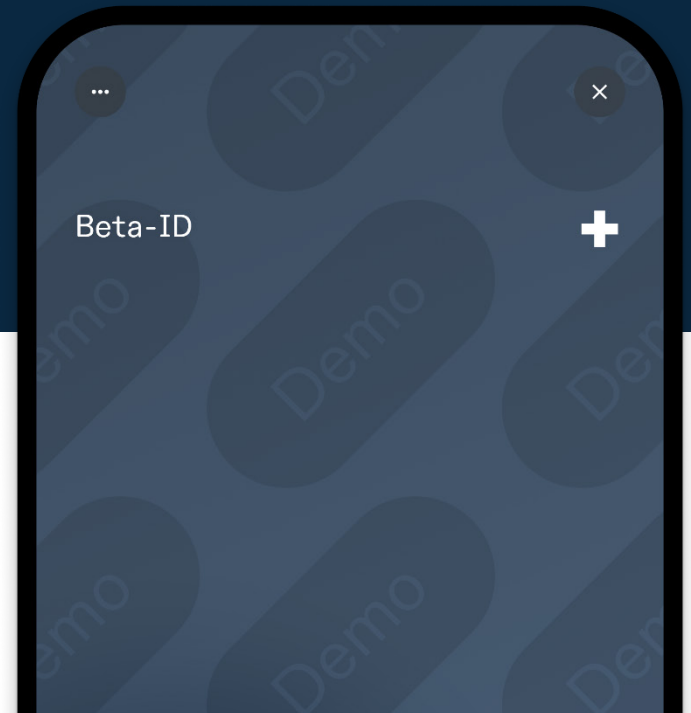
Partizipations-Meeting e-ID
Réunion participative e-ID

06.02.2025



Das Partizipationsmeeting wird aufgenommen und auf YouTube publiziert.

La réunion participative est enregistrée et publiée sur YouTube.

Agenda (1/3)
Agenda (1/3)

- Begrüssung & Ablauf
- Stand und Ausblick
  - Gesetzgebung
  - Unverknüpfbarkeit
  - Public Beta
  - Fachbereich e-ID
- Bericht vom OpenWallet Forum High Level Panel Meeting in Davos

- Accueil & déroulement
- État des lieux et perspectives
  - Législation
  - Non-traçabilité
  - Public Beta
  - Unité e-ID
- Rapport du OpenWallet Forum High Level Panel Meeting à Davos

Agenda (2/3)
Agenda (2/3)

- Pilotierung der OpenID-Federation in der internationalen Bildungs- und Forschungsgemeinschaft
- Interoperability Profiles in Practice: Leveraging Verifiable Credential Metadata and Trust Registries (Präsentation auf Englisch)

- Projet pilote pour l’utilisation d’ OpenID-Federation dans la communauté internationale de l’éducation et de la recherche
- Interoperability Profiles in Practice: Leveraging Verifiable Credential Metadata and Trust Registries (présentation en anglais)

Agenda (3/3)
Agenda (3/3)

- Was ist ein Vertrauensprotokoll und welche Strategie verfolgt der Bund?
- Fragen aus dem Publikum
- Schluss

- Executive Summary in English

- Qu'est-ce qu'un protocole de confiance et quelle stratégie suit la Confédération ?
- Questions de l’audience
- Conclusion

- Executive Summary en anglais

Stand und Ausblick Gesetzgebung
État des lieux et perspectives sur la législation

Rolf Rauschenbach, BJ/OFJ

Unterschriftensammlung gegen das BGEID
Collecte de signatures contre LeID

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

BBl 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 (1er 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.

Haltung des Bundes während Sammelfristen
Position de la Confédération pendant les délais de collecte

- Das Sammeln von Unterschriften für ein Referendum ist ein verfassungsmässiges Recht.
- Der Bund nimmt dazu keine Stellung. Politische Aussagen werden weder bestätigt noch korrigiert.
- Der Bund informiert und beantwortet fachliche Fragen.

- La collecte de signatures pour un référendum est un droit constitutionnel.
- La Confédération ne prend pas position à ce sujet. Les déclarations politiques ne sont ni confirmées ni corrigées.
- La Confédération informe et répond aux questions techniques.

Vernehmlassung Ausführungsbestimmungen
Consultation sur les dispositions d'exécution

- Vernehmlassung der Ausführungsbestimmungen ist vor Mitte 2025 geplant

- La consultation des dispositions d'exécution est prévue avant la mi-2025

Stand und Ausblick Unverknüpfbarkeit

État des lieux et perspectives sur la non-traçabilité

Andreas Frey Sang, BJ/OFJ

Was bisher geschah
Ce qui s'est déroulé jusqu'à présent

- Q3/Q4 2023: **Technical Advisory Circle** (Diskussionspapier)
- Q1 2024: **Informelle Konsultation** (Evaluationsbericht)
- Q2/Q3 2024: **Verwaltungsinterne Konsultation**
- 6.12.2024: **Technologie-Entscheid** des Bundesrats

- Q3/Q4 2023: **Technical Advisory Circle** (document de consultation)
- Q1 2024: **Consultation informelle** (rapport d'évaluation)
- Q2/Q3 2024: **Consultation interne de l'administration**
- 6.12.2024: **Décision technologique** du Conseil fédéral

Umsetzungstrategie Unverknüpfbarkeit
Stratégie de mise en œuvre de non-traçabilité

- **e-ID** soll so schnell wie möglich **eingeführt** werden.
- **e-ID** soll so schnell wie möglich **unverknüpfbar** sein.
- Die **Einführung** der **e-ID** wird **nicht** an die **Umsetzung** der Unverknüpfbarkeit geknüpft.
- Es werden dedizierte **Mittel und Team-Ressourcen** eingesetzt, um das Thema voranzutreiben.

- **L'e-ID** doit être **introduit** le plus rapidement possible.
- **L'e-ID** doit atteindre la **non-traçabilité** le plus rapidement possible.
- **L'introduction** de **l'e-ID n'est pas** liée à **l'implémentation** de la non-traçabilité.
- Des **ressources** sont dédiées pour faire progresser le thème de la non-traçabilité.

Was ist Unverknüpfbarkeit?
Qu’est-ce que la non-traçabilité ?

- Unverknüpfbarkeit bezieht sich auf die Unmöglichkeit, **unterschiedliche Transaktionen**, die mit einer e-ID vorgenommen werden, verknüpfen zu können
- Es geht um die Frage, ob es möglich ist **nachzuvollziehen, was eine Person mit ihrer E-ID macht** (Profilbildung)
- Blogpost zur Unverknüpfbarkeit

- La non-traçabilité se base sur l'impossibilité d'établir un lien entre **différentes transactions** effectuées avec une e-ID.
- Il s’agit de la question de la possibilité **de savoir ce qu’une personne fait avec son e-ID** (profilage)
- Article sur la non-traçabilité

Themenfelder
Thèmes

- **Observability:**
  Nachvollziehbarkeit anhand der Nutzung der Infrastruktur
- **Deniability:** Abstreitbarkeit für Inhaberinnen
- **Purpose limitation:**
  Zweckgebundene Datenfreigabe technisch sicherstellen
- **Post-Quantum Kryptographie**

- **Observability:**
  Traçabilité à partir de l'utilisation de l'infrastructure
- **Deniability:**
  Répudiation pour les titulaires
- **Purpose limitation:**
  Assurer techniquement que le partage de données se fasse uniquement à des fins définies
- **Cryptographie post-quantique**

Aufruf zum Diskutieren und Mitmachen
Appel à discuter et à participer

- Sind die Themenfelder **richtig** gewählt?
- Wurde ein wichtiges Thema **vergessen**?
- Gibt es **Expertinnen und Experten**, mit denen das E-ID Programm sprechen sollte?

- Les thèmes sont-ils **bien choisis** ?
- Un sujet important a-t-il été **oublié**?
- Y a-t-il des **experts** avec lesquels le programme e-ID devrait s'entretenir ?

Link auf Github

Stand und Ausblick Public Beta
État des lieux et perspectives 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

Stand und Ausblick Fachbereich e-ID
État des lieux et perspectives Unité e-ID

Rolf Rauschenbach, BJ/OFJ

Stand und Ausblick Fachbereich e-ID
État des lieux et perspectives Unité e-ID

- Der Fachbereich e-ID konnte seine Arbeit aufnehmen
- Die Ausschreibung von drei weiteren Stellen steht kurz bevor; ein Hinweis per Newsletter wird folgen

- L’unité e-ID a pu démarré ses activités
- La publication de trois autres postes est imminente ; une information suivra par newsletter.

Bericht vom OpenWallet Forum High Level Panel Meeting in Davos
Rapport du OpenWallet Forum High Level Panel Meeting à 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

Pilotierung der OpenID-Federation in der internationalen Bildungs- und Forschungsgemeinschaft

Projet pilote pour l’utilisation d’ OpenID-Federation dans la communauté internationale de l’éducation et de la recherche

Christoph Graf, Program Manager, Switch

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

Matteo Marangoni, Senior Software Engineer, Digital Identity, SICPA

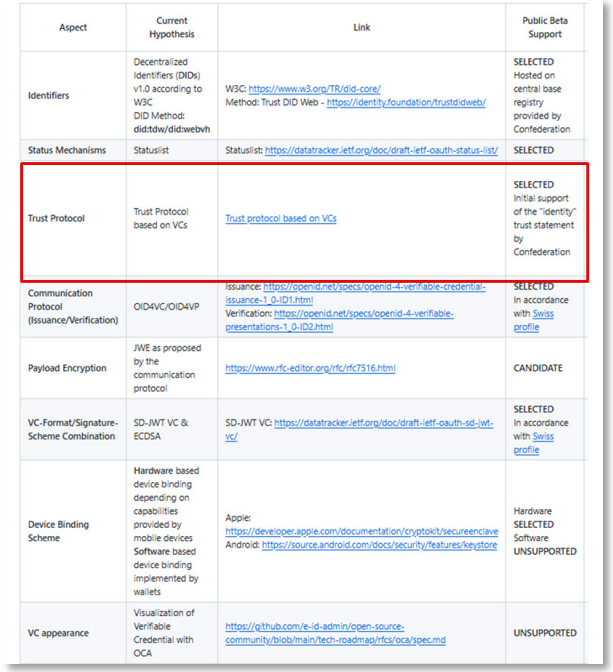
Was ist ein Vertrauensprotokoll und welche Strategie verfolgt der Bund?
Qu'est-ce qu'un protocole de confiance et quelle stratégie suit la Confédération ?

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

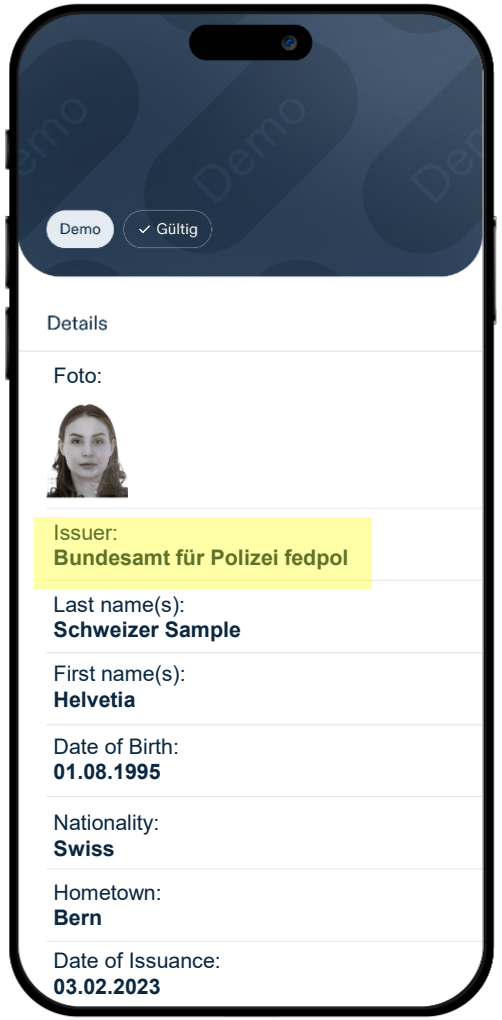
Technical details as published on GitHub



Aspect	Current Hypothesis	Link	Public Beta Support
Identifiers	Decentralized Identifiers (DIDs) v1.0 according to W3C DID Method: did:tdw/did:webvh	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/oca/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

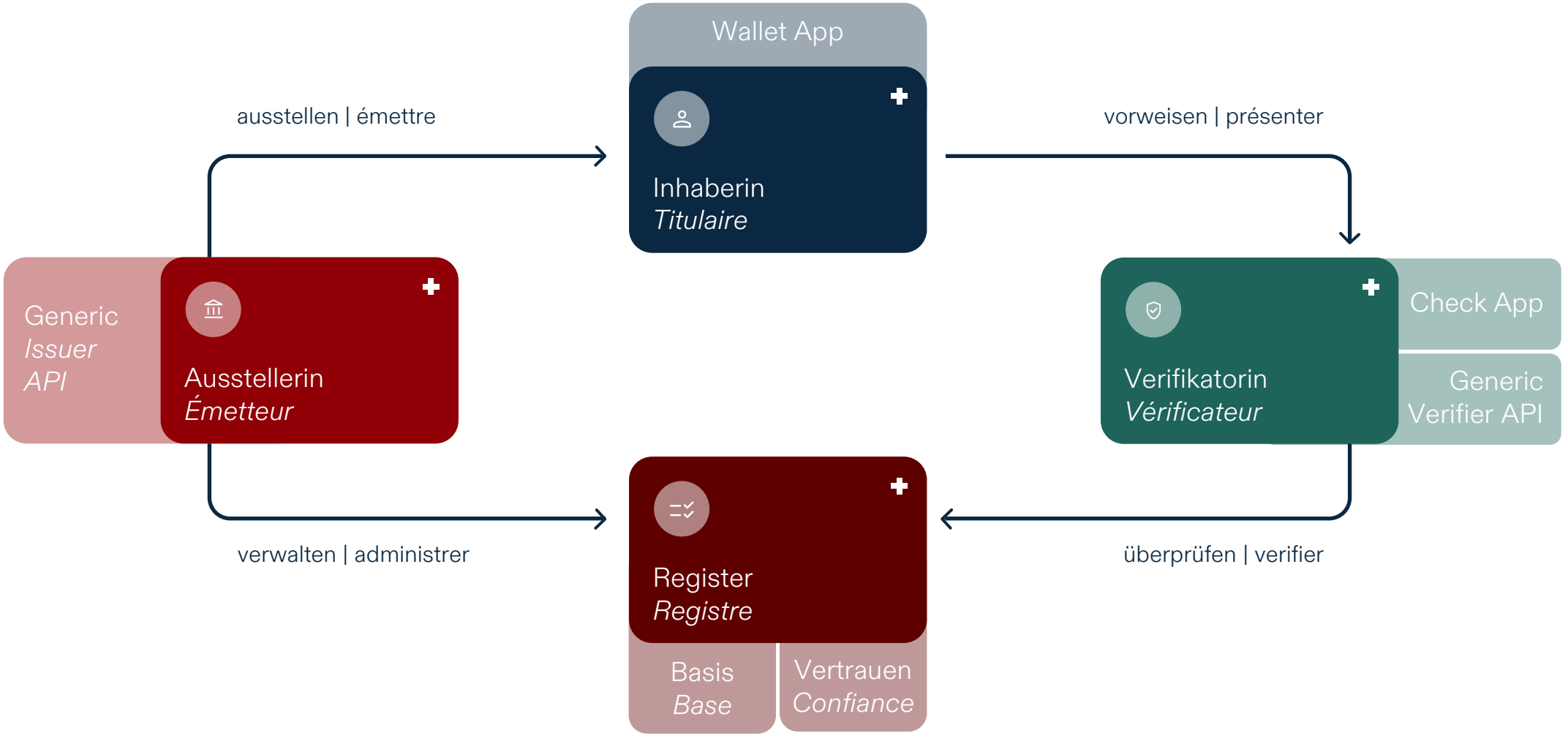
Trust Statement

Represent a machine and human readable statement about trust

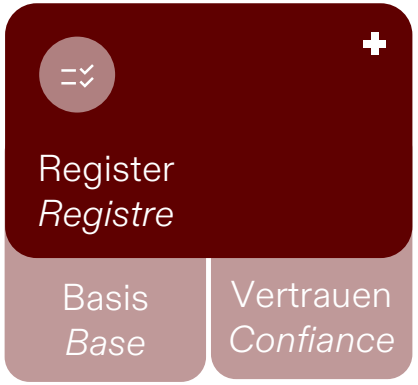
Trust Protocol

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

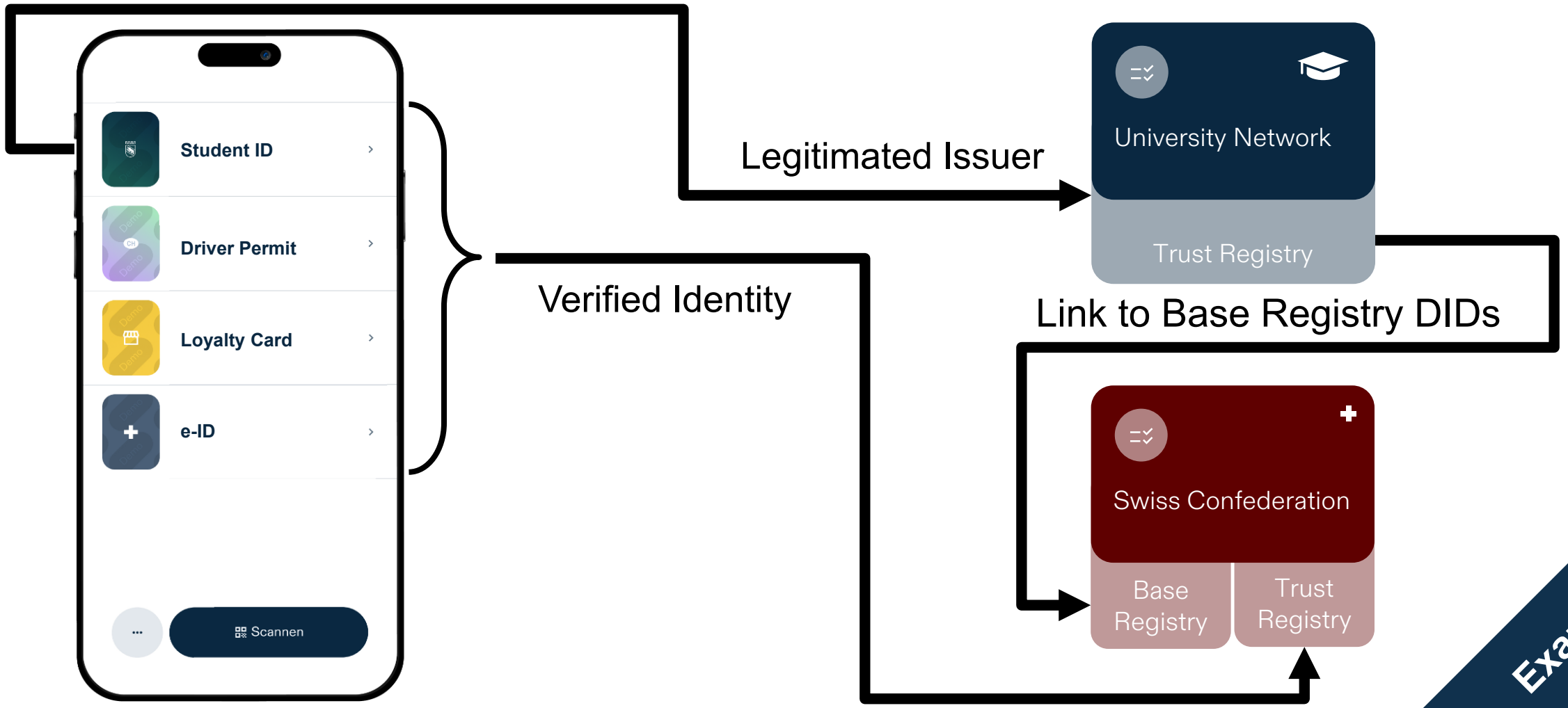
Legitimate issuer

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



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

Verified identity

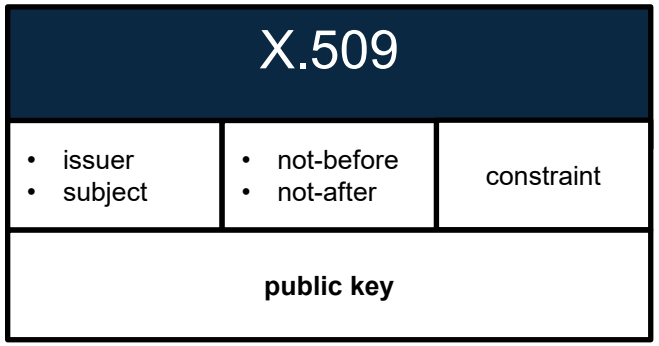
- Actor needs to be registered in the Swiss base registry
- Legal persons require a Swiss UID-number
- Natural persons require a Swiss e-ID

Legitimate issuer and/or legitimate verifier

- The Swiss Confederation only issues legitimacy statement about actors fulfilling regulated tasks

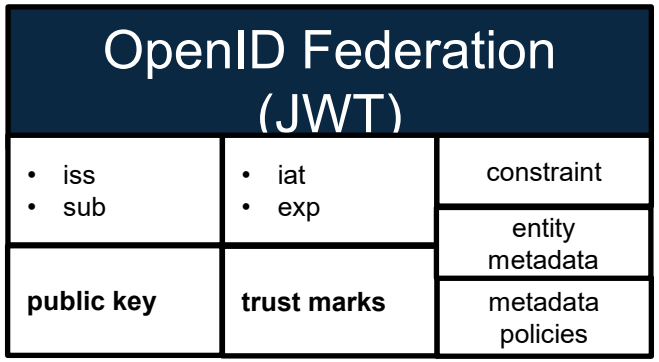
Other actors can operate third party trust registries and issue trust statements according to their sectorial needs

Trust protocol: Initial candidates



Description
- Identity bound to a public key

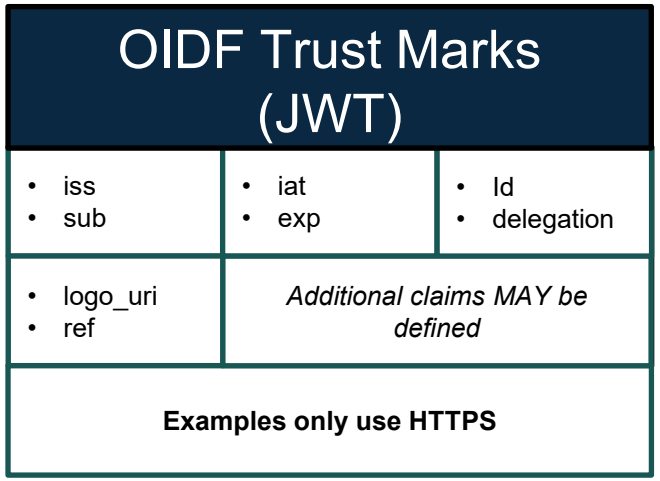
Disadvantages
- Difficult to adapt to Swiss needs

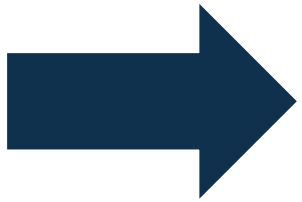


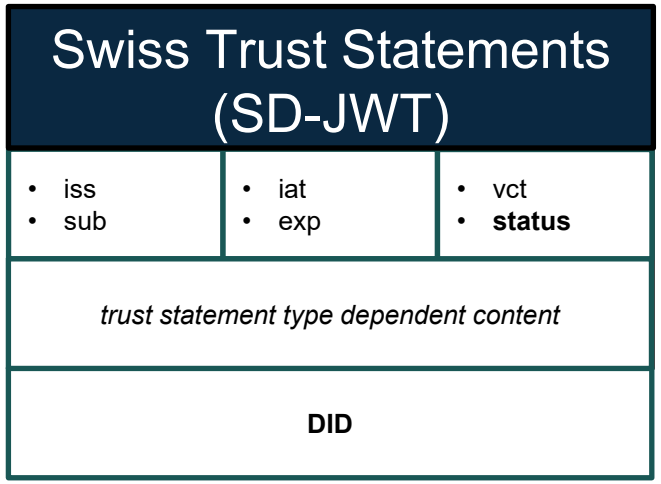
Description
- Identity bound to a public key with advanced federation and metadata support

Disadvantages
- Complex and overly extensive

Trust protocol: The Swiss choice







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 organization?
- Establish a trust mark profile in OpenID Federation?
- Use an abstracted trust protocol query specification?

Questions?

Allgemeine Fragen aus dem Publikum

Questions générales de l’audience

Rolf Rauschenbach, BJ/OFJ

Nächstes Partizipationsmeeting
Prochaine réunion participative

- Donnerstag, 6. März 2025
  16 Uhr
- Executive Summary in English
  18 Uhr

- Jeudi, 6 mars 2025
  16 heures
- Executive Summary en anglais
  18 heures

Kontakt
Contact

Rolf Rauschenbach
Stv. Leiter Fachbereich e-ID
Informationsbeauftragter e-ID|

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz BJ

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

Allgemeine Informationen zur e-ID

Informations générales sur l'e-ID
www.eid.admin.ch

Informationen zur e-ID-Gesetzgebung

Informations sur la législation e-ID
www.bj.admin.ch

Diskussionsplattform zur e-ID

Plateforme de discussion sur l'e-ID
www.github.com

Anmeldung zum e-ID-Newsletter

Inscription à la newsletter e-ID
www.eid.admin.ch