BOOK OF PROCEEDNGS

March 4 -5, 2025
Zurich Switzerland
www.diceurope.org

Thank You to our Documentation Center/Book of Proceedings Sponsor: esatus

Contents


WELCOME
@TRUST
SQUARE
THANK YOU
DICE
ECOSYSTEMS
DOCUMENTATION CENTER
Sponsored by
esatus

About DICE Ecosystems

Building Ecosystem Adoption of Verifiable Credentials & Authentic Data

A two-day collaborative event designed to drive the adoption of decentralized identity solutions across diverse business ecosystems.

Collaborate with leading experts to tackle key deployment challenges.

Shape the agenda to focus on topics that matter most to their ecosystem.

Build partnerships and strategies to accelerate the adoption of verifiable credentials.

Who is dice ECOSYSTEMS for
Building trust and economic impact through ecosystems

Companies cultivating networks of interoperability

Enterprises exploring digital and decentralized identity technology

---

Digital and decentralized identity technology startups

This event is specifically for sector-specific, cross-sector, and cross-border business ecosystems that are building out production use cases to support production applications.

The intention is to bring together business experts and technologists who are working on building the digital identity and data ecosystems in Europe.

Through an Open Space unConference format, participants will choose and lead the topics most relevant to their ecosystem goals, driving in-depth discussions and actionable outcomes.

About Digital Identity unConference Europe | DICE

Event Background
The Digital Identity unConference Europe is an Inspired by IIW™ Regionally focused Open Space unConference. 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 venue partner Trust Square (Mark Degan and his fabulous Team) to host and produce the first event in 2023.

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.

The time was right to host an event for the European region with the same OpenSpace unConference format that the Internet Identity Workshop uses. DICE brings 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.

Thank you to our Event Partners

The third iteration of Digital Identity unConference Europe / DICE Ecosystems would not be possible without the Sponsor Partners who stepped up to make this gathering feasible.

Daily Schedule

Monday March 3 / If you are in Zurich
Pre-Conference Apéro 5:00 - 7:00pm
At Trust Square ~ Bahnhofstrasse 75, 8001 Zurich / 3rd Floor
Brought to You by Swisscom

Tuesday March 4 / Open Space unConference Day 1
Doors Open at 9:00
Coffee/Tea & Breakfast Snacks

Opening Circle / Agenda Creation	10:00 -11:30	Working Session 2	14:00 - 15:30
Working Session 1	11:30 -13:00	Working Session 3	15:30 - 17:00
Lunch	13:00 - 14:00	Closing Circle	17:00 - 18:00

DICE Ecosystems Conference Dinner for ALL Attendees
Hotel Restaurant Bar Helvetia
Stauffacherquai 1 CH-8004 Zurich / a 10 minute walk from Trust Square

Brought to you by The Hashgraph Association

Wednesday March 5 / Open Space unConference Day 2
Doors Open at 8:00
Coffee/Tea & Breakfast Snacks

Opening Circle / Agenda Creation	9:00 -10:00	Lunch	13:00 - 14:00
Working Session 4	10:00 -11:30	Working Session 6	14:00 - 15:30
Working Session 5	11:30 - 13:00	Closing Circle / Report Out	15:30 - 16:30

DICE 2025!
September 2, 3 and 4, 2025
Zurich / Venue TBA

DICE Ecosystems Opening Exercise

To open DICE Ecosystems we first invited everyone to say their name and one thing about themselves as we usually do.

We then invited the participants to share the different ecosystems they are a part of or interested in on individual post it notes, collected them and arranged them by general topic on a large glass window.

Here are the Comments that were shared on post its:

- Kickstarting Adoption
- Ecosystem of Ecosystems Enablers
- Privacy
- Dynamic Data Economy
- TRAIN

Organizational ID & Trade

- Organizational Identity with VLEI - GLEIF (2)
- All Use Cases that need secure, certain digital signing authentication and verification and permissioning for organizations and person representing them.
- Trusted Organization

- Company Passport (2)
- B2B
- eInvoicing (2)
- Invoice
- Trade Risk Mitigation
- Product Provenance
- Sustainability Data - waste transfer and environmental permits
- Regenerative Agriculture
- Circular Economy
- Digital Product Passport (2)
- Payments
- Supply Chain (4)
- Value Chains
- Global Trading
- Trade (2)
- Trace Finance
- Finance (10)
- Banking
- Financial Services
- GAN - Financial Services & Digital Identity
- Logistics
- Customs
- Insurance (2)
- Pension
- Onboarding + KYC
- Portable KYC
- Factoring
- Proof Certification
- Discounts and Benefits
- DEFI
- Payments (2)

Entertainment & Sports

- Ticketing
- Media & Entertainment
- Sport (2)
- Gaming and e-Gambling (4)

Telecoms

- Telecommunication
- Communication
- Caller ID Verification
- Call Center Customer Verification via Telephone

Ecosystems with Names

- KERI - Decentralized Key Management System
- Security
- War/Defence
- MOSIP (2)
- SIDI Hub - cross boarder bilateral and multi-lateral agreements for digital identity
- DIDAS
- FIDES (5)

Travel

- Travel IATA
- IATA IdM for distribution chain for travel agencies
- IATA Aviation Security Framework
- Digital Travel Credentials
- Cross Border Travel - especially EU-> NON-EU

Education

- Migration
- Professional Certifications
- Education
- SURF
- NGDIL
- Certification
- Student ID
- Grades
- Education (4)
- Building a CV with VC and submitting Job Applications
- Verifiable Skills and Education

European Wallet Related

- EU Wallet
- e-Signature
- QTSP - Attribute Attestation (3)
- UK - Digital ID Ecosystem Governance
- eID Wallets
- Government Issued IDs public services
- Government C2G & B2G
- E-Democracy
- Government
- Public Services G2C & G2B
- E-Government
- Government Efficiency
- State-Issued Credentials & Public Services

- Swiss E-ID Ecosystem (2)
- Swiss *2G (C2G, B2G, G2G)
- CH-EU Cross boarder
- Swiss Public Sector Identity and Software Supplychain
- SWIYU

Open Source

- Open Source Ecosystem (LF Foundation as an Example)
- Linux Foundation Digital Trust (formerly -Hyperledger)

Health

- Health (2)
- Digital Health (3)
- WHO Global Digital Health Certificate Network (GDHCN)
- Health Data Authenticity
- Health Data for Research
- Personal Health Data Management
- Healthcare Data Exchange - (Secure Private Authentic Confidential)
- Diagnostics Healthcare - Researchers, Labs, Doctors, Patients, Government & Public Healthcare
- Health Credentials

APAC Region

- Australia-Japan Cross Border Working Group - DNP/MeeCo/ConnectID/NAB/CBA/MUFG
- Japan -> Asia Pacific
- Asia Pacific Digital Identity (Japan, South Korea, Singapore, Taiwan, Myanmar, Australia)
- APDI Ecosystem

Open Source & Platforms

- Meta-Ecosystem
- Open Wallet Forum ITU
- Tooling/DevX
- IOTA
- Hyperledger Identus
- IoT Special Interest Group (DIF)
- Device Identity
- Machine Emissions Data
- Energy

Standards

- DIF - Decentralized Identity Foundation
- DID Methods WG (DIF, W3C, INATBA, ToIP)
- International Standardization (IETF, OpenID, W3C, FIDO, ISO)

- Verifiable Credential “Network”
- Rental Background Site)
- e-Lending In a network of libraries - verification and lending rights
- Digital Public Infrastructure

Creative Arts

- Digital Art
- Creator Assertions / Content Authenticity / Content Credentials

ML

- Edge ML Decentralized AI
- Local First
- Datasets for AI Training / ML
- Local First AI
- Decentralized AI

Mobility

- Mobility (vehicle - public transport)
- Mobility
- Automotive

People in Various Contexts

- HR
- Refugees + Aid
- UK OPen Volunteering - Ecosystem (staff passports)
- IDV - nametag IDV
- Social Media
- Ecosystem of Human Beingness -
- First Person
- First Person Credential Ecosystem proof of personhood and verifiable relationships
- Proof of Personhood
- To be or not to be and trust services provider

Market Readiness for EUDI Wallet

- TWINT
- mDL Acceptance
- Mobile Drivers Licence (2)

Agenda Creation = Sessions Called & Hosted by Attendees

41 distinct sessions were called and held over 2 Days.

All sessions called by participants during Opening Circle/Agenda Creation are included and posted on the Agenda Wall by the individual who announced the session.

Agenda Creation takes place at the beginning of each day.

We received notes, slide decks, links to presentations and photos of whiteboard work 32 of these sessions.

Joerg Lenz • 1st
Working on simplicity meeting compliance in combining artificial int...
2mo • Edited •

Building ecosystem adoption of verifiable credentials and authentic data is the theme of Digital Identity unConference Europe | DICE Ecosystems Edition March 2025.

Heidi Nobantu Saul is now introducing the agenda-setting process and Open Space Technology in her role as a facilitator.

Prior to this round Kaliya IdentityWoman Young was collecting attendee feedback on the many types of ecosystems in digital identity.

Soon attendees will propose session topics they are passionate about. Any format goes - ranging from formal presentations to informal discussions.

Every topic proposed is scheduled and added to the Agenda Wall, ensuring all ideas find a space.

Tuesday March 4 2025 / Sessions 1 - 3

Session 1
1A/ NO SESSION
1B/ TRAIN (Enabling interoperable Trust Anchors) How can EBSI, CHEQD, DID:WEB, OPEN IDFoundation - Interoperate? / Isaac Henderson Johnson Jeyakumar
1C/ "What is a digital trust ecosystem and how do we connect the?" PART 1 / Drummond R & Darrell O & Karla McKenna (AYRA and GLEIF

1D/ Portable K.Y.C - Why? Streamline compliance, improve C.X. + combat fraud during custom etc.. onboarding + RE-KYC
TOPICS - what are the key challenges to establish a portable K.Y.C. data ecosystem? What are the enablers? What is the path to adoption /
1E/ To chain or not to chain: DLT / Blockchain options for decentralized identity. / Renata Toktar DSR corporation
1F/ EUDI WALLET 101 (introduction to EUDI wallet + its ecosystem) / Ester M & Business Wallets 303 (taking it to the next level: organizational identity) Samuel R AND German Wallet & bootstrapping the ecosystem / Christian and Paul
1G/ Mapping Decentralized Identity - Predicting the future of the industry with Data / Niza
1H/ NO SESSION

Session 2
2A/ Making Platforms Adaptable to Many Ecosystems (How we issue in 5 Formats and Don't Lose our Minds) / Meruc Auvo Digital
2B/ Challenge in adopting Swiss e-ID - To improve onboarding and custom acquisition / Michael Jarmolkowicz
2C/ Verifiable Trade & Org - ID in Trade and supply-chain protocol / Stephan Wolf
Kickstarting Adoption = Ideas, Strategies / Maurten Sphereon
2D/ Go-to-market strategies for Digital ID Wallet Ecosystems / Zack and Pavel
2E/ AMA SWIYU - Trust infrastructure Swiss Confederation / Rolf & Team
2F/ Dancing and Fitting In with Ecosystems (First Person Credentials) / Darrell O (AYRA)
2G/ Technical Focus Topics & Missing Building Blocks -> Zero - Knowledge Proofs -> W3C Digital Credentials API / Paul, Micha, Christian, Anja
2H/ Dynamic Data Economy / Human Colossus Foundation

Session 3
3A/ History of ID Tech (pre industrial) / T Serlet
3B/ Paving the way from PDF to VC / Christian, Patrich, Fahian (?)
3C/ How to use CH E-ID as EU - PID (Brainstorming session How to: without waiting - bilateral CH-EI agreement / Ro…Z
3D/ Digital Health - based on trust infrastructure. How to get adoption? / Peter and Oli
3E/ eInvoicing & Blue Pages -> organization discovery / E (?) Hans (?) Al..? Names illegible
3F/ What is missing in the EUDI Trust Model and why won't EUDI Wallets work outside Europe? / Samuel (Findynet
3G/ DID Methods Standardization + did'scid Method (solving cross-ecosystem portability) / Ankur and Markus and Drummond
3H/ Cultivating ecosystems in the real world: California mDLs and IATA Aviation Security Trust Framework / Lucy Y.

Wednesday March 5 2025 / Sessions 3 - 6

Session 4
4A/ How to map a national Digital ID Ecosystem. What we're doing in the UK - Discuss if it works for others / Graham Francis
4B/ SSI + AI Agents - Local First AI, Sovereign Knowledge Graphs, Non-credential data / Pavlyshyn (MYKIN.AI)

4C/ e-GOV use-cases / Hauns, Victor, Daniel
4D/ How to Mitigate: UX,Compliance, Tech, Certificates, - Role of Trust Service Providers - Simplify adoption platforms (29+ EU SWISS UKRAIN etc.) / Roger - Ver.id
4E/ Hardening did: scid, did:webs…. (white boarding session) / Ankur, Markus, Drummond
4F/ About FIDES / Harman, Hans, Eelco
4G/ Privacy & ZKP use-cases & requirements discussion / Anja, Christian, Paul
4H/ Driving Adoption by extending the bubble. FIND THE Target group via a survey in their language / Roman Z

Session 5
5A/ State of the art on AI (e.g., "vibe coding", "boomer prompting") and how decentralized identity can build Verifiable AI / Ankur B (cheqd)
5B/ Business Case / Ecosystem = Sharing Health Data for R&D / Dominik Geller
5C/ Registrant - TRAIN Based onboarding tool for Service Providers (real-world ecosystem eg.) / Lucy and Isaac
5D/ Proposal to Update - FINMA regulations to enable RE-USE of PORTABLE KYC / Michal J and Damian G
5E/ NO SESSION
5F/ ARF 1.6 - Open Discussion : (un) linkability - batch & re-issuance, privacy risks & mitigation / Viky & Ester
5G/ NO SESSION
5H/ NO SESSION

LUNCH SESSION Space C: Educational Offerings re: Digital ID / Kaliya & Emrys

Session 6
6A/ Hedera Hashgraph SSI Ecosystem (DID:Hedra Method) / Renata and Micha
6B/ You get the adoption you deserve. Our journey building truly decentralized identifiers for Swiss healthcare, and the path forward, / Geor + This
6C/ How do we make Value more visible? What are we missing? & ECOSYSTEM ENABLERS - Awareness, Education, Training, Resources, and Gaps / James Monaghan
6D/ NO SESSION
6E/ NO SESSION
6F/ The First BILLION USER Credential / Drummond R. & First Person Ayra Project Contributors
6G/ EU DI Framework + beyond - Mapping the road ahead 2025/26 / Jeorg Lenz AND Existing Ecosystems = Apple's and Google's plans on ID Wallets / Franzinka Granc
6H/ NO SESSION

Session Notes Day 1 / Sessions 1 - 3

SESSION #1

TRAIN (Enabling interoperable Trust Anchors) How can EBSI, cheqd, did:web, OpenID Federation etc interoperate?

Session Convener: Isaac Henderson Johnson Jeyakumar
Session Notes Taker: Ankur Banerjee

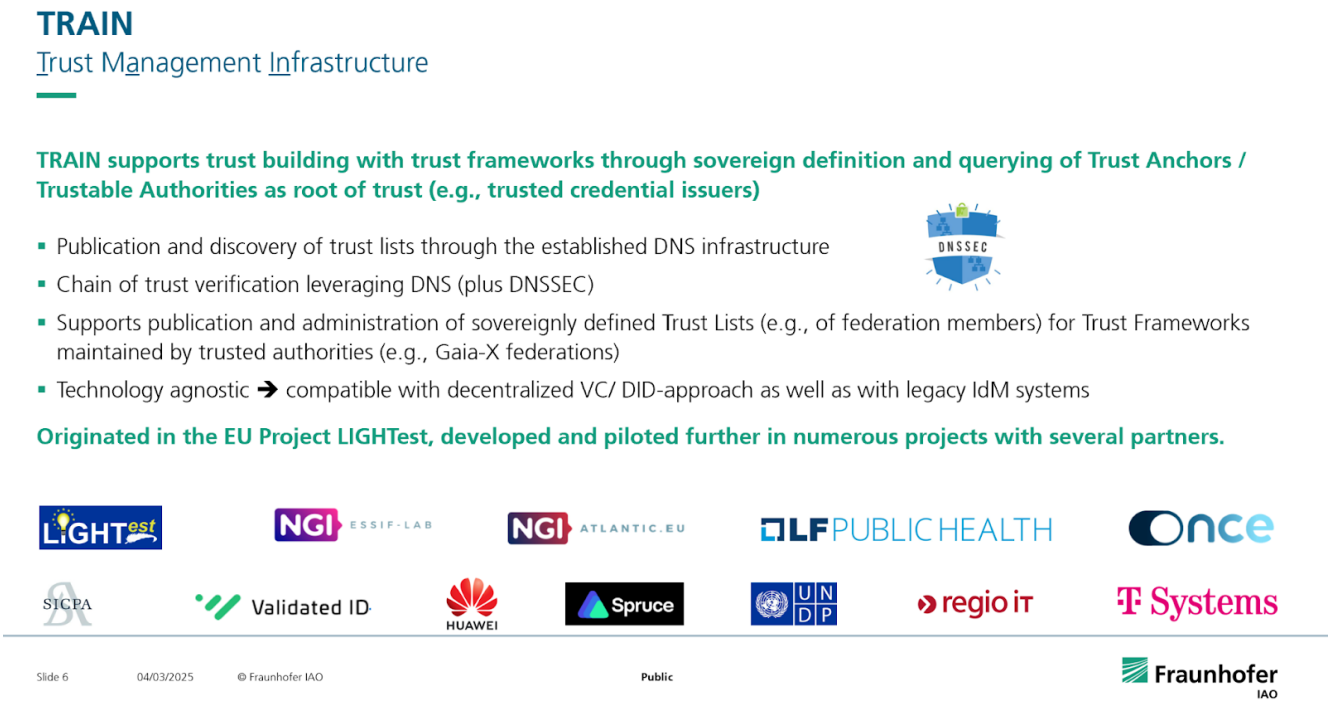
What Ecosystem(s) were present in the room/session?

EBSI (European Blockchain Services Infrastructure), cheqd, did:web

What Ecosystem challenges did the conversation focus on, address?

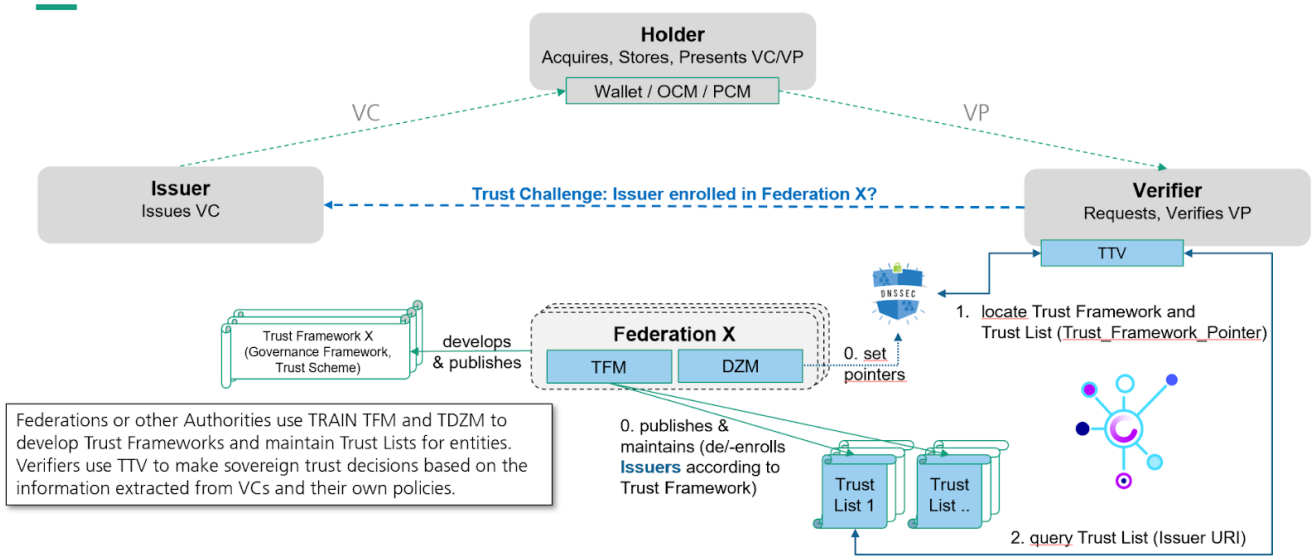
How can trust lists/registries interoperate across multiple ecosystems that use different mechanisms for trust list definition and distribution

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



TRAIN in GXFS

Overview



TRAIN Architecture

Subline

TRAIN DNS Trustzone Manager (DZM)

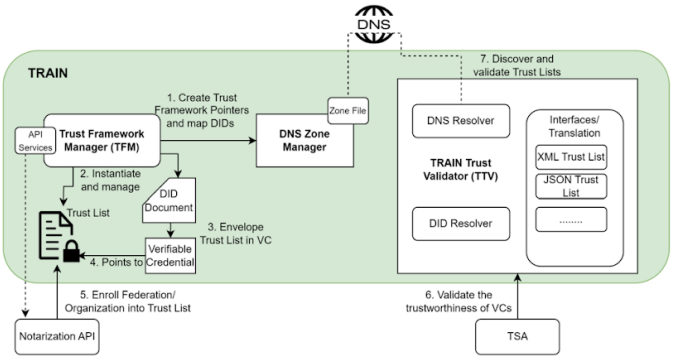
- Anchoring a Trust Framework in the DNS Pointer Resource Record (PTR RR)
- Trust List URI DID is anchored in DNS URI Resource Record (URI RR)
- Global discovery through DNS and DNSSEC for chain of trust

TRAIN Trust Framework Manager (TFM)

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

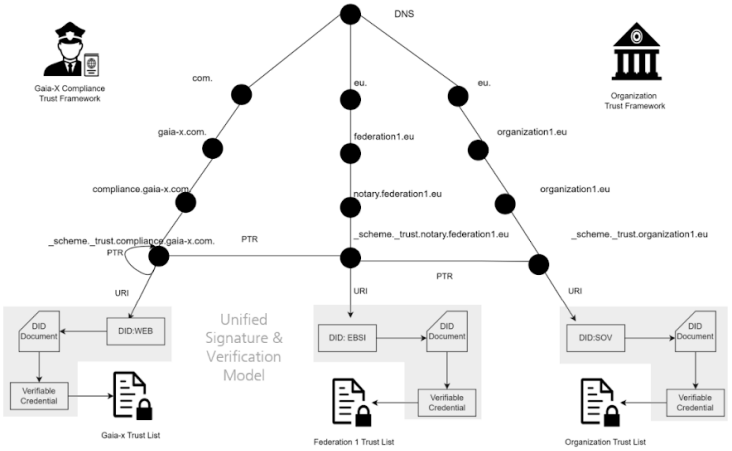
TRAIN Trust Validator (TTV)

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



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

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

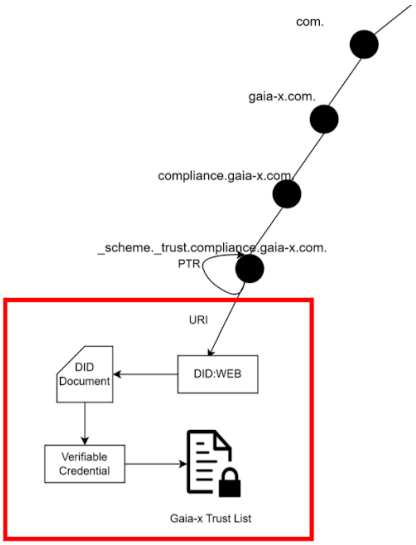


DNS	Resource Record	Function
PTR	_scheme._trust.compliance.gaia-x.com	Trust Framework Pointer
PTR	_scheme._trust.notary.federation1.eu	Trust Framework Pointer
URI	http://some.org/trust_list / did.example...	Trust List Location URI

Unified Signature & Verification Model

Trust Lists via DID and VC

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



Process

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

Follow-Up:

- Credenco Wallet
- Heidi Wallet
- Cooperation with Ayra

Specification: Write a specification on Universal trust resolver for different trust anchors

TRAIN official website: https://train.trust-scheme.de/info/

What is a digital trust ecosystem and how do we connect them?

Session Convener: Drummond Reed, Darrell O'Donnell, Karla McKenna
Session Notes Taker: Drummond Reed

What Ecosystem(s) were present in the room/session?

Ayra, GLEIF, Swiss EID, UK Gov, Germany, Verifiable Trade

What Ecosystem challenges did the conversation focus on, address?

Coming up with a concrete definition of the requirements for a digital trust ecosystem. We agreed that there were three key requirements for a viable ecosystem:

1. **Governance of some kind by a governing body of some kind** (ideally with a primary governance document that has a verifiable identifier such as a DID)
2. **Design of a credential family** (which should be published as part of the governance documents)
3. **One or more interoperable trust registries** (governed by the governance documents and with verifiable identifiers that can be resolved to determine a network endpoint).

We discussed several examples of existing ecosystems that have these elements, including the GLEIF vLEI ecosystem, the UK ecosystem, and the Verifiable Trade ecosystem.

In the final part of the session, we talked about how to connect ecosystems via trust registry query standards such as the ToIP Trust Registry Query Protocol (TRQP). In the session we reviewed the TRQP Specification Overview document on the ToIP wiki. This protocol is "DNS for trust" as described in the Ayra white paper The Ecosystem of Ecosystems Model for Decentralized Digital Trust Infrastructure.

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

The key point was the much more concrete definition of a digital trust ecosystem that we noted above—and the fact that the evidence of the healthy growth of digital trust ecosystems will be the level of activity across a network of interoperable trust registries.

Portable K.Y.C - Challenges, Enablers, Path to Adoption

Session Convener: Damian Glover
Session Notes Taker: Damian Glover

What Ecosystem(s) were present in the room/session?

Financial services companies, Identify verification providers, standards orgs, consultancies

What Ecosystem challenges did the conversation focus on, address?

There is an opportunity for banks to issue BankID-style credentials directly to a new customer after ID proofing. Initially these VCs would probably be for re-use within the group (e.g. to facilitate re-onboarding to new jurisdictions and/or periodic re-KYC), with potential for customers to use the credentials to prove their identity and other attributes within the wider financial services ecosystem (e.g. with financial advisors, mortgage brokers, credit card companies etc).

Key challenges

- Differences between the KYC process within a bank may mean that the KYC data collected in one jurisdiction might not be valid in another jurisdiction (or might only be partially valid)
- Banks may not want to enable competitors to verify credentials they issued (on the other hand, GPDR mandates that consumers have the right to request a copy of their personal information)
- Who is liable for incorrect data, if a third party uses a bank-issued VC to verify a user?
- Credential lifecycle management e.g. how will bank-issued credentials be kept valid, who has the right to revoke credentials?

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

The session team identified a number of steps that could help bring this opportunity closer to reality.

- Agree a common set of attributes for KYC data in the banking sector (banks will have different requirements, the question is what is the minimal set of attributes needed for every customer)
- Define “Portable KYC File v1” (schema for first version of bank-issued KYC credential / presentation request, e.g. based on common data needed by all Relying Parties)
- Consider proposing an amendment to the local AML law that defines authentic data sources for these attributes, enabling them to be issued as re-usable Verifiable Credentials (e.g. speak to FINMA in Switzerland)

To chain or not to chain: DLT / Blockchain options for decentralized identity.

Session Convener: Renata Toktar DSR corporation
Session Notes Taker: No Notes Submitted

What Ecosystem(s) were present in the room/session?

What Ecosystem challenges did the conversation focus on, address?

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

NO NOTES SUBMITTED

What is a (European Digital Identity) wallet? Status of the German wallet. What is an organizational wallet?

Session Convener: Esther Makaay, Christian Bormann, Paul Bastian, Samuel Rinnetmäki
Session Notes Taker: Esther Makaay, Samuel Rinnetmäki

Slides from the introduction (EUDI Wallet 101): 20250303-DICE-Day1F-EUDI-Wallets-101.pdf

If you want to have an early experience with using the EUDI Wallet(s), you can join Phase2 end-user piloting in EWC next week (10 March - open for a few weeks - fully online). Reach out to Esther Makaay & she'll get you an invitation to join.

Useful links:

- EDI Framework legal text: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401183
- eIDAS Regulation - 910/2014 - EN - e-IDAS - EUR-Lex
- Consolidated version (**not official legal text!**) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.EN *not working*
- List of current Implementing Acts with eIDAS: Search results - EUR-Lex
- Consultations on Implementing Acts: European Commission - Have your say
- ARF on Github: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework
- ARF topics raised for open discussion: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/tree/main/docs/discussion-topics

- Reference Implementation wallet: https://github.com/eu-digital-identity-wallet/.github/blob/main/profile/reference-implementation.md
- EC website - starting page linking to all relevant topics (ARF, RI wallet, LSPs, communication topics, legislation and more): https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home

Slides on the German Wallet:
DICE_03_2025-german-wallet
German Architecture Proposal: https://bmi.usercontent.opencode.de/eudi-wallet/eidas-2.0-architekturkonzept/

Slides on the Business Wallet:
How to think about organizational identity and organization wallets

OpenWallet Foundation's list of digital wallets and agents

What Ecosystem(s) were present in the room/session?

- Core focus is the EUDI Wallet ecosystem

Present ecosystems:

- Findynet
- Procivis
- German wallet (SPRIND, Bundesdruckerei)
- EUDI Wallet Consortium large-scale pilot (Esther, Samuel)

What Ecosystem challenges did the conversation focus on, address?

Understanding the basics and having a shared understanding of the core terms.

Challenges related to regulation-based ecosystems: the eIDAS regulation is already in force, and the European Commission will issue implementing regulations pointing to standards and technical specifications still under construction.

Fragmented wallet landscape.

Governments not understanding organizational identity yet.

Focus on eID and authentication (logging in to public online services) – not enough thinking around data-sharing.

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

This was an informational session. See presentations/links above

Mapping Decentralized Identity - Predicting the future of the industry with Data

Session Convener: Niza Gonzalez
Session Notes Taker: Nicole Torres

What Ecosystem(s) were present in the room/session?

DeFi, supply chain, digital assets, education, sustainability

What Ecosystem challenges did the conversation focus on, address?

Data quality assurance and the maintenance of the map

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

- Presentation of the Web of Trust Map
- Why it was built - Bridging the knowledge gap, supporting governments & policymakers, accelerating research, advancing interoperability, growing the community
- How it was built - Timeframe, inclusion criteria, +70 research and technological variables. Variables including ID Projects, consortia, blockchains, private entities, public entities, regulations, standards/protocols, people, DLT tech, DID methods, managing entity, endorses/uses ZKP, has exportable credentials, interoperability or integration, public code repository, targets holders, issuers, and/or verifiers
- Integrations - OWF Digital Wallet and Agent Overview SIG, and DID directory
- Gathered data - +250 projects, +30 Consortia, +1000 public entities, +3500 private entities, +3500 industry experts,126 countries working on Decentralized Identity, Top Industry - Finance, DLTs/Blockchains - 140, DID Methods - 134, Top 5 DID methods used
- Map Demo
- Used the search tool to look up requests from attendees. This included cases such as:

a. DIDAS, DICE, Potential
b. Hedera as an entity and blockchain
c. Blockchain - Findynet Network
d. Filtered type of industry - education
e. DLT Tech - Hyperledger Indy
f. Filtered type of industry - Sustainability
g. Map visualization and geographical view - Switzerland
h. Entity - SICPA Holding SA
i. Digital Credentials Consortium

- Future of Web of Trust Map - Community driven growth, expanding the dataset, automation & AI, advanced Visualization

SESSION #2

Making Platforms Adaptable to Many Ecosystems

Session Convener: Merul
Session Notes Taker: Merul

What Ecosystem(s) were present in the room/session?

FIDES, Walt.ID, Ayra, German EID Wallet, Heidi (Ubique)

What Ecosystem challenges did the conversation focus on, address?

Interoperability between standards

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

We talked about how we can unmarry a product from standards and how platforms can adapt on the fly according to what different wallets request.

slides attached below:
Making Systems Adaptable - DICE.pptx

Challenges in adopting Swiss e-ID to improve onboarding and customer acquisition

Session Convener: Michael Jarmolkowicz
Session Notes Taker: Damian Glover

What Ecosystem(s) were present in the room/session?

Financial services companies, Identify verification providers, standards orgs, consultancies

What Ecosystem challenges did the conversation focus on, address?

- No major technical hurdles were identified to adoption of the Swiss e-ID by banks; rather, the key question raised by the session team was, will citizens adopt the e-ID / will there be a killer use case that drives adoption?

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

- Verification can be performed by the Relying Party, or third party vendor with a direct relationship with the Relying Party
- Clarification is needed regarding what evidence banks should retain following verification of an e-ID
- The key action for banks is to focus on use cases that will improve the customer experience

Verifiable Trade & Org - ID in Trade and supply-chain protocol

Session Convener: Stephan Wolf
Session Notes Taker:

What Ecosystem(s) were present in the room/session?

What Ecosystem challenges did the conversation focus on, address?

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

NO NOTES SUBMITTED

Kickstarting adoption & GTM Strategies

Session Convener: Pavol Hrina, Zack Jones, Maarten Boender
Session Notes Taker: Pavol Hrina, James Monaghan

What Ecosystem(s) were present in the room/session?

Trinsic, Swiss eID, EUDI W.

What Ecosystem challenges did the conversation focus on, address?

- **Chicken and Egg Problem:** Relying parties (RPs) need issuers to issue credentials before they can use the system, creating a deadlock in adoption.
- **Government's Role:** Public organizations should lead by example and incentivize ecosystem development rather than getting pressured into premature implementations.
- **Interoperability Issues:** Wallets should be capable of handling multiple credential types and presenting them seamlessly.
- **User Resistance & Incentives:** Many users already have eIDs or existing solutions, making it difficult to justify switching unless there is a clear benefit.
- **Regulatory Uncertainty:** Consequences of non-compliance with EUDI Wallet deadlines (e.g., December 27, 2025) remain unclear.
- **Low Adoption of mDLs (Mobile Driver's Licenses):** Adoption in the U.S. is low because states control rollout independently, leading to fragmentation.
- **Risk Aversion by Organizations:** Many organizations put digital identity initiatives on risk lists and do the minimum required to avoid fines, similar to GDPR compliance.
- **Lack of a Business Model:** There is uncertainty regarding who bears liability if something goes wrong and what incentives exist for issuers and verifiers.
- **Lack of Compelling Use Cases:** The physical use case for digital IDs isn't strong enough—new use cases must be introduced to drive demand.
- **Adoption Strategy:** Understanding how to drive adoption from B2B to B2C, including leveraging hackathons, large companies, and regulatory pressure.

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

Compelling Use Cases for Digital Identity Adoption:

- **Government Services**: Attestation of residence, tax identification.
- **Healthcare**: Strong authentication for electronic patient records.
- **Logistics**: Address verification and change updates.
- **E-commerce & B2B**: System-to-system trusted credential exchanges.
- **Device-to-Device Verification**: Ensuring sensor authenticity and preventing hacking.
- **Reception Desk & Office Entry**: Identity verification for visitors.
- **Age Verification**: A frequent and valuable use case (e.g., Amazon exploring mDL adoption).

Key Factors for Successful Adoption:

- **Frequency of Use Cases**: Credentials must be frequently used to justify adoption.
- **Wallet Integration into Existing Processes**: Enhance convenience and add new capabilities.
- **Interoperability**: Wallets should work seamlessly across different credential issuers.
- **Government as a Catalyst**: Governments should enforce deadlines and lead by example.
- **Leveraging Large Companies**: Big companies (e.g., G20 pushing LEI adoption) can force ecosystem-wide adoption.
- **Smaller Businesses as Early Adopters**: They have more incentives to adopt digital identity solutions due to their lack of existing infrastructure.
- **Awareness & Education**: Businesses must recognize the legal value of credentials and the benefits of adoption.

Tactics for Breaking the Adoption Deadlock:

- **Regulatory Pressure**: Ensure compliance deadlines are met and understood.
- **Demonstrating Value**: Organizations need a clear value proposition to justify investment.
- **Hackathons & Pilots**: Events like the CA DMV's hackathons can engage banks and businesses.
- **Incremental Steps**: Start with foundational identity verification methods (e.g., DocV) before moving to fully-fledged digital wallets.
- **Industry Collaboration**: Education and consulting can drive local ecosystem adoption, creating opportunities for businesses to provide training and advisory services.

Final Conclusion: **Just find the value and get STARTED!** The digital identity landscape will evolve over the next two years, and businesses must begin building capabilities now to be ready for future opportunities.

swiyu Ask me anything (Swiss e-ID)

Session Convener: Rolf Rauschenbach + team
Session Notes Taker: e-ID Team + Stefan Koller

What Ecosystem(s) were present in the room/session?

STFI (Swiss Fintech Innovations) representing CH Banks, IT Service Providers,

What Ecosystem challenges did the conversation focus on, address?

See below

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

- **SFTI will define schemas for banking use cases and clarify what the government provides in terms of verification tools, verifiable credentials (VCs), and more. What can municipalities and the private industry expect?**
- Regarding e-ID verification, the government provides a generic verifier on GitHub. However, they only offer software, not infrastructure. Municipalities need to take action to perform the verification, with support from the government, although not full support. IT service providers are likely to assist in this process.
- An app will be available for verification, but it does not generate an audit trail. It is not suitable for banks but rather for privacy-preserving topics. The app allows for different identification cases, such as age verification with a limited data set. Full data will not be available on the mobile app, and the verifier's phone will not store the data, including blocking screenshots. The verifier app will be limited in use cases.

- **Timing of trust registers and who is verifying what: any ideas on private cases?**
    - Trust registry offered for very broad set of entities in CH with UID or e-ID and / or gov. agencies. Incl. check if requester is “zeichnungsberechtigt” and check of possession (identity claim). Legitimacy claim: not in scope or Auftrag des Bundes.
    - Governmental actors (schema owners) will define trusted issuer and verifier. For private sector and more complex eco-systems, this can be based on the identity statement in the base registry. Must be deployed by private companies themselves.
- **Is a ticket verification feasible (combining ticket with age)**
    - As of today this is not feasible, but under discussion. More realistic that ticketing solutions as Ticketcorner will do something

- **Can Swiyu be connected to private registers?**
    - Time will tell. In an ideal world this would happen, but we cannot tell at the moment.
- **Policy based validation supported?**

- Yes, GV enables companies to use APIs (abstraction layer available, no need for deep technical / protocol knowhow)
- At the beginning abstraction layer, community highly welcome to add on that with more refined policy.

- **Social security number: can anyone access this with the generic verifier?**
  - Technically yes, legally no. Legal basis is clear.
  - EU plans to onboard each verifier and it's usecase incl. dataset individually. Switzerland has a more liberal approach. Its up to the verifier to define which data is requested. nDSG outlines what is legally possible. Holder can chose to share or not to share.
  - No private company is allowed to access SSN (exceptions and use cases clearly defined i.e. healthcare cases).
  - User guidance / warnings and safeguards for data sharing / disclosing is implemented as well as a reporting process.

- **Every CH citizen can apply for an e-ID. Is residency status part of e-ID status?**
  - Not part of the e-ID data scheme. E-ID will not solve this problem. This must be done by municipality (attestation of domicile). Unfortunately, so far no agreed schema for attestation of domicile exists.
  - SBB is highly interested in this credential. Probably an alliance of willing parties will be established.
  - Any analogue reference document (Pass, ID, Ausländerausweis) will be linked to e-ID

- **Wallet bindings / e-ID in other wallets?**
  - FedPol needs to ensure holder binding. We do this by binding it to a device who is in possession of holder by the time of issuance. This is achieved by the Swiss Federal Wallet.
  - Issuance to third party wallets trough Key Attestation (Certification needed. Competence is given to federal council, unclear if FC will act on this competence)

Access to central trust registry each time?

- Not the goal of BIT, as this would create a honeypot.
- Base registry lookup with credential would be privacy preserving
- Proxy could be deployed in front of registry.

What happens if registry goes down?

- Redundant setup will minimize this
- VC at the holder device will still be available – "only" revocation would not be up to date
- Offline use cases are important as well

Is there a discussion of Switzerland being part of trust registry of Europe?

- Intent to get there. At the moment not directly working on it. All parties are busy getting their own stuff done.
- Legal basis for discussion not yet given.
- Roots of trust in CH and EU are very different, this will not be an easy task.

Is trust registry open to anyone?

- Yes, but organizations must be domiciled in Switzerland.
- It is accessible to anybody globally.

Infra useable to own use-cases?

- Yes, but not for free if you want to be in the trust registry (fee for infrastructure, acts as "firewall" as well)
- Any entity can be in the trust registry (application)

If I want more privacy in my use case, do I stay in the base registry?

- Just do mutual end-to-end encryption. This gives you more privacy.
- All other questions answered before (implementation without constant callbacks to trust registry).

OpenID Swiss version for trust protocol (non- standard / Swiss-finish) implemented. Will this be an interoperability issue?

- No, it will be an asset. Open ID federation might converge in an international standard. We don't want a Swiss finish, but most pragmatic approach is to use Swiss version at the moment.
- Management of tech lifecycle will be challenging.

Duration of the e-ID? Synced to passport?

- Max duration is duration of root document.
- Might be necessary to have a shorter technical duration due to IT security. But legally, the rood document is defining the span.

FINMA discussion: will e-ID be equivalent?

- Cannot give a precise answer, but there is contact between FINMA and BIT.
- Ordonnance should be sufficient to change.

Picture in e-ID?

- Same as on the passport / ID

What data can the verifier see?

- Check app: age verification (zkp age) and picture
- Generic verifier: anything

Biometrically unlocking wallet enforced?

- Either password or biometrics

Can a Verifier re-use data for own VCs? i.E. pictures?

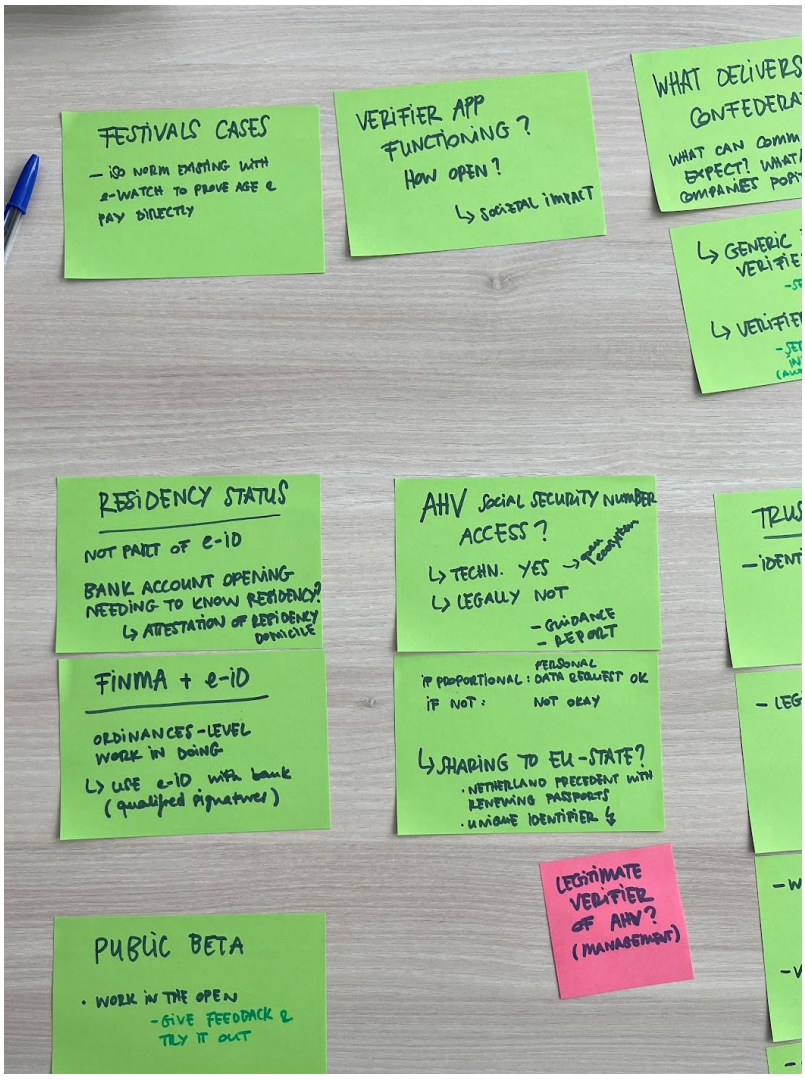
- E-ID act has no wide raging regulation on how the data can be used.
- Must be in line with DSG.
- Each use case has to be evaluated on a legal basis
- Payload can be re-used to issue a new VCs

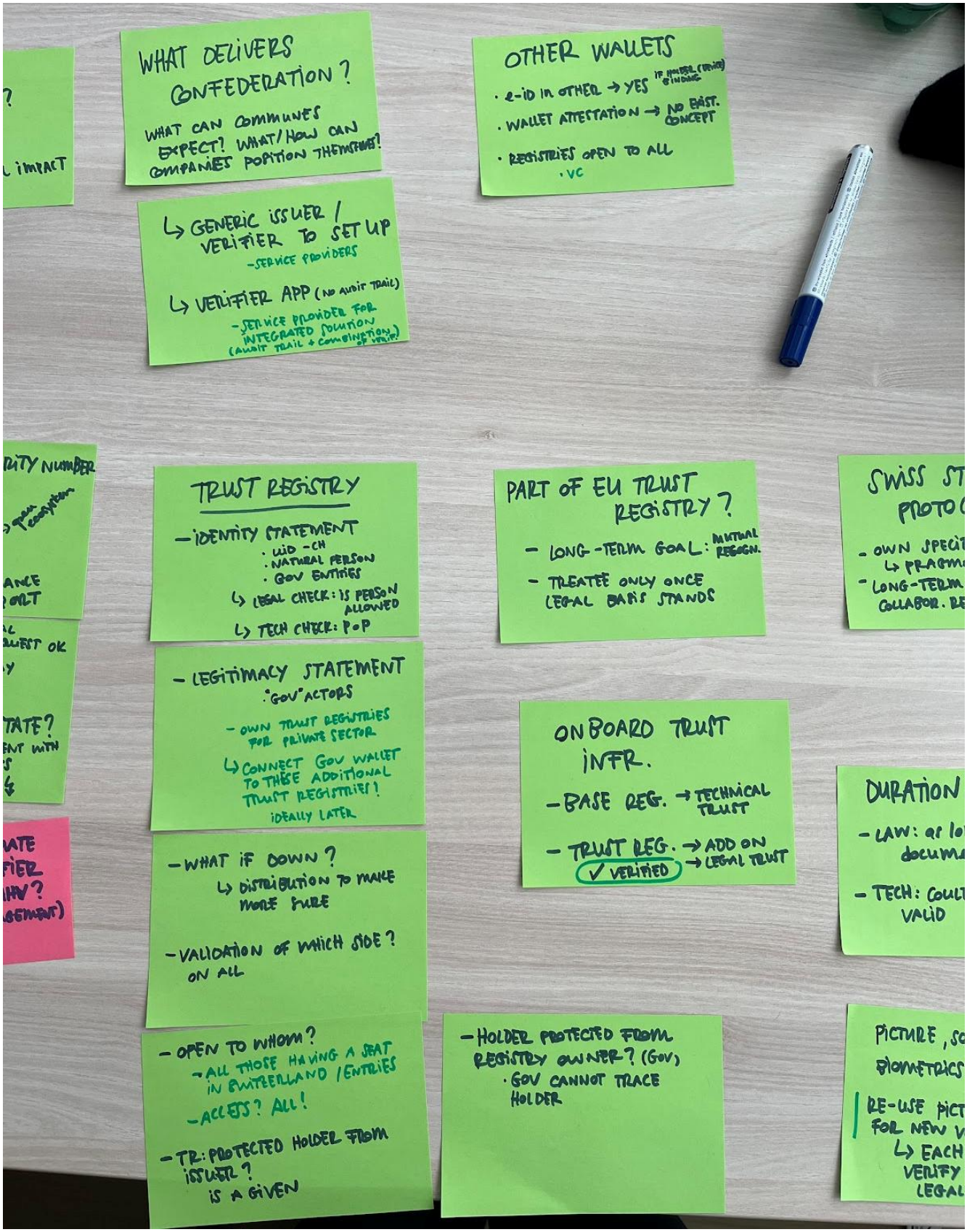
Who is the owner of the data?

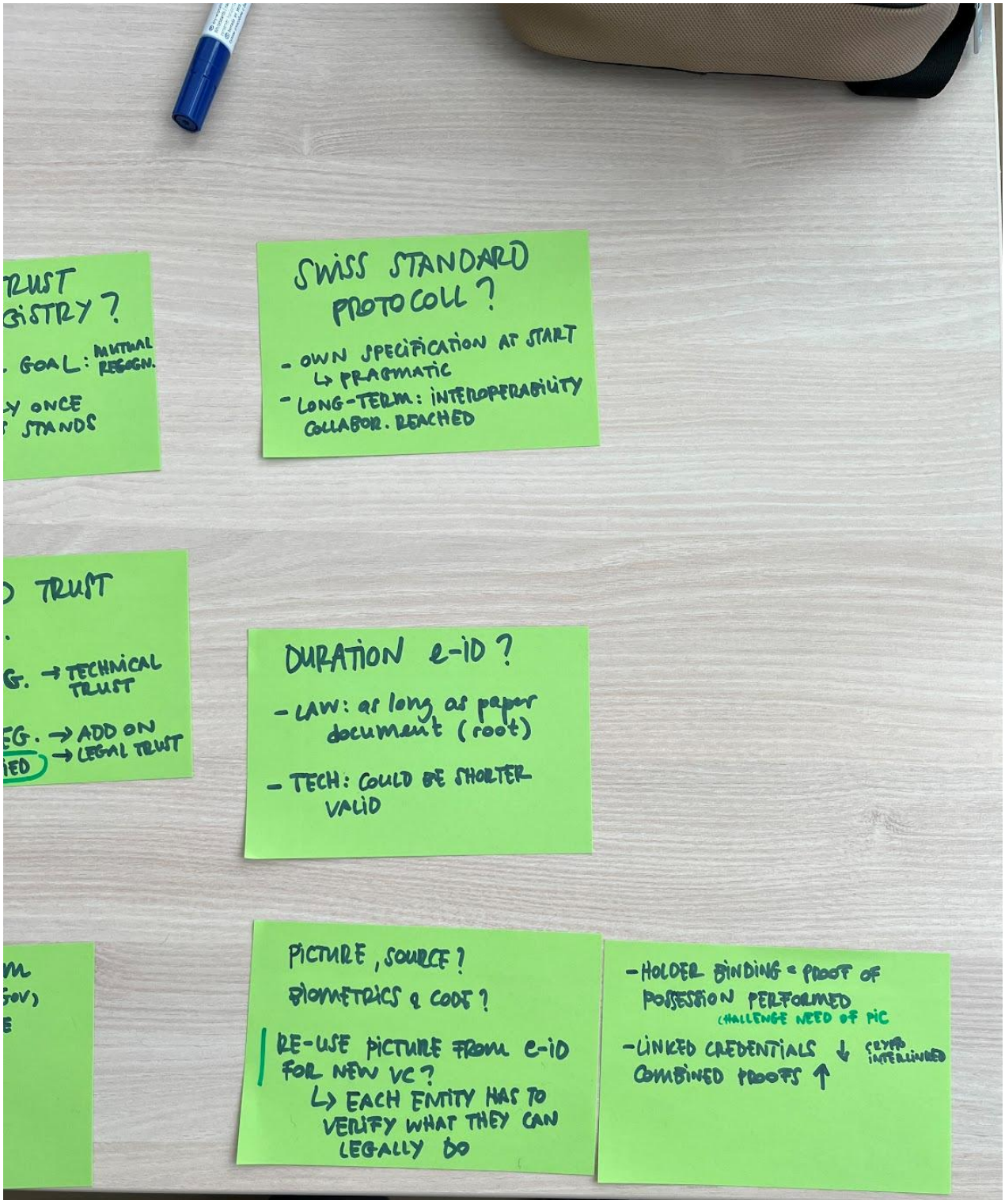
- Its up to the holder, what they share with whom.
- Its up to the verifier, what data is strictly needed for the use-case
- As user-/device binding is strong, picture usecase probably not that important

Interlinking credentials (i.e. conditional ticketing) feasible?

- Combined proofing will be more sustainable use cases instead of interlinking of credentials (this chain might break). Not very automation friendly, but easier to handle.




WHAT DELIVERS CONFEDERATION?
WHAT CAN COMMUNES EXPECT? WHAT/HOW CAN COMPANIES POSITION THEMSELVES?
OTHER WALLETS
· e-ID in other → YES
· WALLET ATTESTATION → NO BASIC CONCEPT
· REGISTRIES OPEN TO ALL
· VC
↳ GENERIC ISSUER / VERIFIER TO SET UP
-SERVICE PROVIDERS
↳ VERIFIER APP (NO AUDIT TRAIL)
-SERVICE PROVIDER FOR INTEGRATED SOLUTION (AUDIT TRAIL + COMBINATION OF VERIF.)
TRUST REGISTRY
- IDENTITY STATEMENT
· UID -CH
· NATURAL PERSON
· GOV ENTITIES
↳ LEGAL CHECK: IS PERSON ALLOWED
↳ TECH CHECK: PoP
- LEGITIMACY STATEMENT
"GOV" ACTORS
- OWN TRUST REGISTRIES FOR PRIVATE SECTOR
↳ CONNECT GOV WALLET TO THESE ADDITIONAL TRUST REGISTRIES!
IDEALLY LATER
PART OF EU TRUST REGISTRY?
- LONG-TERM GOAL: MUTUAL RECOGN.
- TREATEE ONLY ONCE LEGAL BASIS STANDS
ONBOARD TRUST INFR.
- BASE REG. → TECHNICAL TRUST
- TRUST REG. → ADD ON
✓ VERIFIED → LEGAL TRUST
- WHAT IF DOWN?
↳ DISTRIBUTION TO MAKE MORE SURE
- VALIDATION OF WHICH SIDE?
ON ALL
- OPEN TO WHOM?
- ALL THOSE HAVING A SEAT IN SWITZERLAND / ENTRIES
- ACCESS? ALL!
- TR: PROTECTED HOLDER FROM ISSUER?
IS A GIVEN
- HOLDER PROTECTED FROM REGISTRY OWNER? (GOV)
· GOV CANNOT TRACE HOLDER
DURATION
- LAW:
- TECH:
VALID
PICTURE,
BIOMETRICS
RE-USE
FOR NEW
↳ EACH
VERIFY
LEGAL


TRUST
GISTRY ?
. GOAL: MUTUAL RECOGN.
Y ONCE
STANDS
SWISS STANDARD PROTOCOLL ?
- OWN SPECIFICATION AT START
↳ PRAGMATIC
- LONG-TERM: INTEROPERABILITY
COLLABOR. REACHED
TRUST
G. → TECHNICAL TRUST
EG. → ADD ON
IED → LEGAL TRUST
DURATION e-ID ?
- LAW: as long as paper document (root)
- TECH: COULD BE SHORTER VALID
PICTURE, SOURCE ?
BIOMETRICS & CODE ?
RE-USE PICTURE FROM e-ID FOR NEW VC ?
↳ EACH ENTITY HAS TO VERIFY WHAT THEY CAN LEGALLY DO
- HOLDER BINDING = PROOF OF POSSESSION PERFORMED
(HALLENGE NEED OF PIC
- LINKED CREDENTIALS ↓ CRYPTO INTERLINKED
COMBINED PROOFS ↑

Dancing and Fitting in with Ecosystems (First Person Credentials)

Session Convener: Darrell O'Donnell
Session Notes Taker: Ankur Banerjee

What Ecosystem(s) were present in the room/session?

Ayra (previously known as Global Acceptance Network or GAN)

What Ecosystem challenges did the conversation focus on, address?

Creating the first decentralized proof-of-personhood credentials (First Person Credentials) as described in this white paper from the Ayra Association. Also, doing something equivalent to offering a business card to someone and them immediately knowing what to do.

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

- The discussion first covered the Ayra Trust Network, then First Person Credentials
- Ayra Human Trust Fabric
    - Partnering with Customer Commons
    - PoC app (alpha/beta) would be available by IIW
- Discussion about WorldCoin (now World) as the most popular example

The Special Network Effects of Ayra Network Credentials whitepaper

Technical Focus Topics & Missing Building Blocks

Session Convener: Anja, Christian, Paul
Session Notes Taker: Christian

What Ecosystem(s) were present in the room/session?

What Ecosystem challenges did the conversation focus on, address?

Missing technical bits that need to get solved or more people should understand

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

Two major technical discussion points:

- DC API and what the issues are it fixes
- ZKPs - current state of the art and how do we get towards a usable standard

Slides on OpenID4VC & DC API:
https://docs.google.com/presentation/d/1gT3oN2emtwpKrEn4qlMyo5iRhJMNddjCn1x7vXAQqG8/edit?usp=sharing

Links to DC API:
https://wicg.github.io/digital-credentials/
https://github.com/WICG/digital-credentials
Relying Party: https://digital-credentials.dev/
Wallet: https://github.com/leecam/CMWallet/tree/main

Slides on ZKP:
https://hpi.de/oldsite/fileadmin/user_upload/fachgebiete/lehmann/EUDI_anoncreds.pdf

Dynamic Data Economy

Session Convener: Human Colossus Foundation
Session Notes Taker:

What Ecosystem(s) were present in the room/session?

What Ecosystem challenges did the conversation focus on, address?

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

NO NOTES SUBMITTED

SESSION #3

History of ID Tech (pre industrial)

Session Convener: T Serlet
Session Notes Taker:

What Ecosystem(s) were present in the room/session?

What Ecosystem challenges did the conversation focus on, address?

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

NO NOTES SUBMITTED

Paving the way from PDF to VC

Session Convener: Patrick, Christian, Fabian
Session Notes Taker:

What Ecosystem(s) were present in the room/session?

QTSP (skribble, Swisssign), Swiss E-ID, Wallet providers

What Ecosystem challenges did the conversation focus on, address?

Type Here

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

NO NOTES SUBMITTED

How to use CH E-ID as EU - PID (Brainstorming session How to: without waiting - bilateral CH-EI agreement

Session Convener: Ro…Z
Session Notes Taker:

What Ecosystem(s) were present in the room/session?

EU<—>CH

What Ecosystem challenges did the conversation focus on, address?

Let make Swiss E-ID acceptable in EU and other way around

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

eIDAS and the EUDI Wallet Ecosystem are based on this trust model:

Digital Health, based on trust infrastructure

Session Convener: Peter Janes, Oliver Deak
Session Notes Taker: Peter Janes, Oliver Deak
(optional) List of Session Attendees:
Marcel Eichmüller
Michal Jarmolkowicz
Zoe Blanchard
Sandra Jordi

What Ecosystem(s) were present in the room/session?

- Digital Health
- How to get adoption?
- Focus is on structured clinical data

What Ecosystem challenges did the conversation focus on, address?

- Specialized field, which is quite different from engineering disciplines > solutions must be developed in close cooperation with clinicians
- Very fragmented field > challenging to find right cooperation partners

- Often poorly set incentives (organically grown over time) > leads to lack of adoption and partially misuse of the system
- High number of interest groups with their own agenda and lobbyists
- Currently no plan for tangible results visible from Federal Office of Public Health (FOPH) and Digisanté initiative

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

«Crash course» for newcomers

- Current situation with national EPR > 700 M CHF cost, PDF based, 0.8% adoption (ca. 80'000 dossiers)
- Swiss Personalized Health Network (sphn)
- Focus on structured clinical data
- Standards IHE v1/v3, FHIR, openEHR
- Important functionalities > medication plan, vaccination, international patient summary (IPS)
- Situation in Austria (ElGA) > opt-out, 97% adoption; Germany (EPA) > opt-in, poot adoption

Swiss Digital Health Manifesto

- Driven by lack of digital transformation of healthcare system
- Aiming for «quick wins» > waiting is not an option
- Created from discussions about way forward
- 3 parts
    - Manifesto - principles
    - Action Plan - annual focus topics
    - Use cases
- Review and vote for version 1.0 scheduled for 14.03.2025

Prototypes

- 2022 - Health app with medication plan, vaccination, IPS, simulated EPR integration
- 2024 - Award-winning GovTech Hackathon prototype based on verifiable credentials to demonstrate citizen / physician interaction
- 2024 / 2025 - Hackathon follow-up project aiming for Swiss Public Beta
    - Improved architecture
    - Adopting for long transition phase
    - Several pivots based on learnings
    - Finding best granularity of verifiable credentials

Next Steps

- «Swiss Digital Health Manifesto» to drive tangible results
- Health app prototype based on Swiss Public Beta platform to demonstrate to outside users

Additional Material

- Health app prototype - https://youtu.be/T5bYmy_oXMo

- Working Group Health: DIDAS Statement on the Consultation EPDG - https://www.didas.swiss/de/2023/11/13/didas-stellungnahme-zur-epdg-revision/
- GovTech Hackathon 2024, Digital Health with the new E-ID trust infrastructure - https://hack.opendata.ch/project/1103
- Follow-up Project «Health SSI» - https://github.com/Abdagon/health-ssi-2
- Follow-up Project «Health SSI», prototype Webinar - https://youtu.be/D69uVIVHmsw (short teaser video, full webinar linked in show notes)
- Future of Healthcare Data - https://www.linkedin.com/pulse/future-healthcare-data-peter-janes-xlgmf/

eInvoicing & Blue Pages -> organization discovery

Session Convener: E (?) Hans (?) Al..? Names illegible
Session Notes Taker:

What Ecosystem(s) were present in the room/session?

What Ecosystem challenges did the conversation focus on, address?

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

NO NOTES SUBMITTED

What's missing in the EUDI wallet trust model and why won't EUDI wallets work outside Europe?

Session Convener: Samuel Rinnetmäki / Findynet
Session Notes Taker: Samuel Rinnetmäki / Findynet

What Ecosystem(s) were present in the room/session?

Type Here

What Ecosystem challenges did the conversation focus on, address?

- Trust model
- International interoperability

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

Samuel's presentation: https://docs.google.com/presentation/d/1WGjOj7i0vsDYy-0uP7Hpr1qLqeFgCtapxTZPWP2B4Co/edit?usp=sharing

The registration of relying parties improves accountability – they can be investigated and prosecuted in case of over-asking or misusing information. On the other hand, issuing registration certificates to relying parties may lead to a false sense of security and people thinking that a registration credential is a sign that the relying party is *entitled* to the information they ask.

The EU "trust framework" doesn't include a notion of a sector a wallet-relying party (including issuers) operates on.

Some participants felt that the responsibility to choose who to share information with should rely solely on the credential holder. There was a rough agreement that it might be a good thing that a wallet can show warnings in certain situations. Some technical infrastructure (like OpenID Federation) would be needed for the wallet to know when to show those warnings.

The EUDI wallets won't work outside Europe for the reasons stated in the presentation. (A certified wallet is not allowed to request credentials from a non-EU issuer and perhaps not allowed to present to non-EU relying parties.) Fortunately, we can use different wallets for different purposes.

DID Methods Standardization + did:scid Method (Solving cross-ecosystem portability)

Session Convener: Markus Sabadello, Drummond Reed, Ankur Banerjee
Session Notes Taker: Ankur Banerjee

What Ecosystem(s) were present in the room/session?

DIF, Trust over IP (part of Linux Foundation Digital Trust), GLEIF

What Ecosystem challenges did the conversation focus on, address?

- DID Core specification is standardised at W3C, but individual DID methods are not
- did:scid is a new draft that is trying to solve problems with portability

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

- W3C DID method working group is working on v1.0 to v1.1 to DID Core
  - No breaking changes
  - Some maintenance work, some editorial differences
  - CID was created to generalise the structure without DID identifiers
  - Other change is about the IANA media type of DID Documents. Instead of `application/did+json`, there will be `application/did`.
- DID Resolution is now on standards track
  - Specification now makes a difference between how DID resolution works, which fetches a DID Document back, vs DID URLs
- Joint DIF + W3C + INATBA + ToIP working group

  Part 2 was about the `did:scid` specification
  - What was the rationale
    - Came from Bluesky requirements
    - Portability and location independence
    - Can work with all DID methods based on self-certifying identifiers (SCIDs)
      - did:webs
      - did:webvh
      - did:jlinc
  - Status: currently a task force of the Trust Over IP (ToIP) Technology Stack Working Group

Cultivating ecosystems in the real world: California mDLs and IATA Aviation Security Trust Framework

Session Convener: Lucy Yang
Session Notes Taker:

What Ecosystem(s) were present in the room/session?

What Ecosystem challenges did the conversation focus on, address?

Strategy stakeholder communications and meaningful stakeholder engagement
Go-to-market and growth of identity ecosystems

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

Kaliya and Lucy began working together at the beginning of

Our work focuses on cross organization work.
IATA industry association of over 300+ airline members
mDL California Enterprise client

Sharing our experiences getting ecosystems to market.
Last session I was in Swiss eID
Lots of opportunities for mutual learning between different projects.

Our Client is DMV of California
We advise digital transformation officer.
Has gone beyond just mobile drivers licence.

We are a two person consultancy - we work globally.
How do we create impact - we work with great people and work with impactful clients.

Learnings from the CA mDL Community Hackathons

Stakeholder engagement - design and execute with them.

The only State in the U.S. that is implementing both ISO mDL and W3C Verifiable Credential standards. Stakeholders helping them understand the technology landscape.

Official launch into public August 2023 - mDL pilot launched.
It is called a pilot - upper limit of 1.5 million California's.

California DMV - Wallet first milestone
Second milestone launched in Apple Wallet and Google Wallet

DMV offers support with tooling to accept CA mDLs.
This was an opportunity to work with the state.
They worked with any sized company working on real world use-case.

Other Public Agencies in California helped them see the possibilities - and build a case with their own agency. Connecting with other States who are doing similar work.

Peak momentum and keep going.

More about the hackathons at https://www.dmv.ca.gov/portal/file/california-dmv-mdl-hackathon-briefing-and-roadmap/

Future DMV use cases

- Vehicle Registration
- Disability Placard and Smart Parking
- Interim Drivers Licence / Temporary

Learnings:

- Resources constraints and incentives (make strong case)
- Tech and standard readiness (range of readiness - some we helped more then others)
- Community and collaboration

The team still has access to the test app and test credentials.

Got a sense of where actual real world challenges with implementation with different standards.
We got some of the pioneers - they have challenges - for the broader ecosystem of relying parties there are challenges.

Relying parties were able to ask for features in the future.

Community organizations helped spread the word.

IATA Aviation Security Trust Framework
https://www.iata.org/en/pressroom/2025-releases/2025-03-19-01/

Credentials for the airlines.
Government agencies - Nation States
Airlines

Wide range of aviation matters.

The right person with the right qualifications is doing the right thing at the right time.
The process has been quite manual.

ICAO provides high level guidance

Airlines and other stakeholders have to develop their own documents to become compliant.

Conceptual Level
Needs being expressed to us.

Relatively simpler and easy to get started.
How to get a Verifiable Credential Ecosystem started within an existing ecosystem.

Client came up with their ecosystem use-case
They wanted help to build the case for their ecosystem.

Hearing needs from their stakeholders - someone has to “say it louder” to make it official.

Walked through the table of contents of the IATA

Demonstrate how it could work.

Session Notes Day 2 / Sessions 4 - 6

SESSION #4

How to map a national digital identity ecosystem: what we tried.

Session Convener: Graham Francis
Session Notes Taker: Stefan Koller, Swisscom
(optional) List of Session Attendees:

PXL, SICPA, Meeco, Digital Catapult, Spherion, Nimbus, CH Government / e-ID, Hashgraf Association, Radium

What Ecosystem(s) were present in the room/session?

National ecosystems - focussed on the UK approach, but translatable to others

What Ecosystem challenges did the conversation focus on, address?

How to measure a national ecosystem & track trends within it (growth, adoption).

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

We discussed the background to the UK Digital Identity Sector Analysis, and key insights that emerged - see report here:

https://www.gov.uk/government/publications/digital-identity-sectoral-analysis-interim-findings

And blog post here https://enablingdigitalidentity.blog.gov.uk/2024/12/21/understanding-the-digital-identity-market-key-insights/

Aims of Session:

Share approach to tracking growth and development trends in the UK digital identity sector, discuss things we found tricky and explore if these translate to other markets.

Two bits of UK Office for Digital identities. 1) building bit for eGov use cases and gov wallet 2) team to grow and scale beyond gov use cases.

4 Main pillars: Consistent Standards, Assurance that standards are followed, check that standards are followed, Growing the Market by opening up gov data to private sector

Aim of the program: track growth and development trends in UK digital identity sector. Followed a quantitative and qualitative research focus to gain insight into how digital identity projects are perceived in private sector.

Three core areas of tracking (search focus)

1) Digital identity / digital verification provider market
2) Attitudes to digital identities and adoption of digital identities
3) To what extent enables digital identities inclusion

Provider Market Learnings

Definition of the Market, Market Sizing, Key Players, understanding market dynamics (barriers to entry and growth), levels of adoption across primary use cases, establishing digital identity trust framework.

Established a full digital identity taxonomy (see screenshot or report)

Then sized market, classified services and identified sectors and use cases. Leading use cases are onboarding, fraud prevention, KYC / AML, background screening.

Full report should be available in Mai / June 2025 including additional topics such as barriers and opportunities for innovation and growth, competitive analysis across different product types (wallets, age assurance, document verification, …), supply chain analysis (understand sourced components, depth of supply chain), innovation eco-system analysis (academia, investors, universities, …)

Learnings from first failed iteration of digital identity in UK:

- Voice of the industry: Government shall do what only government can do (trust framework and trust marks establishment and setting it into law)

Current research is focused on attitudes towards and public adoption of digital identities (Pt 2 of the research). Will be part of the full report.

- This research is much more complex to conduct. Big public survey (3400 approx.), relying party / stakeholder 1:1 interviews and digital identity provider survey.
- Approach focused on understanding attitudes towards specific use cases: opening a bank online, apply for a job trough online recruiting agency, age-verified purchasing a lottery scratch card, verify identity while renting property.
    - Much more people used digital identification services than initially assumed
    - Security / Privacy was not an overwhelming issue for most people
    - Digital verification makes things quicker and easier
    - Re-useable identity is not “the only game in town”. Wallets are helpful, but not the only solution for digital identity verification.

Questions:

How far will this be applicable globaly?

- Probably pretty good. Approx 10% is specific to UK frameworks, rest of it is pretty much universal.
- Methodology can be shared for additional, national or international research

Will the model be expanded to research beyond digital identity?

- Net economic benefits of over 4tn pounds over 10 years

What are the specific plans on UK digital identity on a government level?

- Role of digital identity office is to write the rules, how a good digital identity looks like.
- A team in the department works on the UK wallet for the mobile driver license. There will be a UK wallet (announced, currently being built by an external company).
- Both, private and public products must follow the guidelines and standards set by the digital identity office.

SSI + AI agents with Sovereign Knowledge Graph

Session Convener: Volodymyr Pavlyshyn
Session Notes Taker:

What Ecosystem(s) were present in the room/session?

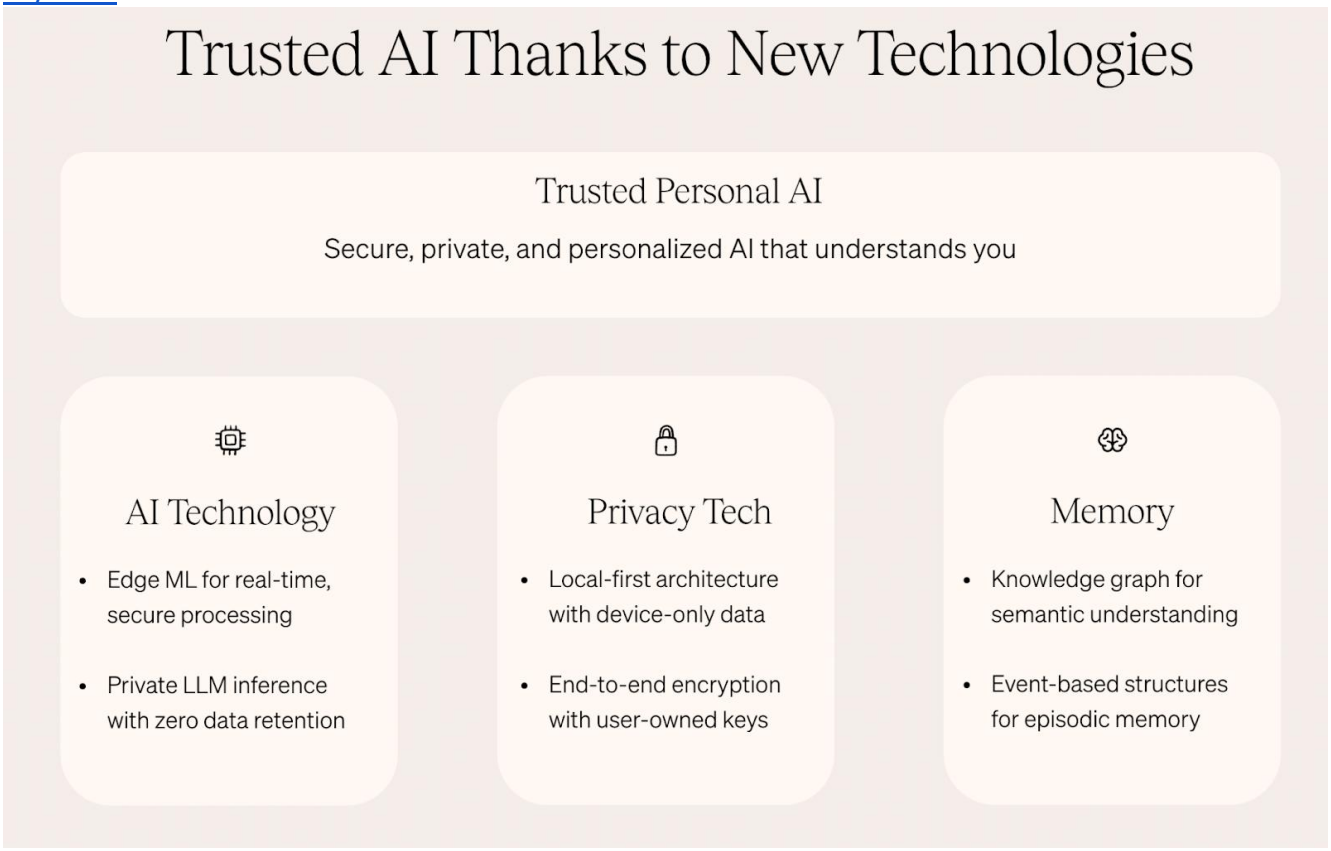
Local first , edge ML and decentralized AI

What Ecosystem challenges did the conversation focus on, address?

- store and process non-credential data
- store and share the knowledge graph and the semantic rich data in a sovereign way
- access to GPU and specific compute

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

MyKin.ai



Corner Architecture Stones

- Local First AI event coming up Local-First Conf. Local first bring Data Ownership with compute closer to user more to read Benefits of LocalFirst for the Good of All | by Volodymyr Pavlyshyn | Feb, 2025

Self Sovereign Identity - we focus not on VC but more on ownership and principles.

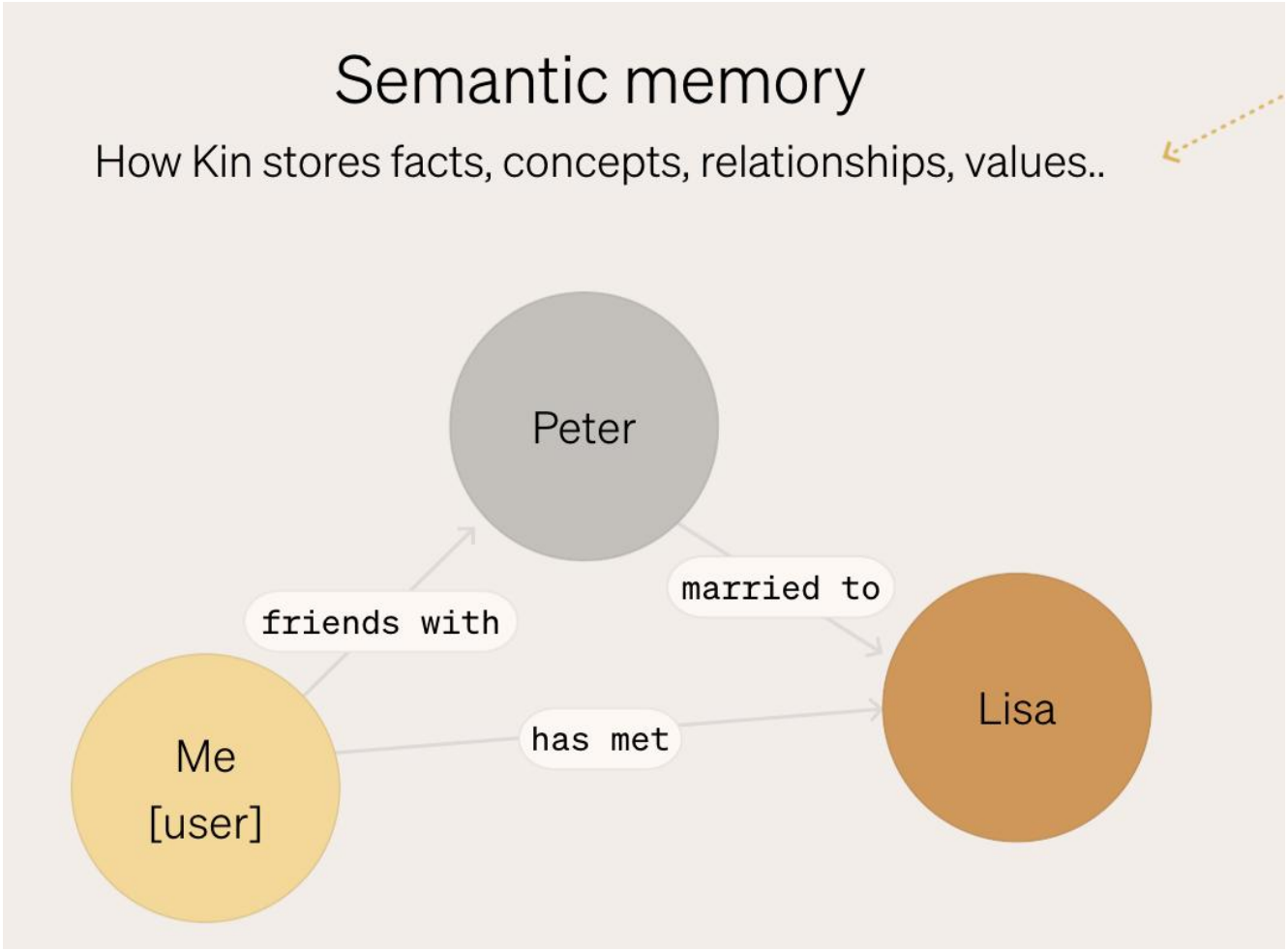
Privacy by Design [Privacy-First AI Agents for Ethical AI | by Volodymyr Pavlyshyn | Jan, 2025 | Artificial Intelligence in Plain English]

Models run on local device.
Device - challenge battery
Challenge speed of inference.

SLM - SMALL language models and specialized
Agentic Framework.

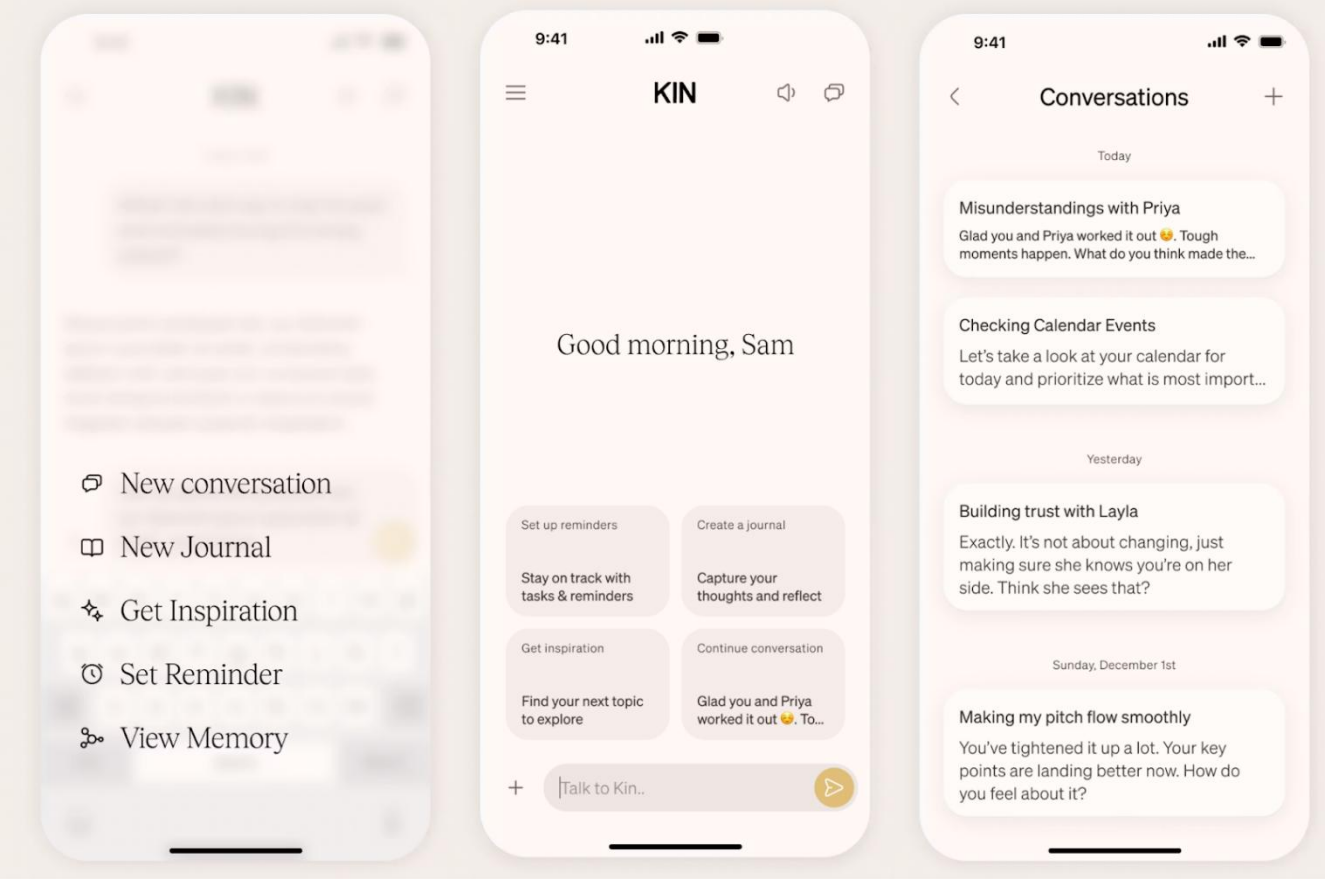
Notes in Obsidian
Conversations start semantic mapping
All your data you talk do Kin

Semantically rich data in knowledge graph.



Semantic Graph
event-based concept graph
(close to how brain works)

Condensed form of linked data of semantic data - all running local



Smart Reminders
Ask Kin to do things with it.

Hands free voice mode - starting.

We use Whisper

Always opt out of things

eGov use-cases

Session Convener: Hans, Vitor, Daniel
Session Notes Taker: Hans, Vitor
(optional) List of Session Attendees: Sandro Scalco

What Ecosystem(s) were present in the room/session?

- Swiss E-ID

What Ecosystem challenges did the conversation focus on, address?

- How to get a broad adoption of Swiss E-ID and other governmental backed attestations

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

1. Overall E-Government (E-GOV) Adoption

- Need to create awareness about the necessary steps for implementation.
- Timeline for E-ID introduction remains uncertain.
    - Uncertainty due to the possible referendum on E-ID.
- Swiss Confederation is forming a group to enhance E-GOV adoption.
- It should be clear, what the Federal government makes available, and what is left open to cantons, municipalities and private service providers/products
- ux centered design of the use-case is needed

2. Current Challenges in Municipal Processes

- Two companies manage the current processes (own the software) used across various municipalities (Innosolv and another company (?)).
- Predominantly rely on outdated PDF-based solutions.
- Lack of clarity on the transition to Verifiable Credentials (VCs).
- Legacy software in municipalities is a significant barrier to VC and E-ID adoption.
- Municipalities need to drive the pressure for modernization.

3. Issues with E-ID Implementation

- AGOV's E-ID usage may create a misleading impression of full digitalization.
    - It primarily addresses verification / login (and registration).
    - Does not fully support digital transactions, such as obtaining a residence declaration as a VC.

4. Improving User Experience and Adoption

- Customer journey should be seamless and user-friendly.

    - Avoid technical jargon like “login” and instead use intuitive terms like “show your ID”
- Need for standardization of VCs for official documents (e.g., Residence Declaration).
    - DVS standardization group working on this
- Extending the validity of certain VCs could:
    - Reduce costs for citizens.
    - Extend usability beyond physical document expiration.
    - Shift costs from human resources to operating IT systems.
    - Blueprints should be developed to facilitate legacy system integration.
- Centralized data storage could simplify processes, but ownership and governance remain key questions for Switzerland.

5. End-to-End Use Cases and Adoption Strategies

- Identifying who will use VCs in practice is essential.
    - Lack of end-to-end use cases, particularly for documents like debt register extracts.
    - Many institutions require PDFs as today (e.g., home rental platforms like Homegate).
- Converting VCs into PDFs could aid adoption.
- Strategies to foster user adoption:
    - Ensure ease of use.
    - Address user preference for digital over paper formats.
- Consider price incentives to promote VCs over physical documents.
    - Problem with discrimination for people with less digital skills.
    - Paper format will remain available due to legal requirements.
- official attestations (such as residency certificates): it’s key that they can be reused as long as they are in the wallet, but should be revoked if not anymore valid (would be a real benefit from the VC based approached in comparison to the paper / PDF based variants)
- Transition Phase:
    - VC → PDF, or other approaches to bridge the gap with verifiers not yet ready
    - (federal) generic verifier app which allows anybody to check / verify a VC (Federal government will issue one for E-ID)
- In the Swiss systems, the bigger players (federal government, cantons) should be first adopters and accepts VCs in their eGov use-cases, municipalities can follow later
-

6. Increasing Regular Use of E-ID and VCs

- What is needed to ensure E-ID and VCs are used regularly, not just a few days per year?
    - Swiss Case: A Check App for verifying 16+ and 18+ age requirements will be available.
    - Users should be able to use the app/E-ID without manually entering their entire data set or personal information.

How to Mitigate: UX,Compliance, Tech, Certificates, - Role of Trust Service Providers - Simplify adoption platforms (29+ EU SWISS UKRAIN etc.)

Session Convener: Roger Oliviera (Ver.id)
Session Notes Taker: Raquel de Horna (Giesecke+Devrient)
(optional) List of Session Attendees:
Micha Kraus (Bundesdruckerei), Elmar Reif (PXL Vision), Miriam XXX (Procivis), I need support here, I didn't write everybody's names

What Ecosystem(s) were present in the room/session?

Roger presented the Netherlands digital identity ecosystem. He introduced us to the different "wallets" and digital eIDs that people in the Netherlands are exposed to including:

- a pre-PID wallet where different types of documents can be stored like: basic id and assertions of being over a certain age, proof of address and proof of business registration.
- The government federated identity access available to all citizens so that they can authenticate in different government sites and applications
- the new EUDIW
- Digital banking wallets that provide different kinds of financial attestations.

An example was shown: a website from the city of Nijmegen where three different login buttons appeared for signing up and authenticating.

What Ecosystem challenges did the conversation focus on, address?

The conversation focused on the challenge of having a very diverse landscape of available wallets and 27 different jurisdictions that have the right to define their own trusted SPs lists. This has a special impact in multinationals that are operating in multiple member states and that will be accepting credentials from multiple wallets. Service providers will have to register themselves in some trusted SP list and it is unclear if there will be a central directory.

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

There was an intense debate around interoperability vs the real world where each member state might do things in a different way.
Some participants think that there is going to be a unique SPs trust list and that if there are local lists, there will be off-the-box interoperability anyways.

Other participants agree with the Ver.ID vision that international cases might not work from the beginning and a trust service provider will be necessary as a layer in between to support SP adoption and facilitate verification of multiple wallets and IDPs.

Micha shared with us that there is a discussion open in the German EUDIW around maybe creating templates for asking for certain attributes depending on the use case. E.g. KYC would mean: "first name", "Last name", "date of birth", etc. This could facilitate the registration of SPs and their approval.
There was also a discussion around the regulators, where differences might happen also on a regional basis. Need for more input from the other participants

Hardening did:scid, did:webs, and others…(whiteboarding session)

Session Convener: Ankur Banerjee, Drummond Reed, Markus Sabadello
Session Notes Taker: Ankur Banerjee

What Ecosystem(s) were present in the room/session?

did:webvh contributors, did:webs contributors

What Ecosystem challenges did the conversation focus on, address?

Creating a stable/portable DID that could was location independent

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

- `did:scid` draft specification
- Issue raised by Ankur
    - In did:webvh, the process of log creation is not per se tied to a file being actually present at a domain, it's just the text + the keys associated (see example)
    - So creating an entirely fabricated history and publishing it on a different domain is possible.
    - Discussion centred around whether this is a problem
- Proposed changes to `did:scid`
- We reached an understanding in this session that we were talking about different types of portability and the portability of different things
- We also reached clarity about some aspects of the resolution architecture for did:scid DIDs by relying on the resolution code for the underlying SCID formats (e.g., did:webvh, did:webs, did:jlinc, etc.)

About FIDES

Session Convener:
Harmen van der Kooij, harmen@fides.community (FIDES)
Eelco Klaver, eelco.klaver@credenco.com (Credenco)
Hans Boone, hans.boone@unifiedpost.com (Unified Post)

Session Notes Taker: Harmen
(optional) List of Session Attendees:
Isaac Hendersen
Darell O'Donell
Esther Makaay
Kaliya Young

What Ecosystem(s) were present in the room/session?

FIDES, Company Passport, Ayra, TOIP, Gaia-X, EWC LSP, IIW

What Ecosystem challenges did the conversation focus on, address?

The conversation focussed on explaining what the FIDES Community is and demonstrating the FIDES Open Sandbox. In addition, a demonstration of a recent (not yet finalized) FIDES Labs experiment about eInvoicing in combination with wallets and credentials. It uses the concept of a federated organization directory, Blue Pages (crawling DID documents from organizations). More info below.

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

FIDES is a new international ecosystem, started july 2024. It is an international public private ecosystem aiming at improving global digital trust and interoperability. Initially focussing on tangible examples of interoperable solutions that use digital wallets & credentials.

Currently the FIDES initiators (Victor van der Hulst and Harmen van der Kooij) are exploring how to more closely collaborate with like minded, global initiatives like OWF and Ayra. In order to join forces and avoid too much fragmentation.

https://fides.community/

FIDES Manifesto
The FIDES Community principles are outlined in the FIDES Manifesto that has been ratified by 55 organizations : https://fides.community/manifesto
FIDES is an international trust ecosystem focussing on collaboration using DIIP - Decentralized Identity Interop Profiles, interop labs and plugfests. Roots in NL ecosystem but changed focus internationally.

FIDES Open Sandbox

The FIDES Open Sandbox provides a comprehensive, neutral showcase of interoperable digital wallet and credential solutions from around the world. The sand box solutions are a combination of credential issuers, relying party websites and compliant personal and organizational wallets. The Open Sandbox only provides pointers/links. So the actual issuers, relying parties and wallets are managed and hosted by others. The FIDES Open Sandbox aims to provide an overview of any interoperable solution. This can include different types of credential formats (SD-JWT VC, mDL, VCDM 11, 2.0 etc) and/or transport mechanisms (OID4VC, DID Comm etc). This allows the community to compare solutions based on different specifications.

- **Use Case Catalog**: Step-by-step walk-throughs demonstrating how solutions work in practice, compliant wallets, credential types, and precise interoperability specifications. Any existing use case https://fides.community/fides-open-sandbox
- **Credential Catalog:** Overview of publicly available credential issuers that issue digital credentials can be re-used for various use cases. Filtering options allow searching for particular credential formats, schemas or languages. https://credential-catalog.fides.community/
- **Pers wallet catalog:** Neutral overview of wallets for natural persons across the world. Plans for integration with OWF wallet overview so it can be filtered by meta data like supported specifications, interop profiles, languages, certifications etc https://fides.community/personal-wallets
- **Org wallet catalog:** Tools for businesses or any type of organization. Neutral overview of wallets for organizations (incl. functionality to issue and verify digital credentials). Plans for integration with OWF wallet overview so it can be filtered by meta data like supported specifications, interop profiles, languages, certifications etc https://fides.community/organizational-wallets
- **Open Test Bed:** Overview of publicly available conformance test scripts and testbeds. All related to wallets and credentials and underlying specifications. For instance:

  OpenID Certification & Conformance Tests
  Aries/OWL Agent Test Harness (BCGov)
  EU Interoperabilty Test Bed (incl EWC and FIDES Testbed)
  “Can I Credential” Test Suite - CanIVC.com (Digital Bazar)
- **Blue Pages (under construction):** organizational directory allowing web and API search based on verified or self issued information that an organization decides to publish in it’s public profile. A “decentralized Google Business Profile”. Organizations can maintain this profile from an organizational wallet. More info on this below in the section about the eInvoicing lab experiment. https://fides-bluepages.acc.credenco.com/
- **Universal Access**: Available to organizations, Legal Service Providers, plugfests, hackathons, domain-specific initiatives, and national programs to publish their credential ecosystem components—issuers, relying parties, and wallets.

FIDES Labs eInvoice part1&2 - Peer Discovery - Blue Pages

FIDES Labs operates both the FIDES Open Sandbox and coordinates specialized lab experiments focused on digital wallet and credential technology. Among these initiatives is the Dutch Small Scale Pilot for eInvoicing, a collaborative effort involving key Dutch institutions.

eInvoice Context and Participants

- **Key Participants:**
  - Credenco and Sphereon (Technology partners)
  - Belastingdienst (Dutch Tax Office)
  - Kamer van Koophandel (Dutch business registry)
  - Unifiedpost (Business platform provider)
  - FIDES Labs (Ecosystem coordinator)

Trust Infrastructure Components - (eInvoice part 1)

In eInvoice part 1, we have implemented a comprehensive trust infrastructure featuring:

- Organizational wallets with DID documents
- DIIP v3 interoperability profile
- OID4VC/OIDVP protocols
- Credential verification mechanisms
- Service endpoint definitions
- Linked verifiable presentations
- Essential credentials (VAT number, LPID, Legal Representative)

eInvoice part 2: DID Document Discovery System

The core innovation of the FIDES eInvloice part 2 is the Blue Pages system, addressing critical eInvoice challenges:

- Ghost and bankrupt companies
- Fake invoices
- Interoperability barriers

See annex - use case discovery - delivery for a more detailed description of the functionality provided by FIDES blue pages

Blue Pages Functionality

1. **Registration and Indexing:**
   - Multiple DID registration methods (web-crawler, EBSI subscriptions, self-registration)
   - Comprehensive identifier indexing (company names, registry numbers, VAT numbers)

    - Quality control mechanisms for trusted credentials
2. **Search and Verification:**
    - Advanced search API with federated search capabilities
    - Google-like user interface experience
    - Complete credential validation (DID resolution, verification of presentations, trusted issuers, cryptographic proof validation)
3. **Real-World Example:**
    - When a business places an order, their Chamber of Commerce number can be used to locate their DID document
    - Credentials are verified through linked verifiable presentations
    - Service endpoints in the DID document enable direct, secure document exchange

Current Status and Future Development

- The Blue Pages prototype is available at: https://fides-bluepages.acc.credenco.com/
- Open source repository: https://github.com/FIDEScommunity/fides-bluepages
- Ongoing work includes publishing the proposed service endpoint format as an RFC and finalizing the eInvoice credential scheme with UBL mapping

The FIDES Blue Pages represents a significant advancement in enabling trusted business interactions through a federated search catalog that makes verifiable company information accessible through familiar directory-style search functionality.

DIIP - Decentralized Identity Interop Profile -
Several of the FIDES Community members participate in the DIIP (Decentralized Identity Interop Profile). However, examples in the FIDES Sandbox don't need to be exclusively using the specs from DIIP.
https://github.com/FIDEScommunity/DIIP/discussions/15#discussioncomment-9216261

OID4VP API
In order to more easily create interoperable Relying Party solutions based on OID4VP a number of organizational wallet providers within the FIDES Community have come up with a suggestion of the "OID4VP API". See https://fides.community/oid4vp-api

Next steps:
- Esther Makaay and Harmen will discuss possibilities for publishing the EWC LSP use cases in the FIDES Open Sandbox.
- Isaac and Harmen will discuss the possibilities for publishing the WHO and/or Gaia-X use cases in the FIDES Open Sandbox.
- Isaac and Eelco will discuss standardisation possibilities and connecting Credenco Wallet to TRAIN.
- Ayra is interested to further discuss the architecture and use of the FIDES Blue Pages experiment.

Annex: Use case delivery of eInvoice using blue-pages

This annex describes a real-world use case for the Blue Pages application, demonstrating how decentralized identifiers (DIDs) and verifiable credentials can streamline and secure the business-to-business eInvoicing process. The scenario follows a transaction between two companies, from initial order placement to invoice acceptance, using decentralized identity verification at each step.

Scenario Description

In this scenario, a customer ("Pierre") from Fabaleus BV purchases custom-printed products from VistaPrint. The process illustrates how DIDs and the Blue Pages registry facilitate secure, efficient business transactions with automatic identity verification and electronic invoice handling.
In the descriptions below, each numbered item (e.g., **[1]**, **[2]**, **[3]**) refers to the corresponding interaction in the web sequence diagram at the end of this document.

A. Initial Order and Company Identification

1. **Customer Places Order**: Pierre visits VistaPrint's website and orders 20 custom-printed water bottles (doppers) with Fabaleus BV's logo.
2. **Business Identification**: During the checkout process, Pierre provides Fabaleus BV's Chamber of Commerce (CoC) number to identify the business entity that will receive the invoice.
3. **DID Resolution via Blue Pages**: VistaPrint uses the Blue Pages registry (FIDES) to search for Fabaleus BV's decentralized identifier (DID) using the provided CoC number.
    - Blue Pages searches its registry and selects the correct match using identifiers (trading name, RSIN, CoC number, etc.)
    - Blue Pages returns the DID identifier of Fabaleus BV to VistaPrint's ERP system

B. Customer Identity Verification

4. **Verification Request**: VistaPrint's ERP system asks its Organizational Wallet (OWA) to verify Fabaleus BV's identity data.
5. **DID Document Retrieval**: VistaPrint's Organizational Wallet resolves Fabaleus BV's DID document through EBSI (European Blockchain Service Infrastructure).
    - The DID document contains cryptographic proof of identity, service endpoints, and credential information
6. **Endpoint Resolution**: VistaPrint's wallet extracts the service endpoint information from Fabaleus BV's DID document.
7. **DID Control Verification**: VistaPrint's wallet communicates with Fabaleus BV's Organizational Wallet (OWB) to verify that it controls the claimed DID.
    - This prevents spoofing and ensures the DID is active and valid
8. **Credential Verification**: VistaPrint's wallet verifies Fabaleus BV's business credentials:
    - LPID (business registry credential)
    - VAT number credential
    - Additional linked verifiable presentations
9. **Trust Framework Verification**: The wallet verifies the linked trust credentials against established trust frameworks.

10. **Revocation Check**: The wallet checks that none of the credentials have been revoked.
11. **Connection Establishment**: VistaPrint's wallet creates a secure connection record with Fabaleus BV's wallet for future communications.
12. **Verification Completion**: The verified business data of Fabaleus BV is returned to VistaPrint's ERP system. Fabaleus BV is accepted as a customer
13. **Customer Creation**: VistaPrint's ERP system creates a customer record using the verified data of Fabaleus BV.

C. produce and deliver goods

out of scope

D. eInvoice Creation and Authorization

14. **Invoice Generation**: VistaPrint's ERP system generates an electronic invoice for the order.
15. **Document Sealing**: VistaPrint's ERP system requests its Organizational Wallet to seal the eInvoice using the company's X509 Qualified Electronic Seal (QSeal) certificate.
    - The sealed invoice contains cryptographic proof of its authenticity and integrity
    - The DID information may be included via one of several mechanisms:
        - Option 1: No DID information included (relies on Blue Pages lookup)
        - Option 2: DID document included in the Subject Alternative Name field of the X509 certificate
        - Option 3: DID document included as part of a UBL extension in the invoice

E. eInvoice Transmission

16. **Invoice Delivery**: VistaPrint's ERP system sends the signed eInvoice to Fabaleus BV's ERP system using one of the following methods:
    - Through the Peppol network using the endpoint specified in Fabaleus BV's DID document
    - Via direct HTTP POST to Fabaleus BV's service endpoint with appropriate authorization token
    - The selected method in this scenario is HTTP POST with access_token_party_A
17. **Authorization**: When using HTTP POST:
    - VistaPrint includes an access token (access_token_party_A) in the Authorization header
    - This token proves VistaPrint's identity and authorization to submit the invoice

F. eInvoice Verification and Acceptance

18. **Verification Request**: Fabaleus BV's ERP system forwards the eInvoice to its Organizational Wallet for verification.
19. **Sender Identity Resolution**: Fabaleus BV's wallet resolves VistaPrint's DID document from the access token issuer information.
    - If no DID information was included in the invoice, it may search Blue Pages to find the match

    - If DID was included in the certificate or UBL extension, it can directly resolve the document
    - If an access_token was send, it's possible to use DNS + /did/.well-known to resolve the DID document
20. **Credential Verification**: Fabaleus BV's wallet verifies VistaPrint's business credentials, including:
    - Business registry credentials
    - VAT number credentials
    - Additional linked verifiable presentations
21. **Trust Framework Verification**: The wallet verifies VistaPrint's linked trust credentials.
22. **Revocation Check**: The wallet checks that none of VistaPrint's credentials have been revoked.
23. **Connection Establishment**: Fabaleus BV's wallet creates a connection record for VistaPrint's wallet.
24. **Acknowledgment**: Fabaleus BV's wallet sends an acknowledgment (ACK) to VistaPrint.
25. **Semantic Verification**: Fabaleus BV's ERP system verifies the semantic content of the invoice.
26. **Signature Verification**: Fabaleus BV's wallet verifies the signature and integrity of the eInvoice.
27. **Receipt Timestamp**: Fabaleus BV's wallet timestamps the received eInvoice and provides this timestamp to the ERP system.
28. **Final Acknowledgment**: Fabaleus BV's ERP system sends a final receipt acknowledgment to VistaPrint's ERP system.
29. **Invoice Acceptance**: Fabaleus BV accepts the eInvoice, completing the transaction.

G. pay invoice out of scope

Benefits of This Approach

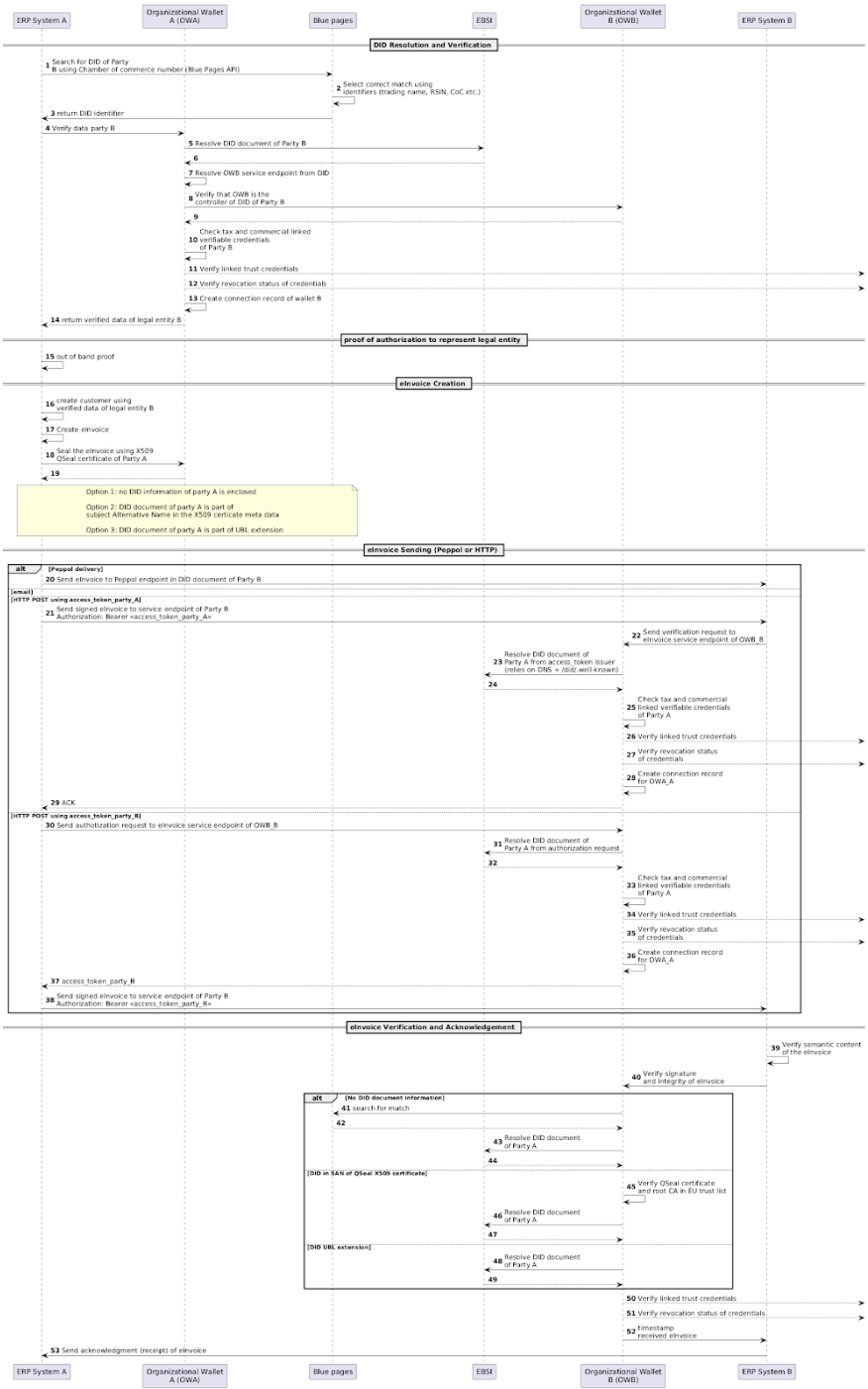
- **Automated Identity Verification**: Eliminates manual verification of business credentials.
- **Enhanced Security**: Cryptographic proofs ensure the authenticity of all parties and documents.
- **Streamlined Process**: Service endpoints in DID documents enable direct system-to-system communication.
- **Interoperability**: Works across different ERP systems and electronic invoice formats.
- **Regulatory Compliance**: Supports requirements for electronic invoicing and business identification.
- **Reduced Fraud**: Cryptographic verification prevents identity spoofing and document tampering.
- **Audit Trail**: All steps create verifiable records for future reference or audit purposes.

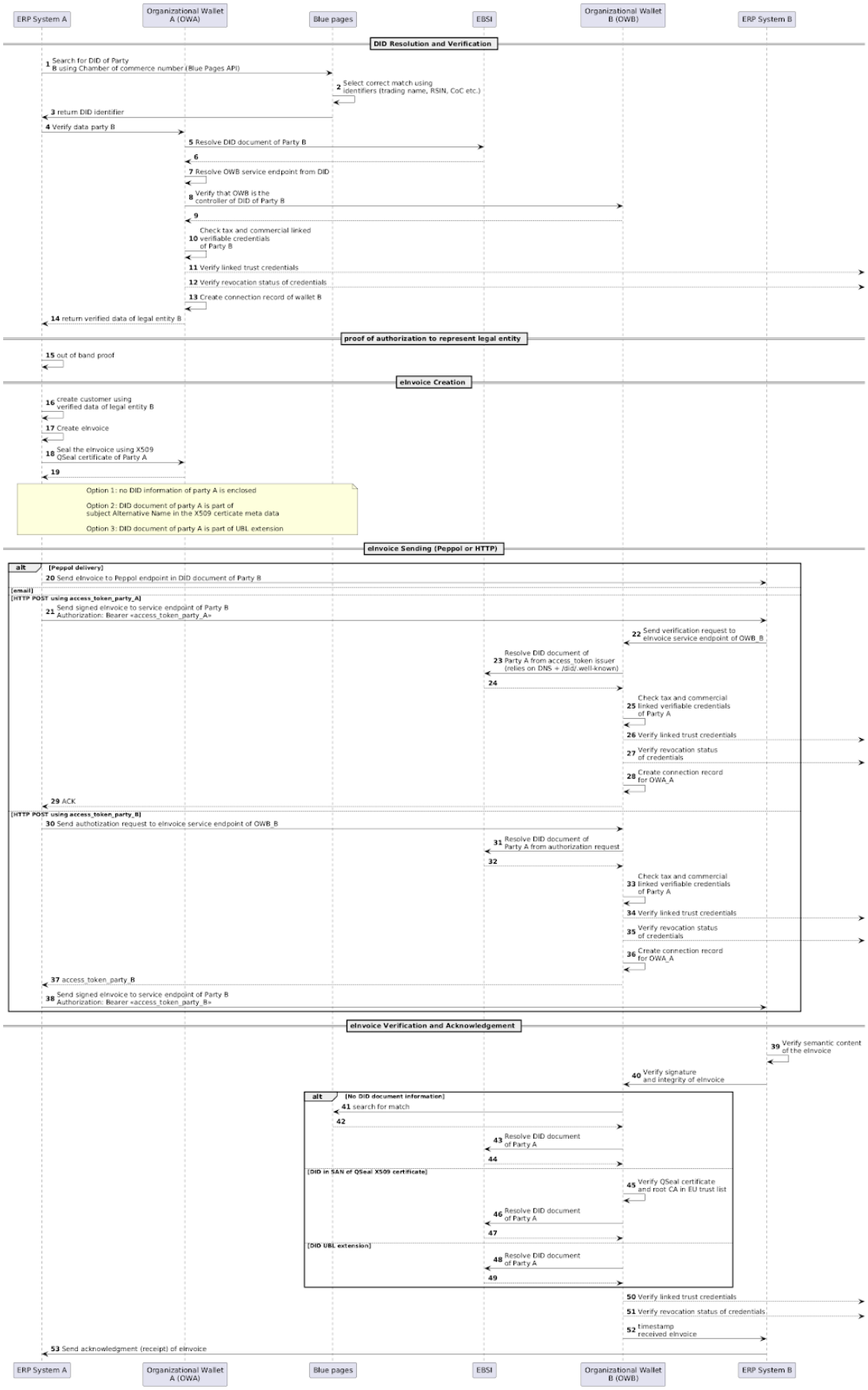
Technical Requirements

To implement this scenario, businesses need:

1. **ERP Integration**: ERP systems capable of resolving DIDs and processing eInvoices

2. **Organizational Wallet**: A DID-compatible wallet for managing business identities and credentials
3. **Blue Pages Registration**: Business identity registered in the Blue Pages (FIDES) registry
4. **DID Document**: Published DID document with appropriate service endpoints
5. **Verifiable Credentials**: Business credentials from authorized issuers
6. **X509 Certificate**: Qualified Electronic Seal certificate for document signing




ERP System A
Organizational Wallet A (OWA)
Blue pages
EBSI
Organizational Wallet B (OWB)
ERP System B
DID Resolution and Verification
1 Search for DID of Party B using Chamber of commerce number (Blue Pages API)
2 Select correct match using identifiers (trading name, RSIN, CoC etc.)
3 return DID identifier
4 Verify data party B
5 Resolve DID document of Party B
6
7 Resolve OWB service endpoint from DID
8 Verify that OWB is the controller of DID of Party B
9
10 Check tax and commercial linked verifiable credentials of Party B
11 Verify linked trust credentials
12 Verify revocation status of credentials
13 Create connection record of wallet B
14 return verified data of legal entity B
proof of authorization to represent legal entity
15 out of band proof
eInvoice Creation
16 create customer using verified data of legal entity B
17 Create eInvoice
18 Seal the eInvoice using X509 QSeal certificate of Party A
19
Option 1: no DID information of party A is enclosed
Option 2: DID document of party A is part of subject Alternative Name in the X509 certicate meta data
Option 3: DID document of party A is part of UBL extension
eInvoice Sending (Peppol or HTTP)
alt [Peppol delivery]
20 Send eInvoice to Peppol endpoint in DID document of Party B
[email]
[HTTP POST using access_token_party_A]
21 Send signed eInvoice to service endpoint of Party B Authorization: Bearer «access_token_party_A»
22 Send verification request to eInvoice service endpoint of OWB_B
23 Resolve DID document of Party A from access_token issuer (relies on DNS + /did/.well-known)
24
25 Check tax and commercial linked verifiable credentials of Party A
26 Verify linked trust credentials
27 Verify revocation status of credentials
28 Create connection record for OWA_A
29 ACK
[HTTP POST using access_token_party_B]
30 Send authotization request to eInvoice service endpoint of OWB_B
31 Resolve DID document of Party A from authorization request
32
33 Check tax and commercial linked verifiable credentials of Party A
34 Verify linked trust credentials
35 Verify revocation status of credentials
36 Create connection record for OWA_A
37 access_token_party_B
38 Send signed eInvoice to service endpoint of Party B Authorization: Bearer «access_token_party_B»
eInvoice Verification and Acknowledgement
39 Verify semantic content of the eInvoice
40 Verify signature and integrity of eInvoice
alt [No DID document information]
41 search for match
42
43 Resolve DID document of Party A
44
[DID in SAN of QSeal X509 certificate]
45 Verify QSeal certificate and root CA in EU trust list
46 Resolve DID document of Party A
47
[DID UBL extension]
48 Resolve DID document of Party A
49
50 Verify linked trust credentials
51 Verify revocation status of credentials
52 timestamp received eInvoice
53 Send acknowledgment (receipt) of eInvoice
ERP System A
Organizational Wallet A (OWA)
Blue pages
EBSI
Organizational Wallet B (OWB)
ERP System B

Privacy & ZKP use-cases & requirements discussion

Session Convener: Anja, Christian, Paul
Session Notes Taker:

What Ecosystem(s) were present in the room/session?

What Ecosystem challenges did the conversation focus on, address?

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

NO NOTES SUBMITTED

Driving Adoption by extending the bubble. FIND THE Target group via a survey in their language

Session Convener: Roman Z
Session Notes Taker:

What Ecosystem(s) were present in the room/session?

What Ecosystem challenges did the conversation focus on, address?

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 #5

State of the art on AI (e.g., "vibe coding", "boomer prompting") and how decentralized identity can build Verifiable AI

Session Convener: Ankur Banerjee
Session Notes Taker: Ankur Banerjee

What Ecosystem(s) were present in the room/session?

N/A

What Ecosystem challenges did the conversation focus on, address?

The AI community is grappling with identity for AI agent issues as they are acting on behalf of humans

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

- State of the art of AI
  - "Vibe coding"
  - https://fly.pieter.com/ - Multiplayer web-based game with real-time players made entirely using vibe coding with Grok 3
  - "Boomer prompting": Generally, being overly descriptive.
- Model Context Protocol: from Anthropic
- We spoke about liability when agents take action on behalf of users

Sharing Health Data for R&D (Secondary Use)

Session Convener: Dominik Geller
Session Notes Taker:
(optional) List of Session Attendees:
Axel Schild (Adnovum)
Peter Janes (Aragon)
Oliver Deak (<Startup>)
Raquel de Horna (Gieseke&Devrient)
Christian Heimann (Fedpol)
Marcel Eichenmüller (SwissSign)
Sean Natoewal (SwissSign)
Sandra Jordi (Bundesamt für Justiz)
..

What Ecosystem(s) were present in the room/session?

Digitising Health Data
Trust Providers
Implementers

What Ecosystem challenges did the conversation focus on, address?

- Delineation of the ecosystem, where do/should we draw the line?
- Obstacles and Drivers of adoption:
    - Motivation/Trigger to take action and onboard
    - Perceived similarity with other applications/solutions (positive or negative) -> image transfer leading to pre-disposition and inclination or reluctance to adopt
        - EPD (electronic patient dossier)
    - Personal experiences of participants when they had actual needs and wished they had a tool like this

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

- Clear positioning vs other players/solutions (differentiating factors) and communicate those clearly
    - Clarity whether users are intended to just transfer their data or whether they should be motivated to keep their data on the platform
- Preparedness to pay. Appeal when users have one of those trigger points when they have an actual need

Registrant - TRAIN Based onboarding tool for Service Providers (real-world ecosystem eg.)

Session Convener: Lucy Yang, Isaac Henderson
Session Notes Taker: Isaac Henderson

What Ecosystem(s) were present in the room/session?

- Retail
- Hyperledger Indy
- Swisscom Sign
- Ver ID

What Ecosystem challenges did the conversation focus on, address?

- How to evolve the technology to ecosystem?
- Interoperability of Health Credentials issued by different ecosystems.

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

Using TRAIN for Digital TRUST Infrastructure for Discovery and Validation (Regi-TRUST)

Evolution of the Regi-TRUST project:

- April 2020 COVID Credentials Initiative (CCI)
- December 2020 CCI merged into Linux Foundation Public Health (LFPH)
- February 2021 Good Health Pass Interoperability Blueprint (at ToIP representing LFPH/CCI)
- June 2021 Global COVID Certificate Network (GCCN at LFPH)
- July 2022 HIV and Health Group at United Nation Development Programme (UNDP)
- August 2022 informal collaboration between UNDP and World Health Organization (WHO) on COVID certificates
- December 2022 Rename GCCN to Regi-TRUST at UNDP to broaden its scope
- June 2023 WHO launched Global Digital Health Certificate Network (GDHCN)
- From then until now exploration and validation of Regi-Trust to support the onboarding and verification of GDHCN trust services (informal collaboration between two UN agencies)
- Next step: A MVP to demonstrate end-to-end verification of digital health certificates

Learning more about Regi-Trust here: https://www.sparkblue.org/Regi-TRUST

Proposal to Update AML regulations to enable re-use of portable KYC data

Session Convener: Michal Jarmolkowicz and Damian Glover
Session Notes Taker: Damian Glover

What Ecosystem(s) were present in the room/session?

Financial services companies, Identify verification providers, standards orgs, consultancies

What Ecosystem challenges did the conversation focus on, address?

Marcel shared that the Swiss AML Act will be updated to enable Relying Parties to accept the Swiss e-ID for customer onboarding and KYC as soon as it is in citizens' hands (FINMA has already drafted an amendment that will be published in May, with a public consultation phase following after).

We also recapped a discussion about the opportunity for banks to issue BankID-style credentials directly to a new customer after ID proofing, and whether changes in AML regulations will be needed to enable this opportunity.

See DICE ECO Session 1 BO Space D - Google Docs for notes about this opportunity from a session on Day 1

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

Data Portability on EU Level: Can individuals ask to have their data transferred to another organisation? - European Commission

ARF 1.6 open discussion

Session Convener: Viky Manaila and Esther Makaay
Session Notes Taker: Esther Makaay

What Ecosystem(s) were present in the room/session?

Type Here

What Ecosystem challenges did the conversation focus on, address?

Alignment to legal and technical requirements in the EDI Wallet ecosystem that is being developed and defined.

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

ARF 1.6 was released yesterday (4 March). This is an open discussion to take a look at what has changed. The main changes are on:

- Batch issuance and re-issuance of PID and attestations
- Privacy risks mitigation, specifically on mitigation of linkability

In this ARF v1.6.0, relevant text from the Discussion Paper for Topic A (Privacy risks and mitigations) was included in Section 7.4.3.5. Similarly, relevant text from Discussion Paper for Topic B (Re-issuance and batch issuance of PIDs and attestations) was included in Sections 6.6.2.7 and 6.6.5.2.
The High-Level Requirements introduced in these Discussion Papers were included in Annex 2, mainly in Topic 10/23 and Topic 7.

RP-RP unlinkability
Issuer-RP unlinkability

(Issuer being PID or attestation issuer)
Does the issuer have an incentive to be (dis)honest? Offer “surveillance as a service”.
The issuer is the only one who knows everything about the datasets and any correlating data elements in there (storing the signatures, the salt could be an encryption of the identity, tracing user activity). Batch issuance is introducing new risks and is unwanted from most of the wallet providers.
You have to be very paranoid on the dataset to prevent this. It is not possible to fully mitigate linkability without ZKP. Introducing BBS+ signatures could work.

Swiss approach: there is no batch issuing.

Wallet provider: batch issuance actually is not adding that much complexity in respect to all the other complexity in there. ARKG is an optimisation for batch attestation.

Question on synchronous issuing of short-term validity PID and attestation. (Or on-demand issuing.) Wallet requests PID at the moment a RP requests for PID. It's similar to batch presentation. Just-in-time delivery: the wallet has no current valid PID (or attestation) and requests it on-demand. This gives the issuer more information on usage (risk). It also adds more complexity to the wallet (same as batch issuing, where the batch contains multiple short-lived attestations).

On some smart-phones every proof-of-possession of a key might require user interaction and it won't improve UX.

Question: how far should we go in working on mitigating unlinkability when the actual tools needed (ZKP) are out of bounds? Should we just accept the linkability risks until a better way of handling mitigation is available? (RFC 1925 flashback “With sufficient thrust, pigs fly just fine.")

No alignment from cryptographers on an approach - this doesn't help. They agree to disagree, but still working on a plan to move forward.

3 major topics that are unclear at this point:

- wallet attestations / key attestation
- revocation
- trust reference

The more options you have or allow for, the more wallet-providers have to handle in terms of complexity.

But it would be a good idea to maybe make a distinction on requirements for high-trust-assurance use cases versus everyday low-assurance use cases. But the risk is that a lot of non-qualified services will be “free-riders” taking all the components from the qualified services and use them without any security or privacy considerations.

Useful links:

- ARF on Github: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework
- ARF topics raised for open discussion: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/tree/main/docs/discussion-topics

Educational Offerings re: Digital ID

Session Convener: Kaliya & Emrys
Session Notes Taker: Kaliya

What Ecosystem(s) were present in the room/session?

We talked about the educational ecosystems around digital ID.

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

This session was inspired by a conversation that Kaliya and Emrys have been having about Educational opportunities.
Where can leaders who are asked to consider how to create digital ID systems in their countries get neutral educational opportunities to make sense of the complex landscape of digital ID.
Could there be an executive education program - at the Graduate Institute or at LSE
What about middle managers who care

We listed some resources
Linux Foundation EdX Course about Self Sovereign Identity written by Kaliya & Lucy
Kaliya also has a book Domains of Identity

We touched on the fact that the Master of Science in Identity Management and Security at the University of Texas at Austin changed its name because it didn't really go into identity management that much and was teaching very incorrect things (like passwords are identifiers and the factors of authentication are types of identifiable information).

Could an LLM be trained on good information sources on digital ID along with a Chatbot

We listed several potential case studies that could be developed

- British Columnbia
- Bhutan
- California Mobile Drivers License
- India
- EUDI
- Silicon Valley Innovation Program (DHS, CBP)
- Philippines

We touched on how Data and Identity are integral - how can they get along together.

We think there is a big demand for good educational resources for key leaders.
One key blocker is having money for curriculum development for which a number was floated between $50,000-$75,000

SESSION #6

Hedera Hashgraph SSI Ecosystem (DID: Hedra Method)

Session Convener: Renata and Micha
Session Notes Taker:

What Ecosystem(s) were present in the room/session?

What Ecosystem challenges did the conversation focus on, address?

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

NO NOTES SUBMITTED

You get the adoption you deserve. Our journey building truly decentralized identifiers for Swiss healthcare, and the path forward

Session Convener: This Loepfe (More Than Bits), Georg Greve (Vereign)
Session Notes Taker:

What Ecosystem(s) were present in the room/session?

Health, Government, Banking

What Ecosystem challenges did the conversation focus on, address?

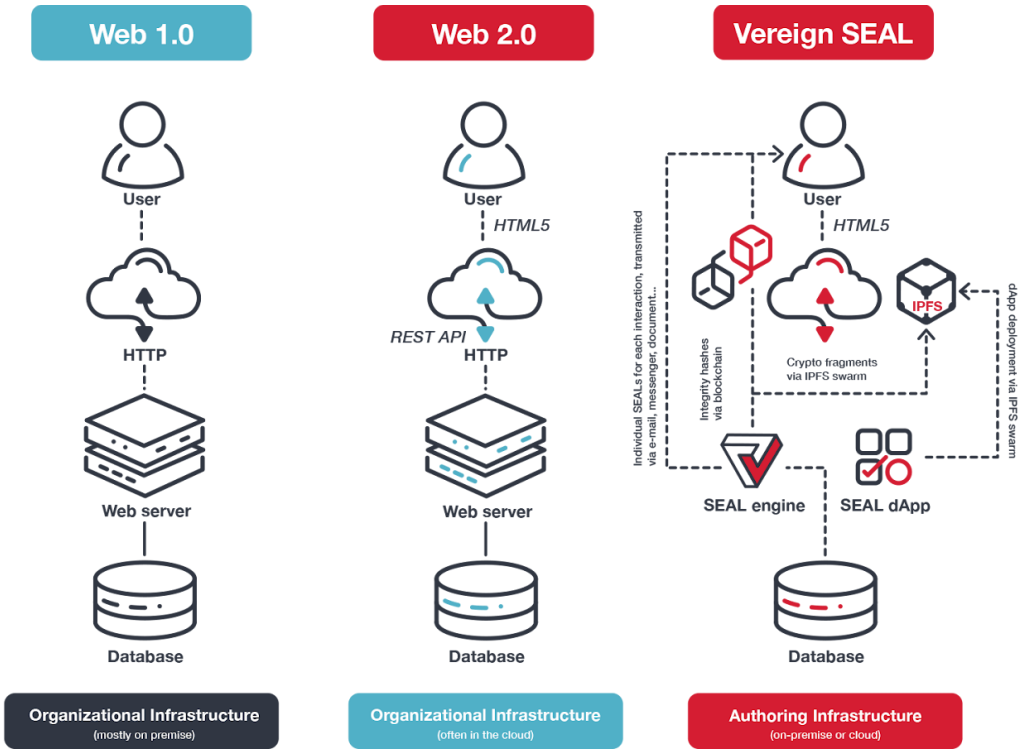
Health

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

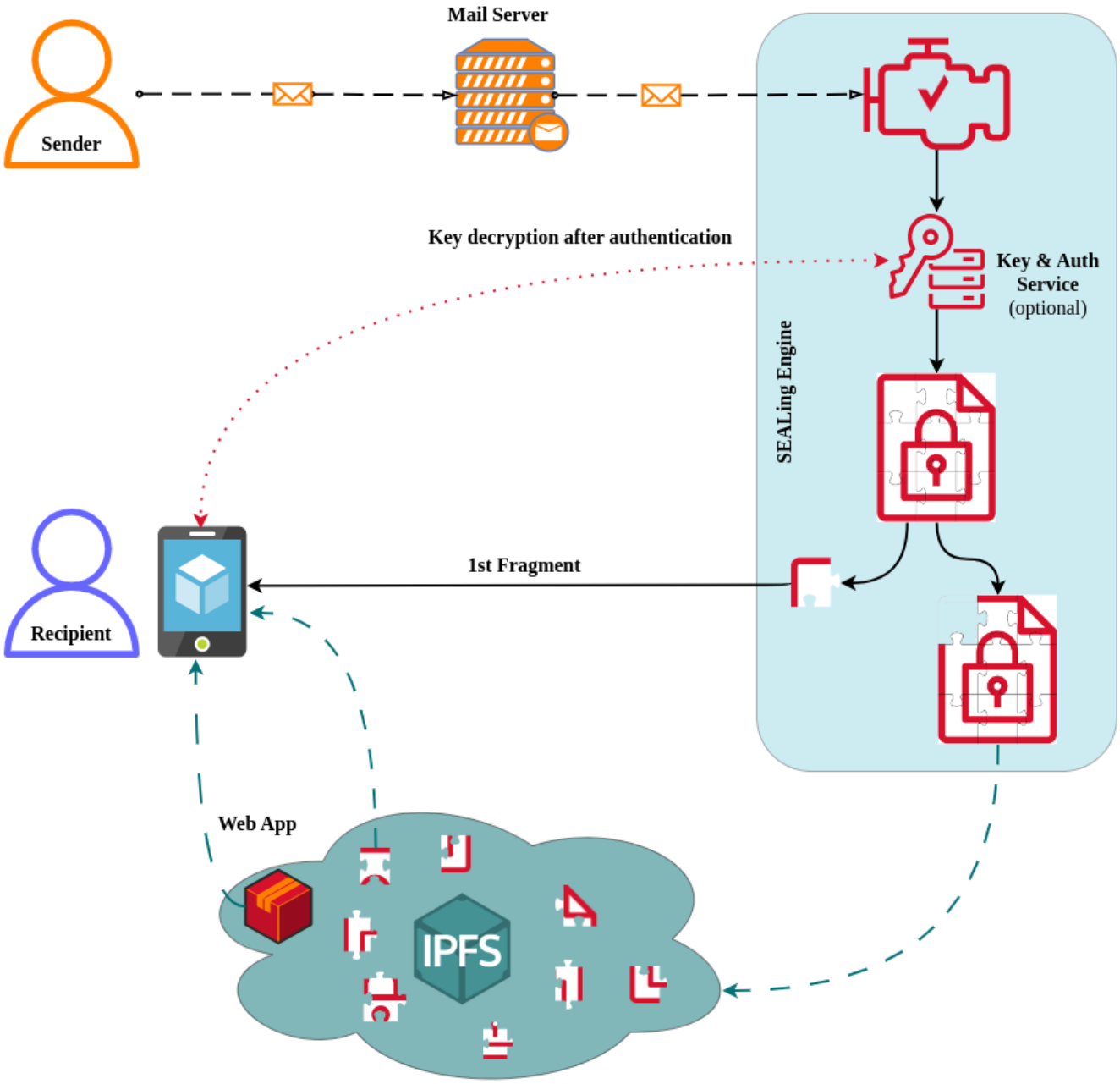
Adoption Requirements

- 9x Better Than Today -> Harvard Business School https://hbr.org/2006/06/eager-sellers-and-stony-buyers-understanding-the-psychology-of-new-product-adoption
- See Verifiable Trade Session: Paper is Peer to Peer, it is "good enough" for many things, and has fundamental benefits that trade platforms cannot match, none of them is 9x better
- Web Technology (OpenID4VC, DID:WEB, DID:WEB*) is only 1.5x better than traditional Web2.0
    - Security issues
    - Privacy issues
    - Ongoing dependencies on intermediaries
- Works only for natural monopolies (governments)
- Does not change networking effects & dynamics
- eIDAS1 did not see adoption for these exact reasons, it was only 1.5x better than paper
- eIDAS2 started out with decentralized idea, but is meanwhile eIDAS 1.1, at best
- If we want adoption, we must build PAPER, not PLATFORM
- Articles dealing with these issues:
    - https://ggreve.medium.com/self-sovereign-identity-over-before-it-started-661b4b0dbdc6
    - https://ggreve.medium.com/a-future-for-self-sovereign-identity-c237caa5e46f
- Our journey trying to be ready for adoption started with the understanding we had to take SECURITY, PRIVACY, DECENTRALIZATION seriously
- KERI was front-runner, but had issues in implementation
    - Python -> not fit for long-term production, incomplete
    - Rust -> incomplete, exotic license
    - Community path unclear
- DID:SVDX (Sovereign Data Exchange) was the result
    - based on IPFS

    - Key Event Chain
    - truly decentralized
    - built to be upgradeable
- First product on top of this stack: SEAL



- Mail delivery to the edge, based on SEAL



- Next steps: DIDComm, Wallet
- Decentralized network for authentic data delivery

A lively discussion about the properties of IPFS, and the attempt to understand the overall properties of the resulting architecture resulted.

An interesting session that ended when the time was up and people called us into the closing circle.

How do we make Value more visible? What are we missing? & ECOSYSTEM ENABLERS - Awareness, Education, Training, Resources, and Gaps

Session Convener: Daniel S., James, Zoé B.

Session Notes Taker:
(optional) List of Session Attendees:

- Vitor Bernardo (vitor.bernardo@adnovum.ch)

What Ecosystem(s) were present in the room/session?

IT providers, DIDAS, Governments (CH, UK, NL)

What Ecosystem challenges did the conversation focus on, address?

How to get the future issuers & verifiers (businesses and gov) to envision, plan and act on the coming innovation?

How to bring awareness and understanding among businesses and help them to build use cases that will compose a striving and attractive ecosystem?

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

What enablers?

TOOLS / STARTER KIT

- "how to come to relevant use cases for your organisation?"
- visualise opportunities and make business benefits graspable
    - Value Proposition Model (advice: pains relievers before gain creators)
    - Business Model Canvas
    - Stakeholders Mapping
    - Personas & Journeys (use cases visualisations)
    - Data & Growth Flywheel Concept

AWARENESS

- quantity and figures (x% of …)
- reference examples (success stories, use cases catalogue)
- value articulation (we help … to …)
- association interviews (what are the pains?)
- adapt language (no "transactions" but "business processes"

EDUCATION

- digital identities for dummies

SOLUTIONS

- template for municipalities portals to use with wallets (trust infr. integrators & UI)
- solutions catalogue
- architecture solutions adoptions map to guide people in their choice (who is using which tech, etc.)

generally:
Target and focus context pro context (not trying to highlight value for the whole ecosystem at once)
treat use case pro use case as a startup

Who is needed at the table?

- People in diverse industries
- Product managers
- innovation teams & managers
- channels owners
- architects
- tech providers

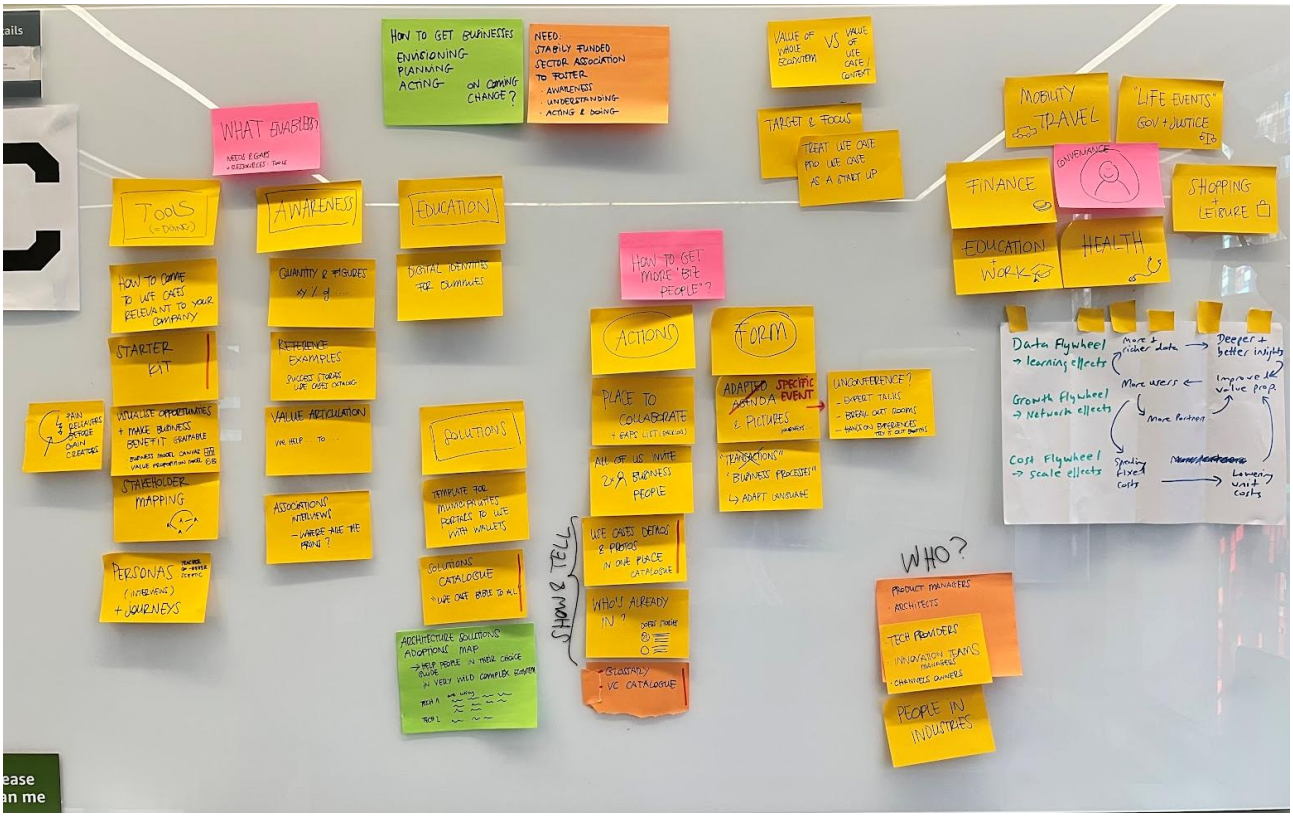
What can we concretely do? What's next?

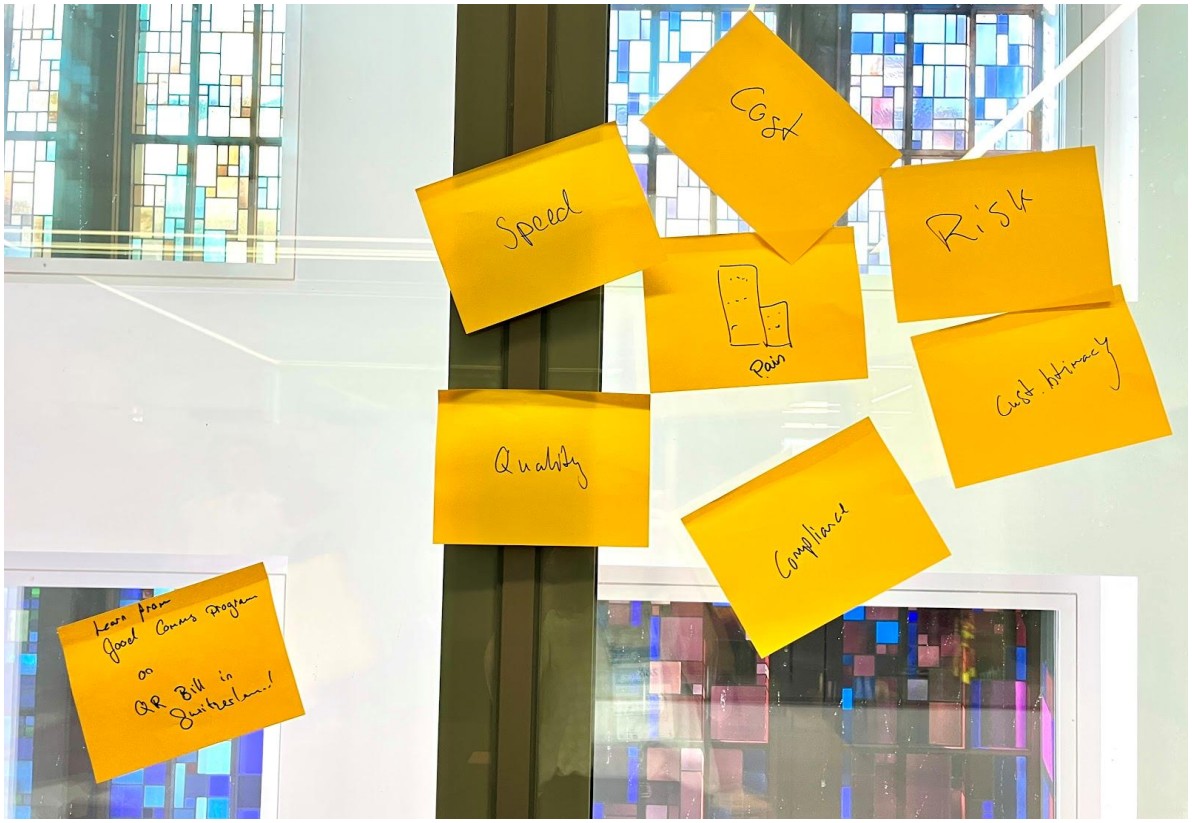
FORM

- A specific event
    - experts talks
    - break out sessions
    - hands-on experiences / try it out booths,
- All of us invite 2 Business people

ACTIONS

- Place to collaborate provided by DIDAS
- Create Backlog for show & tell motions
- Identify what is already there and what are the gaps
- ARTIFACT 1: use cases demo & protos catalogue (*what all is possible?*)
- ARTIFACT 2: build-my-use-case-starter-kit (to use in roundtables)
- ARITFACT 3: doers stories / who is already in? (*who can I relate to and feel I might be missing out?*)
- ARTIFACT 4: Glossary
- ARTIFACT 5: VC catalogue
- ARTIFACT 6: architecture solutions map & adoption


HOW TO GET BUSINESSES
ENVISIONING
PLANNING
ACTING
ON COMING CHANGE?
NEED:
STABLY FUNDED
SECTOR ASSOCIATION
TO FOSTER
- AWARENESS
- UNDERSTANDING
- ACTING & DOING
WHAT ENABLERS?
TOOLS
AWARENESS
EDUCATION
HOW TO MAKE
TO USE CASES
RELEVANT TO YOUR
COMPANY
STARTER
KIT
QUANTITY & FIGURES
XX % of ...
DIGITAL IDENTITY
FOR COMMUNITIES
REFERENCE
EXAMPLES
VALUE ARTICULATION
VIA HELP TO
VITALIZE OPPORTUNITIES
+ MAKE BUSINESS
BENEFIT GRAPPABLE
STAKEHOLDER
MAPPING
ASSOCIATIONS
INTELLIGENT
- WHERE ARE THE
PAINS ?
PERSONAS
(INTERVIEWS)
+ JOURNEYS
SOLUTIONS
TEMPLATE FOR
MVNO PILOTES
PORTALS TO USE
WITH WALLETS
SOLUTIONS
CATALOGUE
- USE CASE BRICKS TO ALL
ARCHITECTURE SOLUTIONS
ADOPTIONS MAP
→ HELP PEOPLE IN THEIR CHOICE
WITHIN A VERY WILD COMPLEX ECOSYSTEM
HOW TO GET
MORE "BIZ
PEOPLE"?
ACTIONS
FORM
PLACE TO
COLLABORATE
+ BAPS LIST (PACKAGE)
ALL OF US INVITE
2x BUSINESS
PEOPLE
USE CASES DESIGN
& PILOTES
IN ONE PLACE
CATALOGUE
WHO'S ALREADY
IN ?
- GLOSSARY
- VC CATALOGUE
SHOW & TELL
ADAPTED SPECIFIC
AGENDA EVENT
& PICTURES
"TRANSACTIONS"
"BUSINESS PROCESSES"
↳ ADAPT LANGUAGE
UNCONFERENCE?
- EXPERT TALKS
- BREAK OUT ROOMS
- HANDS ON EXPERIENCES
WHO?
PRODUCT MANAGERS
- ARCHITECTS
TECH PROVIDERS
- INNOVATION TEAMS
- CHANNELS OWNERS
PEOPLE IN
INDUSTRIES
VALUE OF
WHOLE
ECOSYSTEM
VS
VALUE
OF
USE CASE/
CONTEXT
TARGET & FOCUS
TREAT USE CASE
AND USE CASE
AS A START UP
MOBILITY
TRAVEL
"LIFE EVENTS"
GOV + JUSTICE
GOVERNANCE
FINANCE
EDUCATION
WORK
HEALTH
SHOPPING
LEISURE
Data Flywheel
→ learning effects
More + richer data
Deeper + better insights
More users
Improved UX
Value Prop
Growth Flywheel
→ Network effects
More Partners
Cost Flywheel
→ scale effects
Spreading fixed costs
Lowering unit costs


Speed
CoGx
Risk
Pain
Cust. Intimacy
Quality
Compliance
Learn from
Good Corona Program
as
QR Bill in
Switzerland!

The First BILLION USER Credential

Session Convener: Drummond Reed
Session Notes Taker: Ankur Banerjee

What Ecosystem(s) were present in the room/session?

Ayra, Linux Foundation

What Ecosystem challenges did the conversation focus on, address?

First Person Credentials are described in an Ayra white paper called The Special Network Effects of Ayra Network Credentials. As one of a small family of Ayra network credentials, they are designed to work across any number of ecosystems in the Ayra Trust Network.

The goal of the session was to explain the structure of First Person Credentials and the strategy of how to drive adoption to the first billion users.

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

- One subtopic was self-certifying identifiers (SCIDs), which are essential to First Person Credentials. This led to a discussion of the DIDs used by Bluesky (Seattle Seahawks How decentralized is Bluesky really? -- Dustycloud Brainstorms) and the new did:scid specification at ToIP.
- The session covered the business, governance, and technical architecture of First Person Credentials as explained in the First Person Project FAQ.
- Drummond noted that a POC of the user experience of exchanging First Person Credentials face-to-face is slated to be ready for Internet Identity Workshop #40 in April — and hopefully will be in full production by DICE in September.

EUDI Framework + beyond: Mapping the road ahead 2025-26 AND Existing Ecosystems = Apple's and Google's plans on ID Wallets

Session Convener: Joerg Lenz, Franziska Granc
Session Notes Taker: Joerg Lenz

What Ecosystem(s) were present in the room/session?

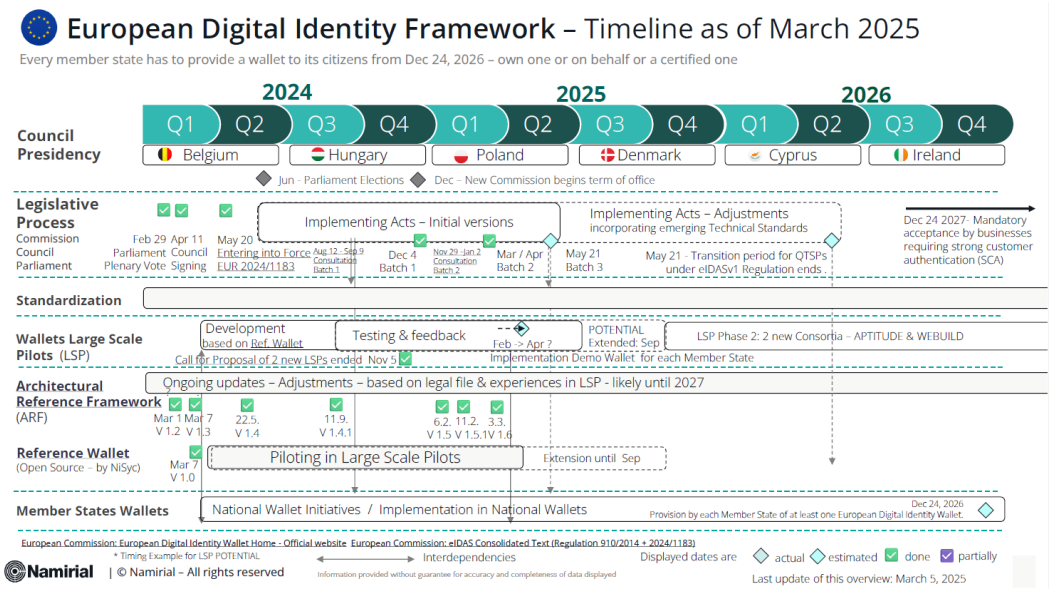
European Digital Identity Framework - stakeholders from organizations engaged in EU Large Scale Pilots piloting EU Digital Identity Wallet, including a range of Qualified Trust Service Providers with different national backgrounds of their headquarters (Switzerland, Norway, Netherlands, Spain, Italy, Germany …)

What Ecosystem challenges did the conversation focus on, address?

Wallet Ecosystems of European Digital Identity and of Apple, Google and Samsung

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

EU ID - This was an informal conversation with slides intended to trigger the Crowdworking Exercise on Identifying Impacts and Milestones of Political, Economic, Legal & Tech Influences regarding EU Digital Identity Framework and beyond - Thanks to the approx. 30-40 attendees joining in a lively discussion, sharing insights on their individual perspectives.



Disclaimer: This overview is not an official one from neither the European Commission, nor the Council of the European Union or the European Parliament. It is an ongoing attempt to track what's expected to be going on based on a compilation from various sources as additional intelligence to content on EU Digital Identity Wallet LinkedIn Channel. Any suggestions for adjustments / updates / clarifications as well as overall improvements are highly appreciated via e-mail to j.lenz@namirial.com.

The session was triggered on short notice based on input from sessions March 4 and March 5 morning by speakers and session contributors Esther Makaay, Viky Manaila and Franziska Granc as we detected that some aspects of the intro session on European Digital Identity Wallet "101" are deserving a deeper dive - in particular in judging the political aspects.

The session delivered background on recent milestones of the EUDI Framework achieved and provided an outlook of what's ahead and which political influences might propel or slow down the progress.

The last part of the session focused on the ecosystems that big-tech such as Apple, Google and Samsung have created over the years and their plans to integrate identity-related attributes to their wallet solutions. The discussion highlighted the existing dependencies that Europe faces when building their own wallet ecosystem. In addition to the significant market advantage big-tech holds in terms of user base and the wide range of low-threshold use cases already covered, a key dependency lies in the access to secure hardware elements within the devices, as well as the ability to govern app-to-app or wallet-to-wallet communication. It was found that to a certain extent regulatory pressure can counteract this. A possible globally standardized wallet API and its pros and cons were discussed briefly and would need further deliberation in the future.
OpenWallet Foundation: Overview Digital Wallets and Agents

Recent events (examples - we talked about most of them in the session)

March 3, 2025:
🎯 Version 1.6 of the Architecture and Reference Framework (ARF) for European Digital Identity Framework was published. Minor changes compared to the previous one (1.5.1):

- Expanded details on data models, trust models and certification and risk management
- New subchapter on Wallet Secure Cryptographic Devices

🎯 Technical Specifications - New versions of initial specifications for:

- EUDI Wallet Trust Mark (v 0.3)

February 2025:
🎯 Several meetings in the 4 Large Scale Pilots - for example in LSP Potential 140 participants tested 15 digital identity wallets in peer-to-peer (AT BE CZ DE FI FR HU IT LU LT PL PT SI UA) in Warsaw
🎯 Standardization - Some progress was made in e g in the European Telecommunications Standards Institute Technical Committee Electronic Signatures and Trust Infrastructures (ETSI-ESI) Meeting 85 in Barcelona where also the First Draft in defining how a Pricing Policy can be implemented within the EUDI Wallet Framework was submitted - ETSI TR 119 479-2.

🎯 Intensifying Discussions about building a sustainable ecosystem - e.g. business models centered around a verification fee paid by Relying Parties (RPs) for identity and credential verifications - as seen February 3 at International Workshop on Trends in Digital Identity (TDI) Luigi Castaldo f Namirial is suggesting to extend the validation service by

- Updating Verifiable Credentials (VCs) before presentation: This allows for custom policies and more frequent validity checks.
- Encrypted VC presentation: Wallets encrypt VCs, RPs receive decryption keys from QTSPs after paying a fee.
- Centralized Attribute Rulebook: Allows for setting pricing models and simplifies pricing for RPs.

🎯 European Union Agency for Cybersecurity (ENISA) Ad Hoc Working Group on the certification of EU Digital Identity Wallets kicked off its work

January 2025:

🎯 Ursula von der Leyen announcing the European Business Wallet as part of the EU Competitiveness Compass 2025 - Detailed Document, January 29, 2025 - This digital wallet for organisations ("company wallet", "wallet for legal persons") will become the hub for business and digitalised transactions within the EU Single Market. Based on the eIDAS framework, the wallet aims to facilitate interaction between companies and public administrations, fostering the digitalisation of services through tools such as e-signature and e-invoicing.

🎯 Switzerland: The Federal Council of Switzerland: Negotiating mandate for recognition of electronic signatures, January 29, 2025 - corresponding LinkedIn Posting "Some light on the horizon for mutual recognition of (Qualified) Electronic Signatures in both EU and Switzerland - perhaps in 2026?"

🎯 Cyprus: eIDAS compliant Electronic identification system IDMe.cy launched, January 27 2025: Business model: First 30,000 applicants receive eIDs for free, next 70,000 pay €15 (usually €50) for a three-year validity. Report in ID Tech Wire

🎯 SPRIND - Bundesagentur für Sprunginnovationen Funke Challenge EUDI Wallet Prototype - Working Group Ecosystem Governance Session: Two proposals for How Qualified Trust Service Providers could collect verification fees from Relying Parties without violating user privacy and unlinkability required by the eIDAS regulation by IDNow and Namirial, January 20, 2025. Session Recording

🎯 Implementing Regulations Batch 2 - Public Feedback was closing January 2, 2025

What happened between our session March 5 and while these notes were finalized March 11

March 9, 2025:

🎯 Technical Specifications - New versions of initial specifications for:

- Specification of Systems enabling the Notification and subsequent Publication of Provider Information (v 0.3)

Coming up…

… are for example sooner or a bit later in 2025:

🎯 Reference Implementation - Expected work in Q2: Wallet Unit Attestation (WUA) and Key Attestation, Wallet instance revocation, Re-issuance of PID or Attestation before the validity ends, Testing Suite for Wallet Providers, PhotoID attestation, Updates to issuance and presentation protocols and standards (Q2/2025) and Open-source proximity verifier (Android) - Work items may be subject to changes - List reflects the status as of March 5, 2025.

Roadmap

🎯 Implementing Regulations (IR) - Publication of IRs Batch 2 (target date. mid March), Batch 3: Lots of drafts to be reviewed; Political deadline for publication Implementing Regulations: May 21, 2025.

🎯 Technical Standards (TS) - Updated versions of drafts to be reviewed. Meeting 86 will be held from May 26-28 in Sophia Antipolis (FR) and Meeting 87 with Plenary is scheduled for Sep 16-18 in Bilbao (ES). Besides, ETSI CEN and CENELEC are also working on standardization.

🎯 Large Scale Pilots Phase II - Two new consortia are expected to start in September 2025 running for 24 months: WE BUILD (197 organizations - led by Dutch and Swedish government authorities) and the Advanced Project for Trusted Identity Technologies and Unified Digital Ecosystem (APTITUDE, 110+ organizations - coordinated by the French government)

Last, but not least next stock taking on developments in Digital Identity in Zurich:

🎯 September 2-4 - Digital Identity unConference

To be clarified down the road (example)**:**

Implementing Regulations may be revised annually as necessary, especially when new standards become available: Will member states adapt laws for national implementation on an annual basis? Germany recently published a tender as the government is requiring support in handling all the IRs

Clarifying a very frequent misunderstanding (as discussed in this session):

The provision of at least one certified EU Digital Identity Wallet by each EU member state to its citizens which is either from an own one or certified for usage in the member state is due by December 24, 2026. There are several other due dates floating around such as November 21, 28 or December 4. To be clear what the joint understanding of the session participants is:we are looking at Christmas Eve as the “Wallet Day” - because there was a minor delay in getting the corresponding Implementing Regulation approved (28 November 2024 instead of 21 November 2024). However, according to EU legislative procedures Implementing Regulations enter into force 20 days after publication in the Official Journal (here: 4 December 2024) become applicable two years later (here: 24 December 2026).

What session participants were expecting

The first releases of national government driven EUDI Wallets in 2025/26 are likely to

- not being completely harmonized as certification is owned by the member states. There is an overall effort by the European Union Agency for Cybersecurity (ENISA) to harmonize

security guidelines and prevent fragmentation but might see some more harmonization rather in 2028 or later.
- just include Personal Identification Data such as the National ID Card, Driving License and Health ID Card with maybe no or just a few additional verified digital credentials / attestated electronic attributes

Recommended Reading

Presentation slides (available for Download via LinkedIn Smart Link)
20250304-05-DICE-eIDAS-updates-Lenz
Many of these slides are frequently updated. If you are accessing that file sometimes later in 2025 and are interested if there is a more recent version of one or the other slide and/or if you detect any errors please reach out to j.lenz@namirial.com

Notes of related sessions in DICE Ecosystems 2025
DICE ECO S1F What is a (European Digital Identity) wallet?
DICE ECO S5F ARF 1.6 open discussion

Recommended Food for Thought - Blog Posts & Slide Sets
Matteo Panfilo: "Possible Architectures of EU Digital Identity Wallets National Certifications and the Roles of Key Stakeholders", Blogpost of February 27. 2025
Luigi Castaldo: Electronic Attestation of Attributes Extended Validation Services, February 3, 2025 at International Workshop on Trends in Digital Identity (TDI) 2025 Bologna - PDF of Slide Set via LinkedIn Smart Link
The Federal Council of Switzerland: Negotiating mandate for recognition of electronic signatures, January 29, 2025
ID Union: Cost savings through Organizational Digital Identities, January 10, 2025
Jörg Lenz: European Digital Identity Wallet: Positions of the Parties in the German Federal Parliament, December 28, 2024

Notes for this session were last edited March 11. 2025

Attendee & Sponsor Posts about DICE Ecosystems 2025

Key State Capital
215 followers
1mo •

🌎 Throughout the 2-day event in Zurich, Digital Identity unConference Europe | DICE brought together leaders and innovators shaping the future of decentralized identity, self-soverign identity, verifiable credentials, and Web3 identity solutions.

The event served as a platform for collaboration, knowledge-sharing, and technological advancements in the decentralized identity space.

We were incredibly honoured to be involved as a sponsor where the unConference format allowed for a unique, dynamic, and attendee-driven event.

It was the first opportunity for players in the industry to engage with the Web of Trust Map. As an interactive tool, it is the most comprehensive attempt to visualize the expansion of the ecosystem; as such, launching this at DICE Ecosystems 2025 was the perfect match.

Massive thanks to Daniel Saeuberli of DIDAS, Kaliya IdentityWoman Young, TRUST SQUARE, and Internet Identity Workshop for co-organising the event along with their partners.

Vladimir Vujovic • 2nd
Head of Digital Product Management at SICPA
1w •

Just came back from **Digital Identity unConference Europe | DICE** where we had some brilliant and very passionate people and some great discussions on ecosystems and adoption. It was good to see this relatively small community coming together on these events, sharing their opinions and passion for these technologies.

Event though different ecosystems in different parts of the world are making steady progress with their technical implementations and regulations, the common feeling around the different sessions was that this community and these events need more representatives of organizations who will be the actual adopters and more representatives of (big) consulting companies and system integrators that will be implementing these technologies into existing business processes.

Validated ID
5,025 followers
3w •

+ Follow ···

🚀 Validated ID sponsors & participates in #DICE Ecosystems 2025! 🔗🔐
On March 4-5, we will be at DICE Ecosystems 2025 in #Zurich, a key event focused on boosting the adoption of verifiable credentials and decentralized identity solutions across diverse business ecosystems.

💡 Our team Guillem Sardà Parreu & Pablo Cosio Molleda will be there, actively contributing to discussions that drive real-world use cases and cross-sector collaboration in the digital identity space.

As a proud sponsors and participants, we are committed to shaping the future of verifiable credentials and ensuring businesses can leverage authentic, trusted data in their ecosystems.

📍 If you're attending, let's connect and explore how decentralized identity can empower trust and interoperability across industries!

Find out more about DICE: https://diceurope.org/

#DICEEcosystems2025 #VerifiableCredentials #DigitalIdentity #DecentralizedIdentity

Joerg Lenz • 1st

Working on simplicity meeting compliance in combining artificial int...

2mo • Edited •

Spoilt for choices today at **Digital Identity unConference Europe | DICE** - the equivalent of **Internet Identity Workshop** (IWW) known in the US- running today and tomorrow at **TRUST SQUARE** in Zurich.

This agenda was crated this morning, based on the proposals from proactive attendees, facilitated and coordinated by **Heidi Nobantu Saul**.

Currently sitting in the workshop session AMA **#swiyu** - the electronic identity trust infrastructure of Switzerland with **Rolf Rauschenbach** and members of the Federal Office of Justice - very informative. **Andreas Frey Sang** diving into many details and cross-pointing to correspondening sources.

Andreas Tölke • 1st

Head FinTech & Digital Trust at Swisscom | Advisor of W3ff Venture | ...

Visit my website

2mo • Edited •

🚀 Ready to kick off the **Digital Identity unConference Europe | DICE**

My colleagues from **Swisscom** and I are looking forward to two interesting days of exchange with thought leaders and experts in the **#digital #identity** space.

Digital Identity unConfernce Europe | #DICEurope 2025

DICE 2025 – September 2 – 4 - Zurich

Sept. 2 - 4, 2025 | **DICE 2025 |** Zurich | Venue TBD
EarlyBird Registration HERE | Sponsorship Opportunities
Our established 3-Day Annual gathering for the companies and individuals working on developing and deploying digital identity systems in Europe.

Follow DICE and Trust Square on LinkedIn

Follow the Digital Identity OpenSpace unConference Europe on LinkedIn and TRUST SQUARE on LinkedIn to see posts about this event and to hear about plans for #DICE 2025!

Digital Identity Unconference Europe | DICE 2025 Co-organizing Partners

Thanks to the DICE Ecosystems 2025 Co-Hosting Team

Andreas Freitag with Procivis
Daniel Sauberli with DIDAS
Kaliya Young with Internet Identity Workshop
Marc Houser with Trust Square
Tim Weingärtner with Lucerne University of Applied Sciences and Arts

The Digital Identity Unconference Europe | DICE is an IIW Inspired ™ Regionally Focused Open Space unConference event.

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

Upcoming IIW and IIW Inspired Events

Digital Identity unConference Europe - DICE
Promoting digital identity collaboration across Europe
With Our Partners TrustSquare & DIDAS

Sept. 2 - 4, 2025 | **DICE2025** | Zurich | Venue TBD
EarlyBird Registration HERE | Sponsorship Opportunities
Our established 3-Day Annual gathering for the companies and individuals working on developing and deploying digital identity systems in Europe.

IIW XLI
October 28 - 30, 2025
The 41st **Internet Identity Workshop**

REGISTRATION OPEN in June
www.InternetIdentityWorkshop.com

Bridging the Digital Identity Gap in the SADC Region
Did:UNCONF AFRICA 2026 | With Our Partner DIDx
February 24 - 26, 2026 | STIAS Stellenbosch, South Africa
REGISTRATION OPEN SOON | Sponsorship Opportunities

You can see the Inaugural DID:UNCONF AFRICA Event Summary here:
Photo Gallery, Event Overview Video, Highlights, Video Testimonials

Visit www.didunconf.africa for updates or email info@didunconf.africa for more information about attending and sponsoring. Stay tuned for updates via IIW email, LinkedIn, we'll be sharing news, programme highlights, and ways to get involved.DID:UNCONF AFRICA