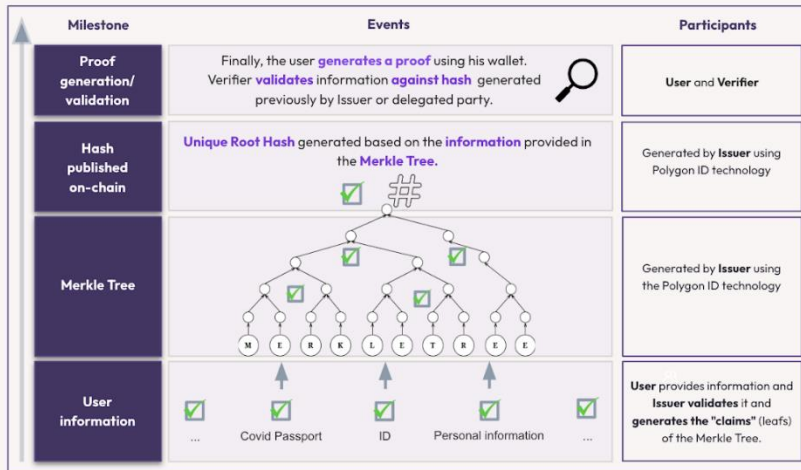
# “SIG Method”: Issuance of Credentials with Baby JubJub (BJJ) Key Signatures



The **credential** is not added to the Issuer's Merkle tree, instead a baby jub jub (BJJ) signature is used which is then verified upon presentation.

After the initial issuer state has been published on-chain; it is free to issue claims off-chain (similar to did:ethr).

# “MTP Method”: Issuance of Credentials with Claims Merkle Tree (Merkle Tree Proof)



The validation of the proof is done against the state published on-chain. No personal information is stored on-chain.

A key difference with this method is that the identity state has to be published on-chain (the hash of the merkle trees), since the Identity State Transition function has to be executed.

Another important difference is that through this method smart contracts can issue credentials.

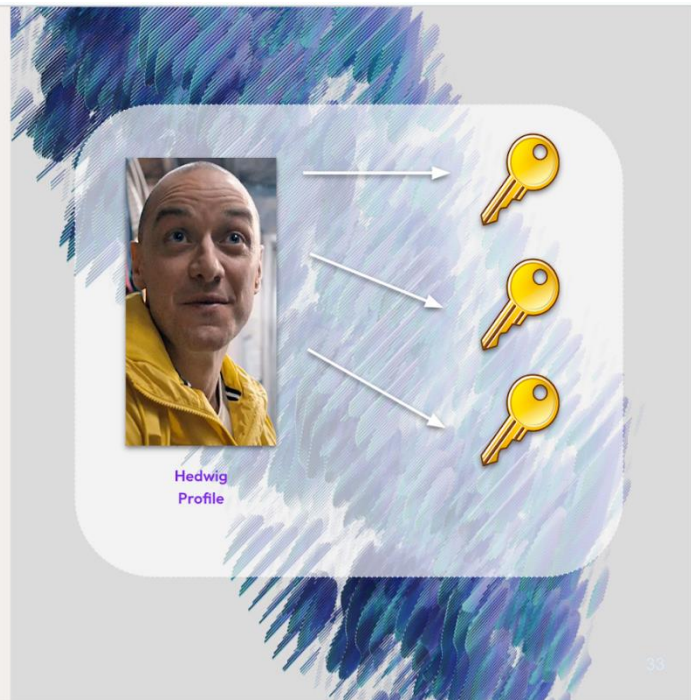
## Additional Features

### Splitting keys from identities

Identities can prove that control multiple keys, which allows

- Having as many identifiers (dids) as they like

↔ Key rotation ↔



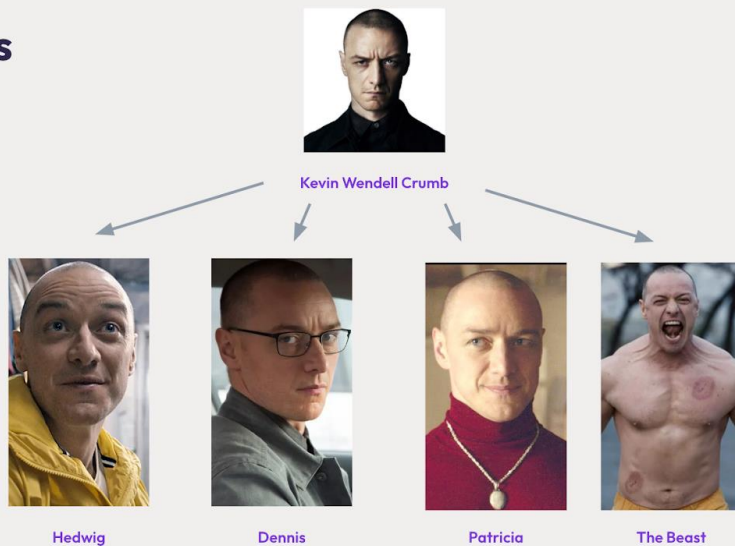
33

## Additional Features

### Profiling

Since users can have as many identifiers (or dids) as they like

- Default behavior: anonymous random identifier generated for each interaction
- User can decide to select a permanent identifier for interactions with a verifier
- Identity Profiles allow users to hide their Genesis Identifier during interactions. Instead, users will be identified by their Identity Profile.



34

## SESSION #7

### Revocation

Session Convener: Andreas

Session Notes Taker: Andreas, Samuel

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

Link to the presentation:

[https://docs.google.com/presentation/d/1zHtuwU8AE0zajnAlMv9kTpJfOqk3q76w/edit?usp=drive\\_link&oid=113403237479658121506&rtpof=true&sd=true](https://docs.google.com/presentation/d/1zHtuwU8AE0zajnAlMv9kTpJfOqk3q76w/edit?usp=drive_link&oid=113403237479658121506&rtpof=true&sd=true)

- Draft Paper  
<https://eprint.iacr.org/2022/1658.pdf>
- zKP JSON-LD BBS playground  
<https://github.com/zkp-ld/zkp-ld-playground>  
<https://playground.zkp-ld.org/>

At the end of the session, [Samuel](#) argued that holder is not a part of the revocation check step in the verification process. After the holder presents their verifiable credential to the verifier, the holder has no way of knowing whether the verifier checks the revocation status. There is no action performed by the holder (after presenting their credential), no functionality needed in the holder wallet, no holder wallet APIs queried, etc. in the revocation check process. Thus, on the [slide 6 in the presentation](#), the contents of all cells in the  $H_c$  column of the  $Verif.$  table should be  $n$  instead of  $y$ . (Perhaps  $y$  for rows Credential update and LVVC, if user can present an updated verifiable credential after a revoked credential is rejected by the verifier.)

In the sense of privacy, this is not a big difference, since revocation status is often performed right after the holder presents the verifiable credential to the verifier, and the holder is aware that the verifier *may* conduct some kind of revocation status check. In the sense of protocol implementation, the fact that the holder wallet has no role in the revocation status check phase, may be of importance.

## ***Role of Government to build up an eID-encryption and within an established Trust Framework***

**Session Convener:** Jan Rehder

**Session Notes Taker:** Jan Rehder

**(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.**

- First of all we shared experience and practises from different countries eg.
  - Germany: not clear strategy, constantly role changing > facilitating the development of an eID ecosystem; technical development of wallets or infrastructure; policy development
  - UK: rule setting (regulation and framework), Data providing, facilitating and bringing together different sectors
  
- Inputs for obligations of the government
  - to ensure interoperability internationally
  - promote for inclusion, ensure equality in using eID
  - to encourage private sector to join
  - educating citizens > in the sense of SSI > to give citizens the ability to cope with this control of data

## ***USEFUL Interactions with trusted relationships DIDcom***

**Session Convener:** Sebastian Bickerle / Adrian Doerk

**Session Notes Taker:** Adrian Doerk

**(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.**

### **Relationships > credentials**

Can enable (group) chatting via DIDcomm

We think digital identity is about much more than verifiable credentials - we need trusted relationships.

The trust over IP foundation defines trust tasks - which can also be payment or consent topics

**Demonstration of the lissi wallet** with focus on the relationship part  
requesting credentials as a pull from the organisation  
providing context as an organisation is important e.g. privacy policy or where a issued credential can be used  
we need to enable people to do automated consent management

**Demo by 2060:**

Messaging chat based on DIDcomm protocols Basic message, action menu, present-proof  
organisations use the wallet to build the trusted relationship (e.g. customer authentication) and then use the Chatbot to offer individual service with offers etc.

**Using the Wallet chat:**

Trust in the organisation is the first and important step.

When providing my information to the organisation - who they are giving it to and what do they do with it?

Be transparent: Is it a human or an automated LLM I'm interacting with?

swiss bank would not like to use it - because they want to have everything under their control, best in presence not via email - Rather for B2B cases

For government stakeholders to adopt such a technology it will probably take some time

non-repudiation: Protection against an individual who falsely denies having performed a certain action

**Technical issues for mass adoption:**

we would need to agree on a a common protocol,

What infrastructure requirements do we have? What central components would we need (e.g. for group chat)?

scope of the trust spanning protocol at ToIP.

**Dreams:**

Subscribe to some maillinglist

Be able to use my own client for different workflows and protocols

## ***Where does PRIVACY end and SECURITY begin...or... Where does SECURITY end and PRIVACY begin?***

**Session Convener:** Adam Eunson & Keran Kocher

**Session Notes Taker:** Adam Eunson & Keran Kocher

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

The session was an open discussion on where does privacy begin and security end?

Adam presented a few initial thoughts on privacy and security in the world of Self-Sovereign Identity, asking the questions:

- Are our focuses on privacy in the wrong place?
- Where does the balance between privacy and security begin and end?

An example was presented in regard to the focus on tracing DIDs (Decentralised Identifiers) to profile individuals by their digital interactions. If a DID is exposed, then an individual can be traced throughout their digital interactions, which invades the privacy of the individual.

On the other hand, device fingerprints already do this, and are not applicable to the same guidelines and restrictions as is being put on PII and pseudonymous data within the GDPR and eIDAS frameworks. So, having a DID exposed, or not, is irrelevant, if the device can still be tracked.

These precautions are in place to manage fraudulent activity. So when we look at the security and privacy balance, we have to look explicitly at the use case, and the exposure of the data, or pseudonymous data, that is exposed.

A “Nature Communications” Paper was highlighted:

**Estimating the success of re-identifications in incomplete datasets using generative models (2019)**

*Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye*

<https://www.nature.com/articles/s41467-019-10933-3>

This paper outlines the ability through simple generative models, to extract an identity from an individual from a limited set of pseudonymous data. The question was then put forward - should our focus on privacy in the SSI space should go beyond the standards we are working with, and also take into account the surrounding digital infrastructure, and the tracking of devices and the privacy guidelines presented for these within the GDPR?

**Keran followed the introduction by discussing the work and research he is carrying out during his Masters study on the balance between privacy and security in SSI.**

*\*Keran to add notes here\**

The discussion then opened up and it was quickly evident that there are a lot of differing views on privacy and security in the context of SSI.

## **One key takeaway was that both privacy and security are entirely relative to the individual use case that the technology serves.**

In the context of basic use cases, where SSO may be the only purpose, then security aspects of user identity are a low barrier, requiring little data exposure. Whereas, in the context of cross border identification, or government identity, security levels need to be a lot stricter and the privacy of the individual a lot lower, as data sharing is a necessity in these SSI encounters.

This presented a further question:

### **Who is responsible for privacy?**

For interoperability and standardised systems, privacy considerations need to be implemented at the standards, framework, and protocol levels. Without guidelines on interoperable standards such as SD-JWTs, ZKPs, etc. baked into the frameworks and standards we are building with, we are not putting privacy first. To adhere to GDPR and provide selective disclosure or zero knowledge proofs, for them to be interoperable across ecosystems like the EU, these need to be built into policy such as the eIDAS framework, to ensure a foundational level of interoperability and not a misinterpretation that could be detrimental to the interoperability of the ecosystem as different service providers build different interpretations of the solutions.

One of the major points noted throughout the discussion, from a security perspective, was the concerns about security levels of exposure of user data. In every use case, the security aspects of required user verification, through data exposure, boiled down to one thing. Fraud or the falsification and misuse of data.

Every time data exposure was required it was due to the necessity of preventing fraud. This level of exposure, as previously mentioned, was determined by the security levels of the use case, and it was evident that in every case, the user had to choose to expose sufficient data to receive a service or engage in an activity, such as buying alcohol, crossing a border, opening a bank account.

One question that arose here was how do we go about ensuring that users aren't forced to expose more data than necessary to achieve an interaction?

This presented numerous perspectives, from the legal perspective, it is down to jurisdictions and member states to monitor and provide guidance on the levels of data required for certain interactions and enforce this. Also, in many cases, businesses who are required to retain user data, by law, are required to retain this for periods of time, from 30 days, to 10 years.

The problem we have with the current direction of SSI, is that the exposure of data is an easier thing to achieve, a simple one click, and if requested by what may appear to be a legitimate entity, how are we to prevent this data being further abused or used for monetary gain, without our permission?

### **The two main discussion points here were:**

- User education, ensuring users are aware of what, when, and who they are sharing data with, as well as educating service providers surrounding how much data they actually require and the implications of over exposing their users' data.
- Law enforcement in the digital space, an aspect out of most peoples control, but more of an area we can put forward discussion to ensure states and governments are putting a focus on tech privacy.

### **A few other notes that resounded throughout the discussion where:**

- There are serious privacy concerns in regard to the traceability of individuals in SSI ecosystems.
- We must focus on privacy preservation by design, from standards and policies, right through to apps.
- There is an ever growing need for the user to have full control over data.

Having a legal expert in the discussion presented some great insights into the legal implications of the privacy and security aspects discussed in the session.

Some key notes were:

- Separating the legal and ethical from the technical is a very complex process.
- Jurisdiction plays a huge role in defining technical implementation and interoperability.
- It's also important to understand that different use cases fall under different legislation.

One important factor that was presented was that Technology moves fast, law moves slow. Our progress on the technology front is moving a lot faster than the law can, and this can present considerations when implementing the latest technology. Moving too fast may produce a technology that is outside of the law, or falls short of future legislation, policies, and frameworks. WHICH is why it is important to keep the discussion at the top of the list for framework level guidelines and standards for selective disclosure and zero knowledge.

### **Summary**

If interoperability and consistency in deployment is to be achieved, standards and guidelines need to be implemented at a framework level, that reflect current privacy laws, and that support multiple privacy and security scenarios.

The technical features and standards then need to be implemented at a protocol and method level, to ensure all protocols are adherent to legislation. As technology developers and providers, privacy features should be implemented by design.

Developers can then build using these open standards and frameworks with a focus on privacy by design. Providing the highest levels of privacy such as zkp and sd-jwt and giving control of the data exposure to the identity holder. Whilst also allowing for verifiers to adopt varying degrees of security through verification of user data, dependent upon the use case.



## SESSION #8

### *Using Humor & Visual Communication to Gain TRUST 101 / Chance*

Session Convener: Chance  
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.

**No Notes Submitted**

### *Beyond Use Cases: Communicating guiding visions for Digital Government*

Session Convener: R.X. Schwartz  
Session Notes Taker: R.X. Schwartz

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

Sheet 1 (Background and ideas)  
A sheet describing some overarching visions for digital government

#### "Gov CX"/Life Events

- A life event is identified and the service is designed around it
- Examples: Baby is born/Immigrates for work/heart transplant

#### Co-production

Citizens involved with digital government

- Co-initiation/co-commissioning

- “Processes where citizens collaborate with public employees to identify social problems and needs, and set the agenda for developing an innovative solution” (Sorensen and Torfing, 2018)
- Co-design
  - Citizen-involved design processes for testing and improvement purposes (user consultations, journey mapping, public forums, ethnography)
- Co-implementation and co-management
  - “Third-sector organizations produce services in collaboration with the state” (e.g. open-source collaboration) (Brandsen & Honingh, 2016; Brandsen & Pestoff, 2006)
- Co-delivery
  - Citizens are responsible for delivering the service (volunteerism, peer training, etc.)
- Co-assessment
  - Monitoring and evaluating public services is a collaboration between state and lay actors

Quotes and framework sourced from Mergel 2020.

### 2+20 Project

- For each government process:
  - Less than 2 weeks of passive waiting (time spent waiting for the output)
  - Less than 20 minutes of active waiting (time spent in line, filling out the form, or getting to the office)
  - 95th percentiles (note: may not be interpretable)
  - The output of the process must be useful in the real world (e.g. not just a form you bring to another govt. office)
- Discussion:
  - Q: Does the “20 minutes” start at the door of the government office? A: If so, then this vision may not be comprehensive enough, because if the government offices are not close to the citizens or if there are few government offices then it will be very difficult for citizens to complete the process even when the vision is followed. For this reason “20 minutes” must start at the moment of the desire to complete the interaction, although it can include 20 minutes starting from certain points in the citizen’s daily life path and doesn’t have to be measured from the citizen’s home
  - Q: Is 20 minutes too long of a delay for the 95th percentile? A: Perhaps it is too long for some processes that are digital, routine, and need to be completed at home in digital format (such as paying a bill)
  - Q: Should KPIs be used as messaging for the public, or instead should KPIs be used internally, and general communications should be used as messaging for the public (e.g. “services will be faster”)? A: Perhaps it is necessary to develop a specific sense of possibility and expectation among the public, which would then need to be measured against specific metrics.

Sheet 2 (Brainstorming activity with sticky notes)

We brainstormed and grouped successful visions for digital government, particularly making reference to projects that have been communicated well to citizens

Digital government communication/visions

Honesty congruence transparency

Manage expectations

Set expectations for failure

Even some statistics sharing with citizens is good

Really bad failures are dealt with promptly

And incorporated into future reforms

Decentralized cryptographic proof sharing

H <-----> V (water tube metaphor)

2-level communication strategy for tech projects: simple + deep dive

Missing rainfall %

Internal to government cost-saving project justification

Once-only principle

Experimentation "safe to fail"

Experiment has good measurements

Communicating possibility of failure

"One stop shop"

## Building Blocks, Abstraction Layers & Multistack environments - *discussing long-term perspectives & how to survive multi-year ecosystems in an volatile tech environment*

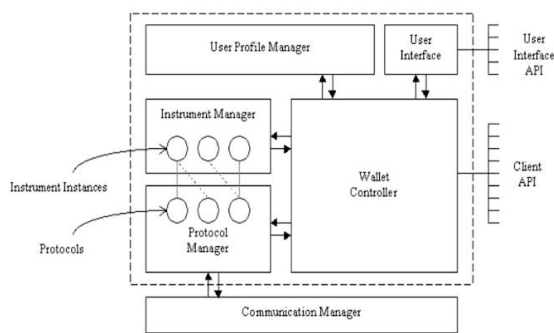
**Session Convener:** Carsten Plum with Andi Frey Sang, Jonas Niestroj, Raphael Guye & Stephan Halbritter

**Session Notes Taker:** Carsten Plum

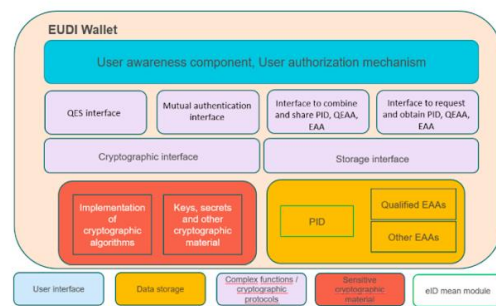
**(optional) List of Session Attendees:** quite a lot 😊

We started with a short pitch on the “problem context”, which is how to build software in an environment which is “technically volatile”. From a computer science perspective this means building modules, Building Blocks and abstraction layers – the approach not being new in computer science:

### 🇨🇭 ...not new in Computer Science :-)



→ a 22-year-old model from Stanford for digital Wallets  
<http://diqlib.stanford.edu:8091/~testbed/doc2/DigitalWallets/index.html/>



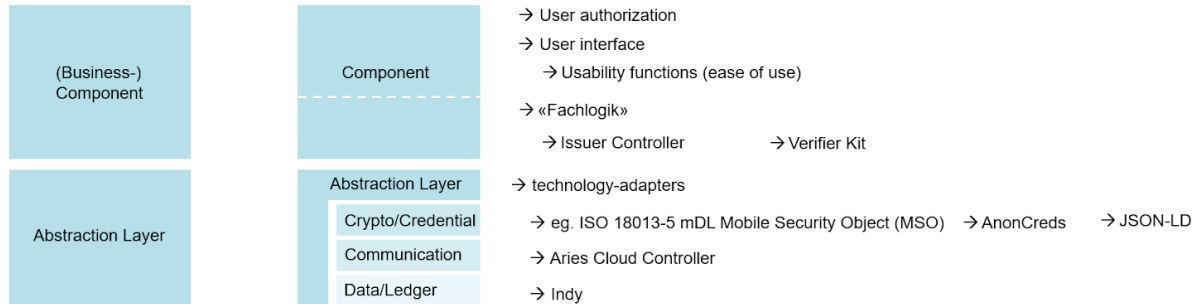
→ EU digital identity architecture and reference framework

We then looked at a general approach:



## ...how we could start...

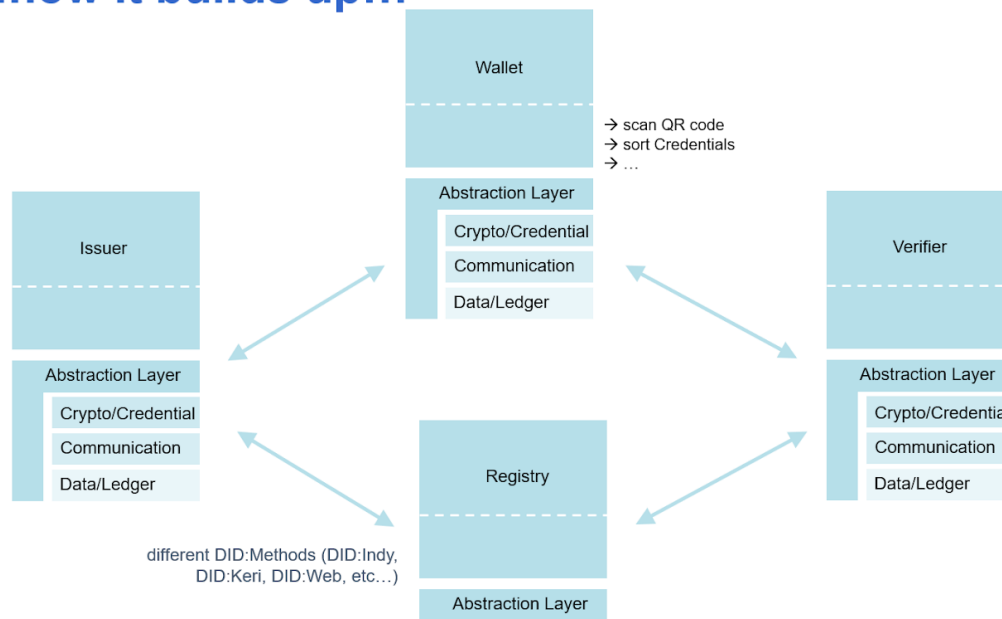
start evaluating and thinking in reusable components or multistack environments, which reduces sunk costs



And then adopted this on the trust diamond:

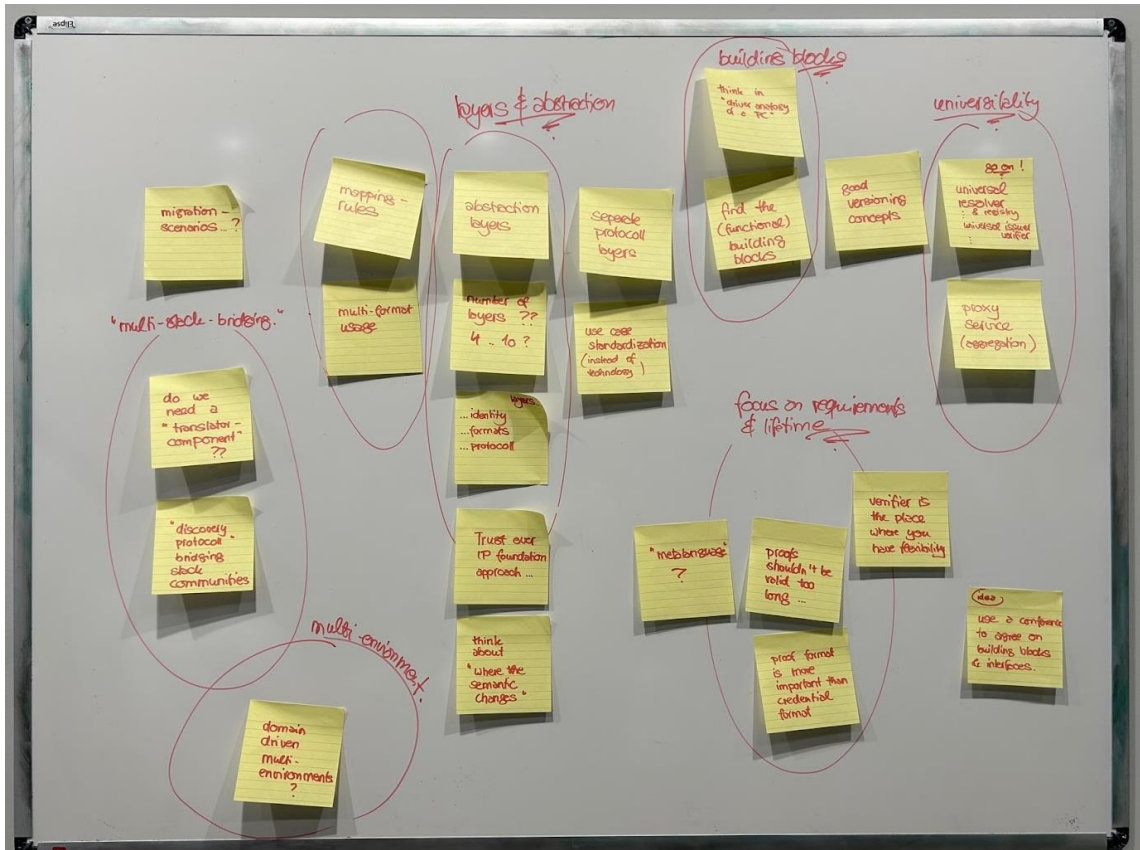


## ...how it builds up...



We also posed the question: Does a multistack environment also mean supporting multiple roots of trust or are there practical approaches where a root of trust starts to support multiple frameworks?

Brainstorming as a group, we had the following suggestions & ideas:



for better readability please find a little summarising table below:

Main topic	Ideas	Summary/Description
<b>Building Block</b> definition	<ul style="list-style-type: none"> <li>find functional building blocks</li> <li>think in "driver analogy of the PC world" ( a computer mouse should work on all computers)</li> </ul>	if the SSI-community can agree on Components/Building Blocks which need to "just work" (like plugging in a mouse on a PC), we could more easily create and interoperate ecosystems.
<b>Universality</b> approach	<ul style="list-style-type: none"> <li>universal resolver <a href="#">A Universal Resolver for self-sovereign identifiers   by Markus Sabadello   Decentralized Identity Foundation   Medium</a></li> <li>universal issuer</li> <li>universal registry</li> <li>aggregation</li> <li>proxy service</li> </ul>	the idea is directly connected to the "driver Architecture" and approach of the building Blocks above: the more "universality" the more interoperability.
<b>Layers</b> and Abstraction	<ul style="list-style-type: none"> <li>major layers: identity-layer, format-layer, protocol-layer</li> <li>agree on the number of layers (currently from 3..10)</li> <li>think about "where the semantic changes"</li> <li>Trust over IP foundation approach <a href="#">The ToIP Model - Trust Over IP</a></li> </ul>	Like the analogy with the PC-drivers and connecting a mouse this analogy refers to a "layered stack" just like TCP/IP in the net-domain.

<b>Multi-Stack &amp; multi-Environment</b>	<ul style="list-style-type: none"> <li>• structure domain-environments/sectors</li> <li>• agree on “meta-language” with translator-component or discovery protocol?</li> </ul>	
<b>design the lifecycle of proofs &amp; VCs</b>	<ul style="list-style-type: none"> <li>• proof format is more important than credential format</li> <li>• verifier is where you have flexibility</li> </ul>	look at proofs and verifying to gain flexibility

***“Circle of Specialists” - Do’s & Don’ts learned the hard way: Tech - Marketing - Governance***

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

**Session Notes Taker:** Stephan D. Hofstetter

**(optional) List of Session Attendees:** “A bunch of 10 specialists”

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

We collected a number of Do’s and Dont’s from our professional life. They essentially clustered around:

- Developing Governance - Process - Technology should not be considered a linear process. The first step is educating the multi-disciplinary group in the respective tasks, concerns, objectives, methods, vocabulary and the specificities of their role. The second step is then to entertain an iterative process around legal boundaries, use-cases and expected UX and technological capabilities and constraints.
- Involve Co-opetition rather than firewalling. This creates allies, opportunities, and can mitigate constraints due to limited expert-resources
- Security products need to take a risk-based approach and not be handled as “banana-software”: Focus, accomplish, move-on.

The full map is provided as Picture 5 below.

## “The circle of ~~experts~~ *specialists*”

- Do's and don't's, learned the hard way
- Technology | Marketing | Governance



## Objective

- Have fun discovering, you are not the only one having experienced mistakes or failures
- Share the insights within the group
- Aggregate traps and learnings



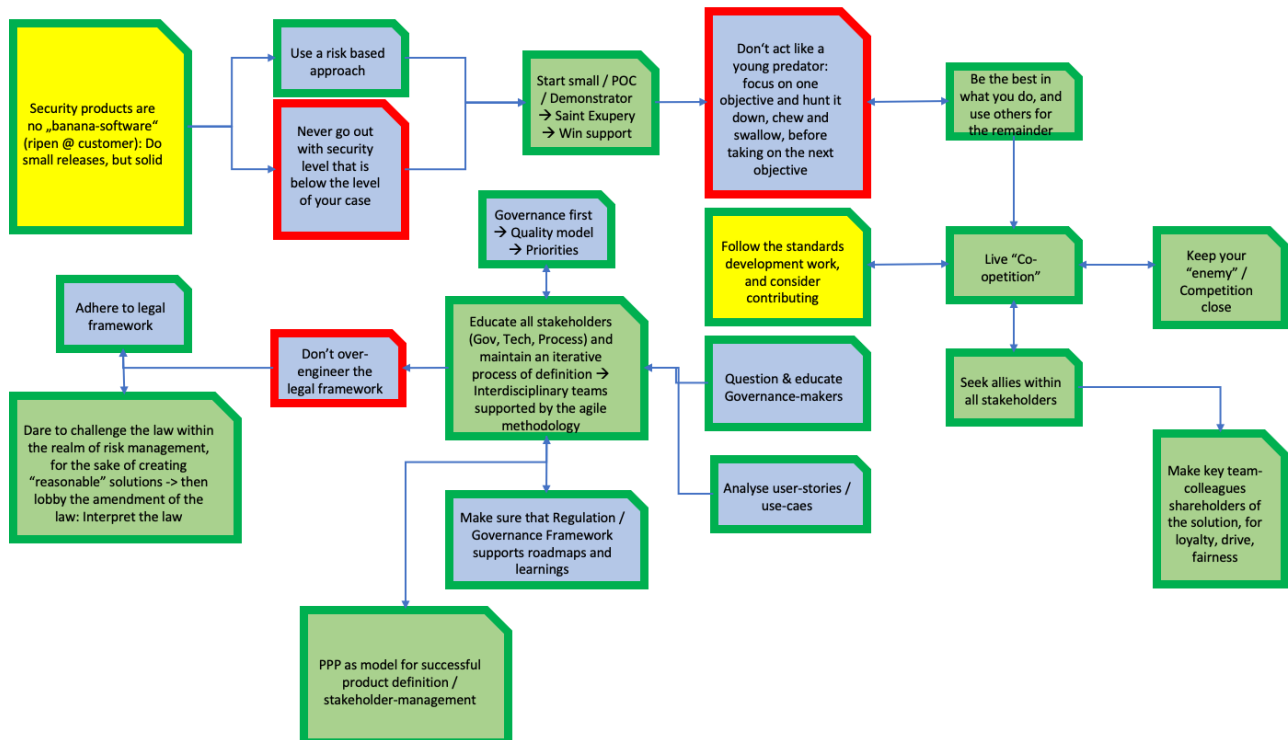
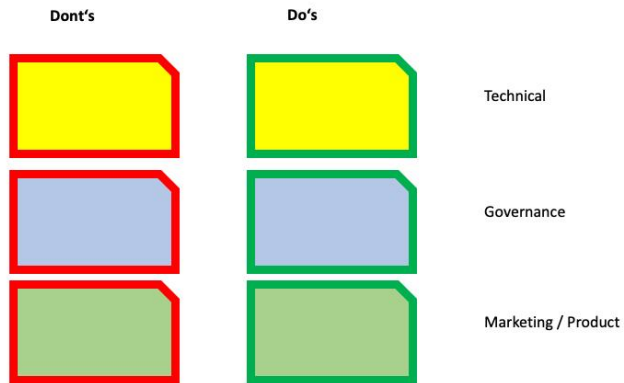
“Well, now we know what not to do.”



# Approach



**"I think we're in good enough shape to start making the same mistakes again."**



## ***Decentralized Social Media + SSI***

**Session Convener:** Dmitri Zagidulin

**Session Notes Taker:**

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

W3C...

'give people a fighting chance' - (but not fully decentralized)

## ***Legal Values for SSIs - Binding SSIs to eIDAS***

**Session Convener:** Andreas Abraham

**Session Notes Taker:**

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

Preliminary notes

- Demo
  - Presentation of an issuer service that issues credentials face-to-face to VIPs to grant access to restricted areas in a hospital
  - Issuance using OID4VC und SIOP2
  - Possibility to manually revoke credentials
  - Manual input of credential data in the issuers web interface
  - Usage of an online signature service to sign (draw a signature by hand)
  - Transmission of the credential offer to the holder via email
  - Legal value
    - Audit trace of the credential issuance and revocation process
    - The audit trace contains the "contract" for issuance that is signed using an eIDAS DSS
    - The credential itself does not contain an eIDAS signature but is regularly signed

## SESSION #9

### *eIDAS 2.0 EUDIW ARF*

**Session Convener:** Andre Kudra, Franziska Granc,  
**Session Notes Taker:** Adrian Doerk



Find more information and the latest version of the ARF here: <https://github.com/eu-digital-identity-wallet>

#### **Overview of eIDAS 2.0 ecosystem / EUDI Wallet** - picture by Intesi Group

PID = Personal identification data (eID)

QEAA = Qualified electronic attribute attestation

Authentic sources = sources of reliable data for different sectors

New trust service: qualified archive service

Introduction of obligations for certain issuers and verifiers to support the EUDI wallet -> e.g.

member states need to offer a wallet and a PID, Big platform providers according to Digital markets act need to accept the EUDI Wallet for authentication

Introduction of the ARF incl. Type 1 and type 2 configuration.

**Is the wallet custodial or self-custody:** Both should be possible - it depends on the wallet integration. For the Level of assurance high a secure hardware is required - not all phones necessarily have that. Then for use cases with high trust requirements might need additional smart cards like existing eID cards. It's also possible that cloud wallets are used. Only a small number of use cases will require level of assurance high.

#### **wallet instance with and without PID?**

A wallet instance itself is a means of identification. Without PID a user would not be able to identify him/ herself, but would still be able to use other credentials. The PID doesn't contain a picture.

### **Who can issue a wallet?**

Member states can decide if a) they offer the wallet themselves b) contract a third party or c) open the market for a certification scheme. Currently there is no peer review process for the notification of eID schemes of member states (eIDAS 1.0). It's currently discussed how a certification scheme for the EUDI Wallets will work.

### **Who can issue and verify credentials to and from the wallet?**

There is a process for the registration of relying parties, but it's unlikely that all relying parties will need to register. There are multiple options to enable authentication of the organisation a wallet is interacting with. Organisational digital identity is and QWAC certificates are potential options.

### **What data from whom can I store in my wallet?**

It's unlikely that it's possible to derive a e.g. Belgian PID into a French wallet. However, a citizen will be able to store and present (Q)EAs from other Member states or organisations.

### **Are there talks about restrictions about relying parties?**

It would be very difficult to build a policy framework to ensure that citizens can't e.g. present sensible attributes to the wrong relying party. There needs to be a certain degree of freedom.

### **Are the current proposed standards sufficient to solve e.g. credential discovery and the transmission of privacy policies?**

Currently probably not. There will be changes over time, currently it's aimed to keep it simple. Too much complexity would cripple the development.

### **What are the large scale pilots?**

There are four large scale pilots funded by the European Commission led by the 2-3 member states, which include organisations from different member states. They run for 2 years and focus on different use cases based on the ARF to provide practical feedback to the legislation. There will be an open source reference implementation, which we can expect to be available in a very early stage in one month.

### **What is type 1 and type 2 credentials?**

They are introduced to group set of requirements. Type one = QEAA and PID, type 2 = everything else. It's recommended to focus on type 2 for general use cases.

### **Will the EUDI Wallet have a biometric engine or will it rely on the device's biometric means?**

There will be a certification on such processes and if they comply with the requirements it's likely that the device based biometric authentication can be used.

### **What about recovery mechanism?**

Recovery of hardware-bound / holder-binding information, which can't be exported a recovery won't be possible. With cloud wallets this might be easier.

## *Open conversation on data vaults*

**Session Convener:** Maaike

**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**

## *Trust frameworks practical (technical) implementation what is out there?*

**Session Convener:** Gabriel Marquie

**Session Notes Taker:**

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

2 families of solution:

- A. chain of trust - PKI / CA based like (credential chaining)
- B. horizontal - Trust list

2 categories of actors to decide to trust or not:

- issuer - for authenticity / trustworthiness
- verifier - for mutual authentication / holder

A. Chain of trust:

there is no known implementation of chain of trust using VCs

B. Trust lists

TRAIN is developing a trust list framework to support trust framework implementations. additional information available here: <https://train.trust-scheme.de/info/>

It was inspired by ETSI trust list.

The list includes for each entity:

role: issuer / verifier

authorisation level: what credential or data element can be issued/verified

W3C verifiable issuers and verifier working group under CCG is working on trust list standardisation <https://w3c-ccg.github.io/verifiable-issuers-verifiers/>

We also touch base on the need for verifier to advertise why they need certain data and the associated privacy policy:

- could be made available in the trust list
- could be passed on in the presentation request
- could be advertised at some given endpoint

this is to be further investigated

Lists of lists need to be also further discussed for delegation scenario

### ***Models of Identity and Interaction - An Exhibition ?***

**Session Convener:** Will Abramson

**Session Notes Taker:** Charles Blass

**(optional) List of Session Attendees:** Daniel, Chance, Michal, Charles, Bart

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

based on Will's PhD work, completed Sept.2022, website new in 2023

<https://iiexhibition.studio>

### ***Practical: Overview and roadmap of Aries Framework Javascript! (it supports more than you think)***

**Session Convener:** Timo - Ajay

**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 #10

### *The usability and privacy trade off - A Technical/Standards bases/ Timo*

**Session Convener:** Timo

**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**

### *Make Credentials Look Good. Together. Today.*

**Session Convener:** Christian Heimann

**Session Notes Taker:** Christian Heimann

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

#### **Starting Point**

Wallet Builders make today that credentials look good – in their own wallet. But it seems that there is currently a lack of common goal to tackle the way, how an issuer can describe, how his credential should look like – across different wallets.

#### **What was done?**

Lissi Wallet started 4 years ago. They implemented the necessary things themselves and the images come from an image server.

Another project uses the OCA-Framework of Human Colossus Foundation.

E-ID Switzerland Project implemented their own way for the prototype wallet.

To define how credentials should look like, it was defined e.g.:

- Skeumorphism (make it look like an analogue Card)
- Image
- Background Image
- Main Color
- Secondary Color
- Logo

- Formats: must be thought dynamically: portrait, landscape, stacked etc. Responsiveness is important.
- User-Info-Signals (as the green Check sign or an orange warning sign)

On a additional Layer data for

- Classification or tagging of the credential is important to improve user experience when a lot of credentials are present — where a simple

The example from Microsoft is mentioned, where only a color, a Logo and an Image is set. The feeling came up that there is no surprise, what attributes need to be defined that a credential can be described and then rendered in a wallet – and across all kind of wallets in the same way.

### **Why is visual representation of a credential important?**

- The attendees agreed upon the definition, that the visual representation never makes a credential authentic. The authenticity always must be checked through the cryptographic proof.
- Marketing. The very first impression is very important. So credentials must look good; from the beginning.
- The Issuer wants to define how his credential looks like.

### **Parking space of thoughts**

- We should differentiate “The List Browser”, where each Credential appears with its complete visual; and how a credential content will be visualized.
- Very specific credential visualizations needs always to be implemented in the wallet; but then the consistency across different wallets could be lost.
- Is it a good way to download the resources from the issuer via URL?

### **How to continue?**

Swiss E-ID Project will have a look at potential solutions OCA, OID4VC as well as the W3C Draft “Verifiable Credentials Rendering Methods” (hint received after the session itself but worth to mention here).

When work happens in this area, the Swiss E-ID Project Team will communicate in a transparent manner, e.g. through the regularly held participation meetings or via their GitHub Repo.

“Start in a pragmatic way” was a well received advice.

### **Links**

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

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



## Standardization and wallet overview

Session Convener: Maaïke

Session Notes Taker: Maaïke

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

Relevant links to the overviews:

- [credential profile comparison matrix](#)
- [wallet overview](#)
- [standardisation overview](#)



**Validated ID** @ValidatedID · Jun 8



We are happy to see Andreas Abraham and Mauro Lucchini, from our team of #VIDchain engineers, at the Digital Identity unConference (#DICE) in Zurich 🇨🇭, engaging and participating in conversations on #identityecosystems. [bit.ly/3P2nAMW](https://bit.ly/3P2nAMW) #digitalidentity #DICE2023 #SSI





## Attendee Comments on Participating in #DICE2023

At the end of the unConference we provided a few minutes for participants to reflect on their experience and to complete the sentence:

**“As a result of attending the Digital Identity OpenSpace unConference Europe....”**

- *I have more perspective about the issues that still need to be shaped for the future of e ID – And these are not limited to technical questions but very much also of legal and political nature. I also will take more the role of an ambassador on this topic in professional as well as personal capacities. Thanks for the positive energies given and shared*
- *I feel more connected to the community leading the world in SSI technology*
- *I got leads to solve some of my challenges*
- *We are on the right track for a global eID System*
- *As a result of attending DICE 2023 I will consider attending IIW*
- *More concepts became clear and I learned more about the industry as a whole*

- ... I'm tempted to attend future SSI Open Space unConferences
- I know that I'm doing the right thing
- I've expanded my bubble, got new insights, and had great discussions
- Finally saw OpenID 4UCI in practice
- I will spend more time learning about the technologies around DDI and think about real life use cases that SSI can help with
- I have seen a lot of people in person for the first time!
- I made some great connections and was inspired by the knowledge of the experts present
- I see the Swiss e-ID project better integrated into the global SSI initiative
- I'm motivated more than ever to share, join forces to promote our community
- I am motivated to dive deeper
- I think everyone needs to work together
- I am completely sold on the OpenSpace unConference format and I got back in touch with the identity community
- I realized that the whole world is striving for a better version of itself. This DICE was of equal insights, brainstorming that of IIW. Looking forward to the next one.
- I know there are many excellent people working on e-ID topic in many different areas with the same goal but different views/approaches, which is great
- I got a very thorough insight into SSI technology in a very short time, met a lot of nice and helpful people who were more than happy to keep helping out even after the unConference, and last but not least got a much clearer picture of where the company I work for could position themselves in the ecosystem
- I got to meet like minded people, make friends, learn the progress in Europe, share the experience of Bhutan NDI and lastly memories for a lifetime!!
- Help closing the gap between business and technology perspectives of SSI framework. I gained a nice network; I explored different ways of deploying SSI
- I met likeminded people and learned a lot
- ... I met cool folks
- I will be busy following up connections, technologies, solutions and communities and I'm more encouraged than ever to stay engaged in the SSI sphere
- I know that government players just have to be brave to make decisions – to go further than...
- I will engage more with the community around SSI/DID's and open social web
- I will deep dive in topics I had on the radar but not in my focus
- I met a lot of experts
- The network of SSI has grown in Europe with deep roots, and we will see a thousand flowers bloom over the next 18 months



**Animo** @AnimoSolutions · Jun 8

Very interesting session on 'How to solve subject binding?' hosted by Maaïke v. Leuker from @TNO\_Research on the balcony at #DICE2023



1



1



9



481



- *I learned a new way to communicate and present much more productively than I knew, I learned a ton of new things that are going on in the SSI community. I realized there is hope / brain power driving this technology forward. I met some great new and old friends*
- *I learned, shared, and collected a lot of crucial things to go ahead to the next level of SSI. Connected with people, organizations and progress with what I will collaborate on.*
- *I feel more interested than ever in SSI*
- *I got to know a new, effective and beautiful way to organize a conference*
- *I secured an invitation to sailing on Lake Geneva*
- *I have some valuable new insights and new ideas. I have some very interesting new contacts*
- *I have enough new follow up activities to keep me busy for the next year*
- *Made new friends and potential colleagues/collaborators. Gained a ton of knowledge and insights re the identity sphere and community - Public Private dynamics Dimensions Had some lovely and profound conversations, including 'off-topic'*
- *I realize we have a long way to go to put the solution into the hands of citizens*
- *I have more new questions than new answers*
- *I discovered a lot of new problems to address in order to develop a sophisticated ID-system and yet by only talking to a few other attendees found ideas and new ways to tackle these problems. Yet this OpenSpace*

*unConference left me with the need of at least another day in order to brainstorm on potential solutions*

- *I better understand my own industry and have met people in person I never would have otherwise*
- *Appreciated did=web more and became aware of potential future developments around it, as well as did=plc / BlueSky uses*
- *Realized that I need to master GITHub*
- *I learned ore about the technology and the passion that goes into making it*
- *There are so many people doing exciting thins in DI and SSI and if we work collectively towards a common global cause we can truly be exceptional and transformative*
- *I feel dumber on a smarter level*
- *I learned to explain what is important in SSI to a wider audience*
- *I want to attend DICE 2024 – I shall visit Zurich more often – my confusion about SSI is now bigger*
- *I could expand my network with diverse, quality contacts*
- *I see which technologies I need to have an eye on in the next months and years*
- *I'm looking forward to join DICE 2024*
- *I believe there are much more sessions like these required – but we made great progress!*
- *I'm eager to attend DICE 2024*
- *I feel enthusiastic knowing I am not alone in the dark. There's light at the end of the tunnel – let's go!*
- *I became more motivated to contribute*
- *Received some clarity on how wallets can be interoperable to share/use VC's*
- *I have a much better understanding of SSI potential and technology. I know where to invest my resources. I appreciate that many in the community also see the social risks and challenges to privacy and freedom*
- *My thoughts/observations about the current status of the SSI stage have been confirmed*
- *Met knew experts face to face, met new people, learned new concepts and ideas*
- *I've found my tribe! Knowing such an engaged and enthusiastic community, ready to work together and share knowledge and experiences, is leading to future of Identity makes me smile*
- *I learned many new ways, methods of implementing SSI. My thought horizon has definitely broadened up. This is the first time I did a knowledge-sharing session and it was a great learning experience.*
- *I am looking forward to attending and participating again*



Lissi @lissi\_id · Jun 9



Our #DICE2023 session: Digital identity is about relationships, not just credentials! With #Lissi wallet demo emphasizing relationships enabled by #DIDcomm powering secure messaging and interactions. #DigitalIdentity



1



6



18



689



Veramo @veramolabs · Jun 8



These pictures from day 1 at #DICE2023 tell it all! 🔥  
Lots of interesting conversations around digital identity, verification, decentralized identity, and more...

#decentralizedidentity #SSI #veramo



4



3



19



720



# Digital Identity OpenSpace unConference Europe #DICE2024

## *Follow DICE on LinkedIn*

Follow the Digital Identity OpenSpace unConference Europe on [LinkedIn](#) to see some posts about this event and to hear about plans for #DICE2024

## *DICE 2024*

Initial planning for DICE2024 is underway and is being planned again in Zurich sometime the second half of June, specific dates to be determined.

Sponsorship opportunities will be published in late August and registration will open in early 2024. Look for undated information at [www.diceurope.org](http://www.diceurope.org) in early autumn.

If you are interested in being a Sponsor and/or helping promote DICE 2024 please email Heidi at [Heidi@HeidiNobantuSaul.com](mailto:Heidi@HeidiNobantuSaul.com)



OpenSpace unConference Facilitation: Heidi Nobantu Saul & Kaliya Young  
Notes Collection & Compilation: Heidi N. Saul



See you at #DICE2024! Mark, Danny, Kaliya and Heidi