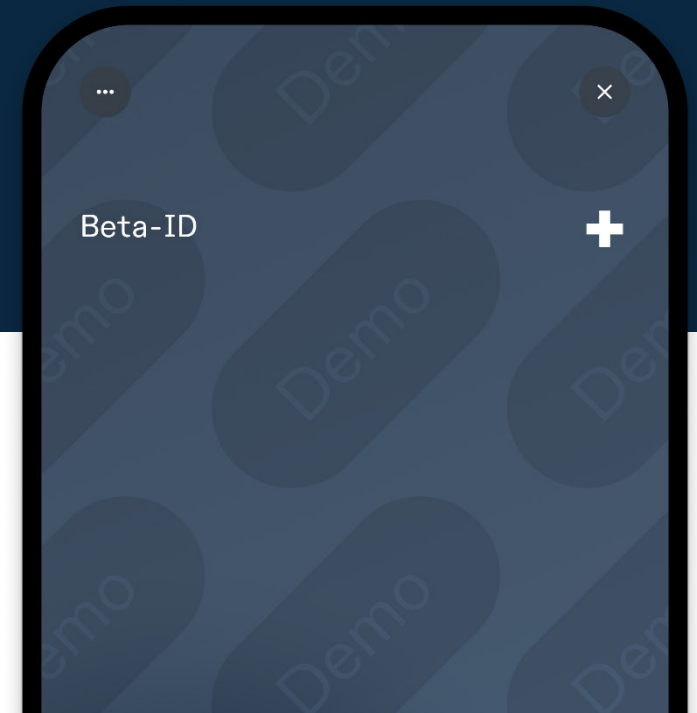


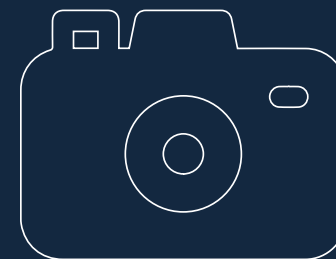


e-ID participation meeting

06.02.2025



**The participation meeting is
recorded and published on
YouTube.**



Agenda (1/3)



- Welcome & Procedure
- Status and outlook
 - Legislation
 - Unlinkability
 - Public Beta
 - e-ID Unit
- Report from the OpenWallet
Forum High Level Panel
Meeting in Davos

Agenda (2/3)



- Piloting the OpenID Federation in the international education and research community
- Interoperability Profiles in Practice: Leveraging Verifiable Credential Metadata and Trust Registries

Agenda (3/3)



- What is a trust protocol and what strategy is the Confederation pursuing?
- Questions from the audience
- Conclusion

- Executive Summary in English

Status and outlook for legislation



Rolf Rauschenbach, BJ/OFJ

Collection of signatures against the BGEID



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

BBI 2025
www.fedlex.admin.ch
Massgebend ist die signierte
elektronische Fassung



Ablauf der Referendumsfrist: 19. April 2025 (1. Arbeitstag: 22. April 2025)

Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

vom 20. Dezember 2024

– Art. 36 Referendum und Inkrafttreten

¹ Dieses Gesetz untersteht dem fakultativen Referendum.

² Der Bundesrat bestimmt das Inkrafttreten.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

FF 2025
www.fedlex.admin.ch
La version électronique
signée fait foi



Délai référendaire: 19 avril 2025 (1^{er} jour ouvrable: 22 avril 2025)

Loi fédérale sur l'identité électronique et d'autres moyens de preuves électroniques (Loi sur l'e-ID, LeID)

du 20 décembre 2024

– Art. 36 Référendum et entrée en vigueur

¹ La présente loi est sujette au référendum.

² Le Conseil fédéral fixe la date de l'entrée en vigueur.

Position of the federal government during collection periods



- Collecting signatures for a referendum is a constitutional right.
- The federal government does not comment on this. Political statements are neither confirmed nor corrected.
- The federal government provides information and answers technical questions.

Consultation on implementing provisions



- Consultation on the implementing provisions is planned before mid-2025

Status and outlook unlinkability



Andreas Frey Sang, BJ/OFJ

What has happened so far



- Q3/Q4 2023: **Technical Advisory Circle** ([discussion paper](#))
- Q1 2024: **Informal consultation** ([evaluation report](#))
- Q2/Q3 2024: **Internal administrative consultation**
- 6.12.2024: [Technology decision](#) by the Federal Council

Implementation strategy Unlinkability



- **e-ID** should be **introduced** as quickly as possible.
- **e-ID** should **be unlinkable** as quickly as possible, possibly in a second phase.
- Dedicated **funds and team resources** are used to drive forward the topic of unlinkability.

What is unlinkability?



- Unlinkability refers to the impossibility of linking **different transactions** carried out with an e-ID
- The question is whether it is possible **to track what a person does with their E-ID** (profiling)
- [Blog post on unlinkability](#)

Additional topics



- **Observability:** Traceability based on the use of the infrastructure
- **Deniability:** deniability for e-iD holders
- **Purpose limitation:** technically ensure purpose-related data release
- **Post-quantum cryptography**

Call for discussion and participation



- Have the topics been chosen **correctly**?
- Has an important topic been **forgotten**?
- Are there **experts** with whom the e-ID programme should speak?

[Link to dicussion-thread on GitHub](#)

Status and outlook Public Beta



Rolf Rauschenbach, BJ/OFJ

Public beta open-source repositories



- **Base Registry**
- **Status Registry**
- **Trust Registry**
- **DID Toolbox**
- **DID Resolver**
- **iOS Wallet App**
- **Android Wallet App**
- Issuer-agent → will be published soon
- Verifier-agent → will be published soon

Status and outlook e-ID Unit



Rolf Rauschenbach, BJ/OFJ

Status and outlook e-ID Unit



- The e-ID Unit was able to start its work
- Three further positions will be advertised shortly; a newsletter will follow

Report from the OpenWallet Forum High Level Panel Meeting in Davos



Rolf Rauschenbach, BJ/OFJ

OpenWallet Forum High Level Panel Meeting



Beat Jans, Federal Councilor, Swiss Confederation (from left to right)

Doreen Bogden-Martin, Secretary General, International Telecommunication Union

Solly Malatsi, Minister of Communications and Digital Technologies, South Africa

Welcome Remarks by Federal Councilor Beat Jans



Wallets for state-issued credentials must adhere to **democracy, the rule of law, and human rights principles**. Therefore, Switzerland actively advocates for:

- privacy-preserving crypto-processors as **open hardware** in all smartphones.
- **Open-source** solutions, as exemplified by the e-ID Act's commitment to publishing all source code.
- **Multilateral and multistakeholder** approaches for legitimacy and sustainability.



Challenges for interoperability for digital wallets and the need for multistakeholder collaboration



Christina Hirsch, Head Digital Trust, Swisscom (from left to right)

Todd Fox, Vice President Government Engagement, VISA

Edouard Bugnion, Vice-President for Innovation and Impact, EPFL

Guilherme de Aguiar Patriota, Ambassador, Brazil Mission to WTO

Solly Malatsi, Minister of Communications and Digital Technologies, South Africa

Alain Labrique, Director, Department of Digital Health and Innovation (DHI) Science Division (SCI), World Health Organization

Wonseok Baek, Head of Samsung Wallet Global BD/Product, Samsung Electronics

Bill Ren, Chief Open-Source Liaison Officer, Huawei

The importance of international standards for the interoperability of digital wallets



Viky Manaila, President, CSC Cloud Signature Consortium (from left to right)

Mike Milinkovich, Executive Director, Eclipse Foundation

Sergio Mujica, Secretary General, ISO

Arman Aygen, Director of Technology, EMVCo

Bilel Jamoussi, Deputy Director, Telecommunication Standardization Bureau, ITU

Daniela Barbosa, Executive Director, Linux Foundation DT

Seth Dobbs, CEO, W3C

Philippe Metzger, Secretary-General & CEO, IEC

Gail Hodges, Executive Director, OpenID Foundation

Call to action to facilitate global digital trust



The OpenWallet Forum High Level Panel members recognize that

- a) Multipurpose digital wallets will become a crucial component for the **digital public infrastructure** and a vital tool for people and organizations to participate in the **digital economy and socio-economic development...**

[Link to the full Call to action](#)

Global Digital Trust Conference (working title)



- Juli 1 and 2, 2025 in Geneva
- Up to 1750 participants
- Co-convened by the Swiss Confederation, ITU and Linux Foundation (tbc)
- Co-organized by other UN-organizations, Standard development organizations, Open- source organizations and others, including NGOs

Piloting the OpenID Federation in the international education and research community



Christoph Graf, Programme Manager, Switch

Interoperability Profiles in Practice: Leveraging Verifiable Credential Metadata and Trust Registries



**Matteo Marangoni, Senior Software Engineer,
Digital Identity, SICPA**

What is a trust protocol and what strategy is the Confederation pursuing?



Michel Sahli, Innovation Fellow, BJ/OFJ

The Swiss Trust Protocol as one element of the decision on technical implementation



Decision by the Federal Council as per press release



Technical details as published on GitHub

The Federal Council

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

The Federal Council
The portal of the Swiss government

Federal Council Federal Presidency Departments Federal Chancellery Federal law Documentation

Swiss government - Homepage > Documentation > Press releases > Press releases by the Federal Council > e-ID: Federal Council takes decision on technical implementation

< Documentation < Back to overview

Press releases

Press releases by the Federal Council

News subscription

e-ID: Federal Council takes decision on technical implementation

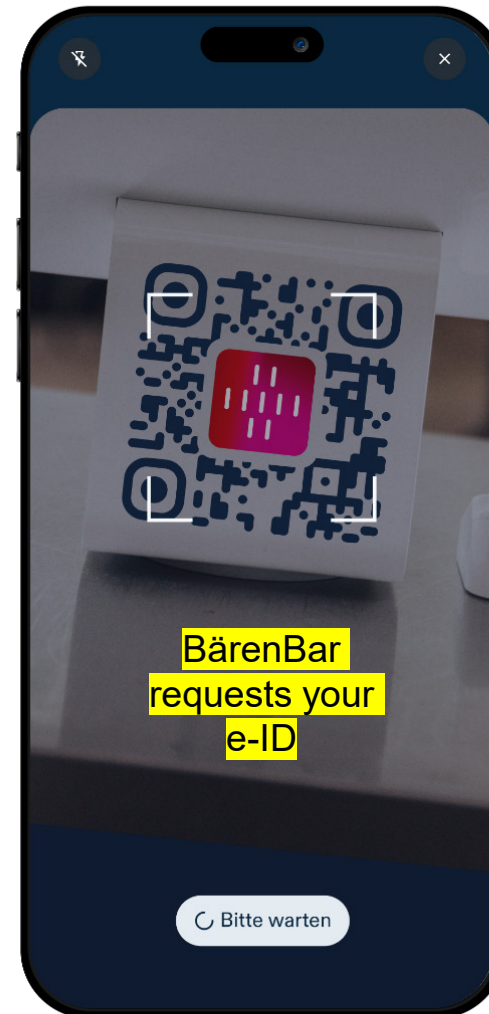
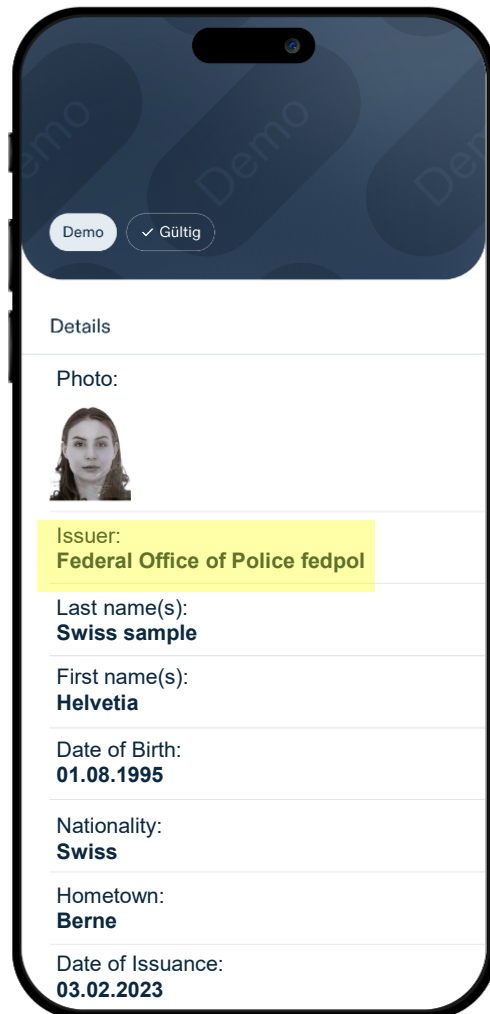
Bern, 06.12.2024 - At its meeting on 6 December, the Federal Council defined the principles regarding the technical implementation of the Confederation's new electronic identity (e-ID), which is to take place in two stages. At the same time, the name of the trust infrastructure was also announced: the federal government's digital wallet is to be known as SWIYU.

Aspect	Current Hypothesis	Link	Public Beta Support
Identifiers	Decentralized Identifiers (DIDs) v1.0 according to W3C DID Method: did:sw/didwebvh	W3C: https://www.w3.org/TR/did-core/ Method: Trust DID Web - https://identity.foundation/trustdidweb/	SELECTED Hosted on central base registry provided by Confederation
Status Mechanisms	Statuslist	Statuslist: https://datatracker.ietf.org/doc/draft-ietf-oauth-status-list/	SELECTED
Trust Protocol	Trust Protocol based on VCs	Trust protocol based on VCs	SELECTED Initial support of the "identity" trust statement by Confederation
Communication Protocol (Issuance/Verification)	OID4VC/OID4VP	Issuance: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-ID1.html Verification: https://openid.net/specs/openid-4-verifiable-presentations-1_0-ID2.html	SELECTED In accordance with Swiss profile
Payload Encryption	JWE as proposed by the communication protocol	https://www.rfc-editor.org/rfc/rfc7516.html	CANDIDATE
VC-Format/Signature-Scheme Combination	SD-JWT VC & ECDSA	SD-JWT VC: https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/	SELECTED In accordance with Swiss profile
Device Binding Scheme	Hardware based device binding depending on capabilities provided by mobile devices Software based device binding implemented by wallets	Apple: https://developer.apple.com/documentation/cryptokit/secureenclave Android: https://source.android.com/docs/security/features/keystore	Hardware SELECTED Software UNSUPPORTED
VC appearance	Visualization of Verifiable Credential with OCA	https://github.com/e-id-admin/open-source-community/blob/main/tech-roadmap/rfcs/oqa/spec.md	UNSUPPORTED

How can I be sure that the issuer or verifier is who they claim to be?



How can I be sure that the issuer is trustworthy?



How can I be sure that a verifier is trustworthy?

What do we need for trust?



Trust Infrastructure

Swiss trust infrastructure, in particular the base and trust registries, operated by the Swiss Confederation

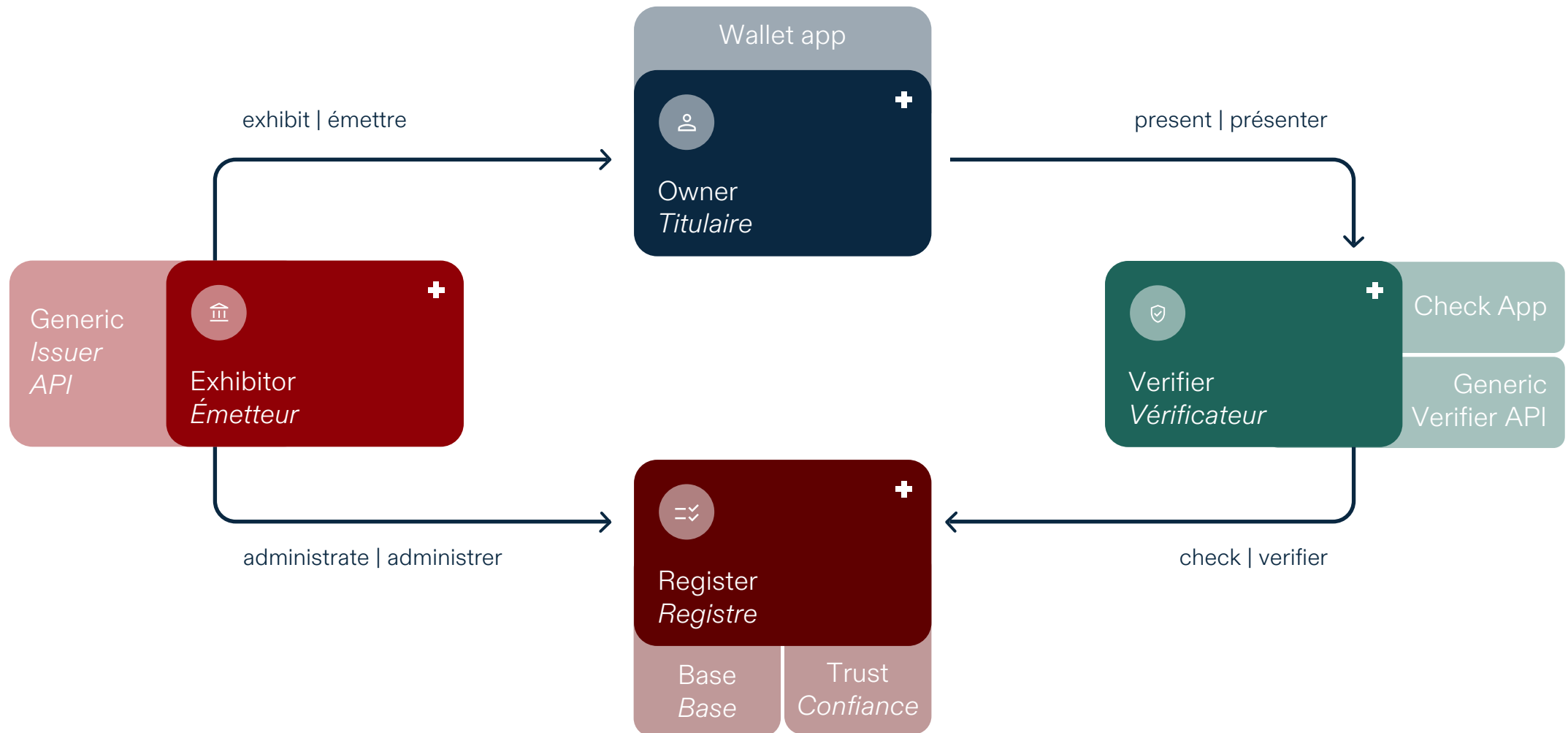
Trust Statement

Represent a machine and human readable statement about trust

Trust Protocol

Defines how to interact with the trust registry

Trust infrastructure: The trust cycle

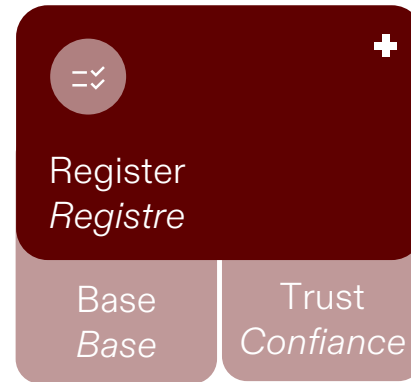


Trust infrastructure: Registries



Base registry provides technical trust via cryptographic identifiers

- `did:webvh:confapw4...`



Trust registry provides human trust via verifiable trust statements

- Verified identity of issuer or verifier
- Legitimate issuer or
- Legitimate verifier

Trust statement: Content



Verified identity

Issuer or verifier is who she or he claims to be

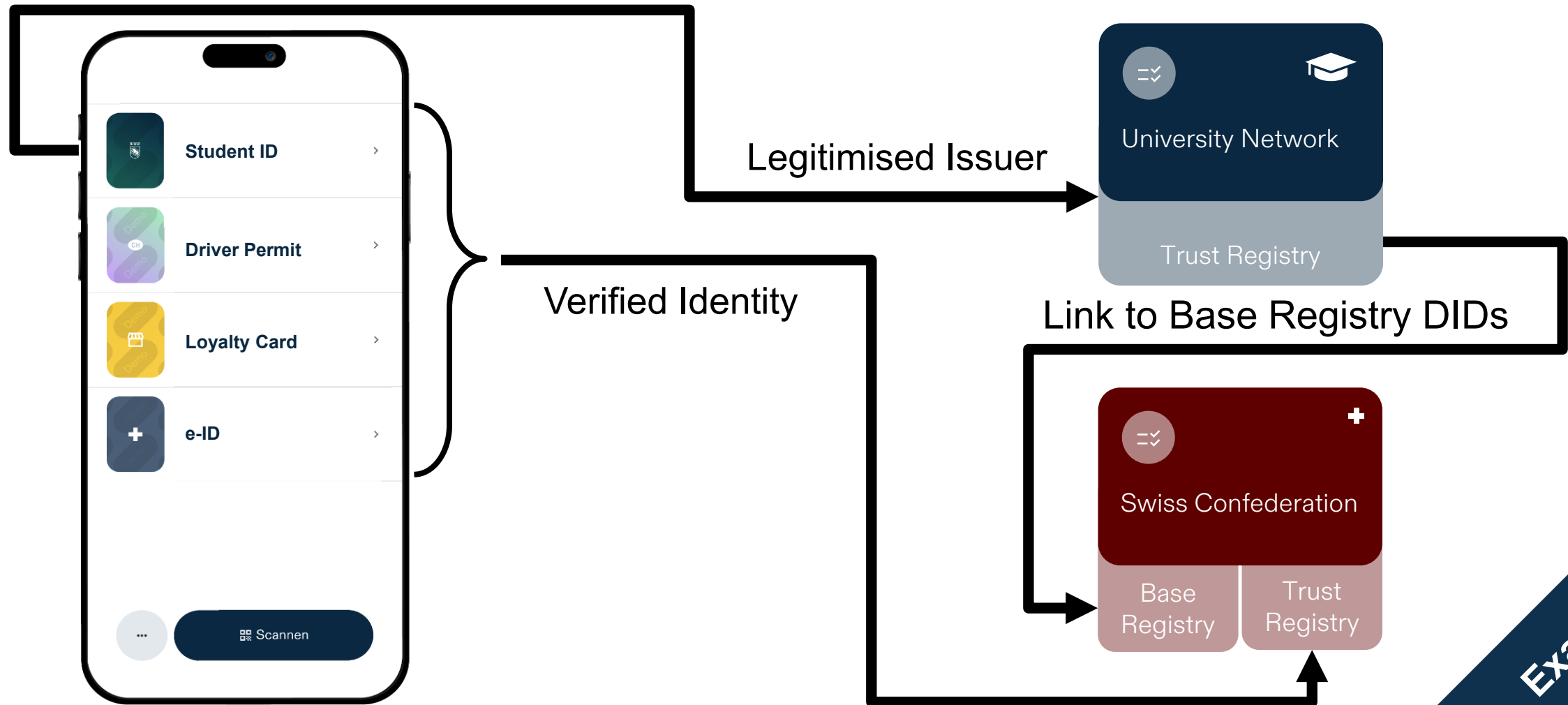
Legitimate issuer

Issuer is legitimately issuing a certain verifiable credential

Legitimate verifier

Verifier is legitimately verifying a certain verifiable credential

Trust statement: Private actors can issue trust statements from their own trust registries



Example

Trust statements: Eligibility for trust statements issued by the Swiss Confederation



Verified identity

- Actor needs to be registered in the Swiss base registry
- Legal persons require a Swiss UID-number
- Natural persons require a Swiss e-ID

Legitimate issuer and/or legitimate verifier

- The Swiss Confederation only issues legitimacy statement about actors fulfilling regulated tasks
- Other actors can operate third party trust registries and issue trust statements according to their sectorial needs

Trust protocol: Initial candidates



X.509		
<ul style="list-style-type: none">• issuer• subject	<ul style="list-style-type: none">• not-before• not-after	constraint
public key		

Description

- Identity bound to a public key

Disadvantages

- Difficult to adapt to Swiss needs

OpenID Federation (JWT)		
<ul style="list-style-type: none">• eats• sub	<ul style="list-style-type: none">• iat• exp	constraint
public key	trust marks	entity metadata
		metadata policies

Description

- Identity bound to a public key with advanced federation and metadata support

Disadvantages

- Complex and overly extensive

Trust protocol: The Swiss choice



OIDF Trust Marks (JWT)		
<ul style="list-style-type: none">• eats• sub	<ul style="list-style-type: none">• iat• exp	<ul style="list-style-type: none">• Id• delegation
<ul style="list-style-type: none">• logo_uri• ref	<i>Additional claims MAY be defined</i>	
Examples only use HTTPS		



Swiss Trust Statements (SD-JWT)		
<ul style="list-style-type: none">• eats• sub	<ul style="list-style-type: none">• iat• exp	<ul style="list-style-type: none">• vct• status
<i>trust statement type dependent content</i>		
DID		

Pain Points

- No API to get all trust marks about an actor
- Trust registry could monitor validity requests
- Additional claims not defined as structured data
- No description on how to use with DIDs

Advantages

- Fulfills the current regulatory requirements

Disadvantages

- No delegation mechanism defined yet
- Not a globally accepted specification

Potential next steps



**First
implementation
in 2026**

**International
interoperability
date tbd**

- Migrate our specification to a standard development organisation?
- Establish a trust mark profile in OpenID Federation?
- Use an abstracted trust protocol query specification?

General questions from the audience



Rolf Rauschenbach, BJ/OFJ

Next participation meeting



- Thursday, 6 March 2025
4 pm
- Executive Summary in English 6
pm

Contact us



Rolf Rauschenbach

Deputy Head of the e-ID Division
Information Officer e-ID|

Federal Department of Justice and Police FDJP
Federal Office of Justice FOJ

Bundesrain 20, 3003 Berne
Phone +41 58 465 31 20
rolf.rauschenbach@bj.admin.ch

General information on the e-ID

General information on e-ID

www.eid.admin.ch

Information on e-ID legislation

Informations sur la législation e-ID

www.bj.admin.ch

Discussion platform for e-ID

Plateforme de discussion sur l'e-ID

www.github.com

Registration for the e-ID newsletter

Inscription à la newsletter e-ID

www.eid.admin.ch