Participation meeting

Electronic identity and trust infrastructure

08.05.2025

swiyu | A service of the Swiss Confederation

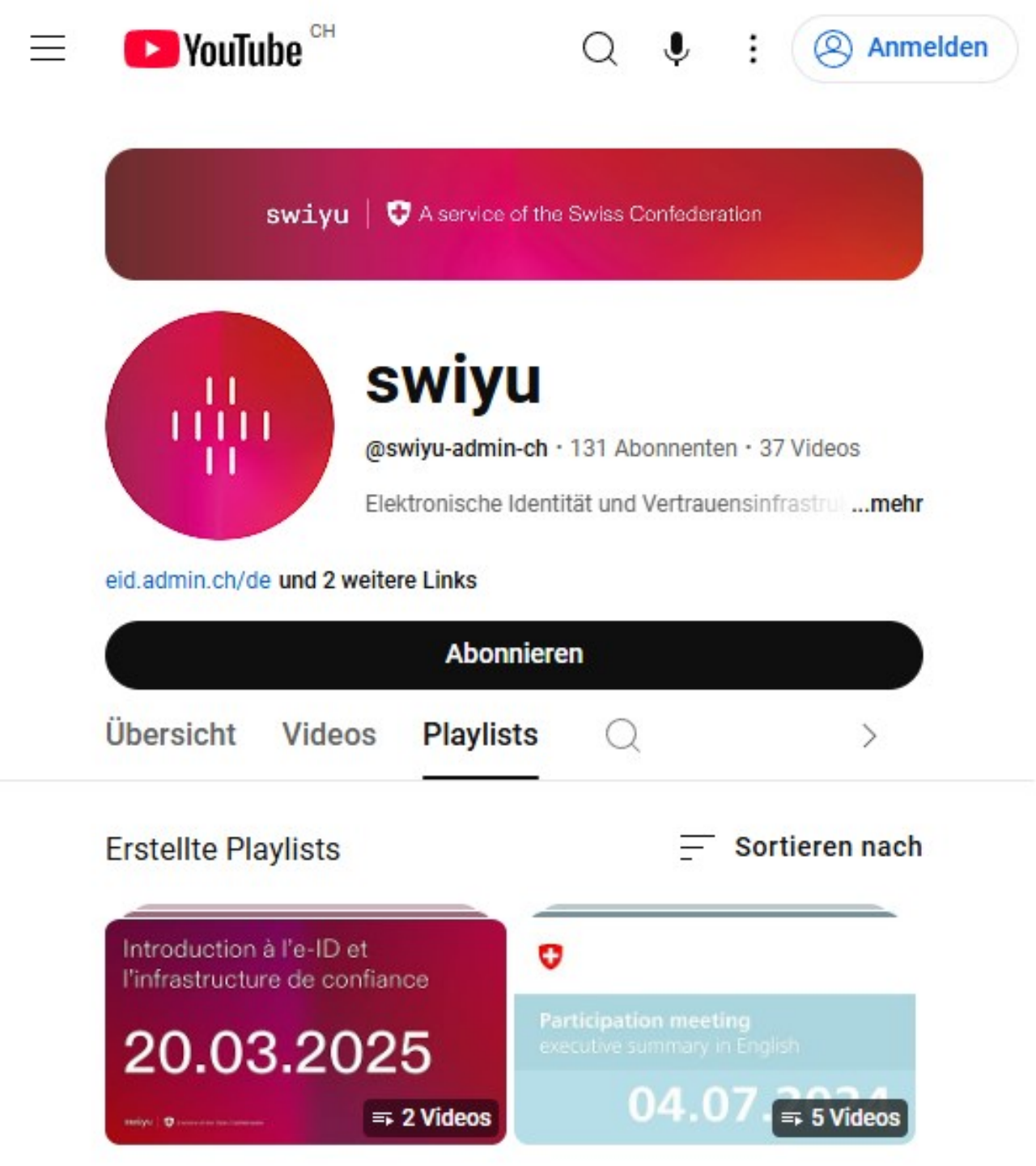
La version française est disponible sur GitHub.

The German version is available on GitHub.

Contents

Recording

The participation meeting is recorded and published on YouTube.



Questions and answers

- Please consult our ressources!
  - www.eid.admin.ch
  - https://www.youtube.com/@swiyu-admin-ch
  - https://github.com/swiyu-admin-ch
- Please ask specific questions via chat - they will be answered via chat.
- Please ask questions that are of interest to everyone via microphone.
- We do not engage in political discussions here.

Vacancies

The e-ID department is looking for new staff

- ICT Consultant e-ID-Ecosystem Marketing
- ICT Consultant e-ID-Ecosystem Integration
- ICT Consultant Technology Scouting and Interoperability

For more information an to apply, please visit www.stelle.admin.ch

Global Digital Collaboration on Wallets and Credentials

Save the date

for the launch of the

Global Digital Collaboration

to foster wallets, credentials and trusted infrastructure
for the benefit of all humans

July 1-2, 2025

CICG Geneva, Switzerland

Hosted by the Swiss Confederation

Information about the conference

Agenda

- 1 July: Geographical and sectoral overview in plenary session
- 2 July: Deep dives in parallel in 15 different rooms
- Conference language is English

Participation

- Participation is free of charge
- Registration at www.lu.ma/gc25 via DIDAS or Digital Society

Legislation

Status and outlook

e-ID: Referendum request successful

- Overall, 55 683 signatures were submitted against the Federal Act on Electronic Identity and other Electronic Credentials (E-ID Act, BGEID). The Federal Chancellery has verified that 55 344 of these signatures are valid.
- The referendum request has therefore formally been approved.

- The Federal Council must determine the referendum topics at least four months before the date of the vote.
- The next referendum dates are 28 September and 30 November 2025.

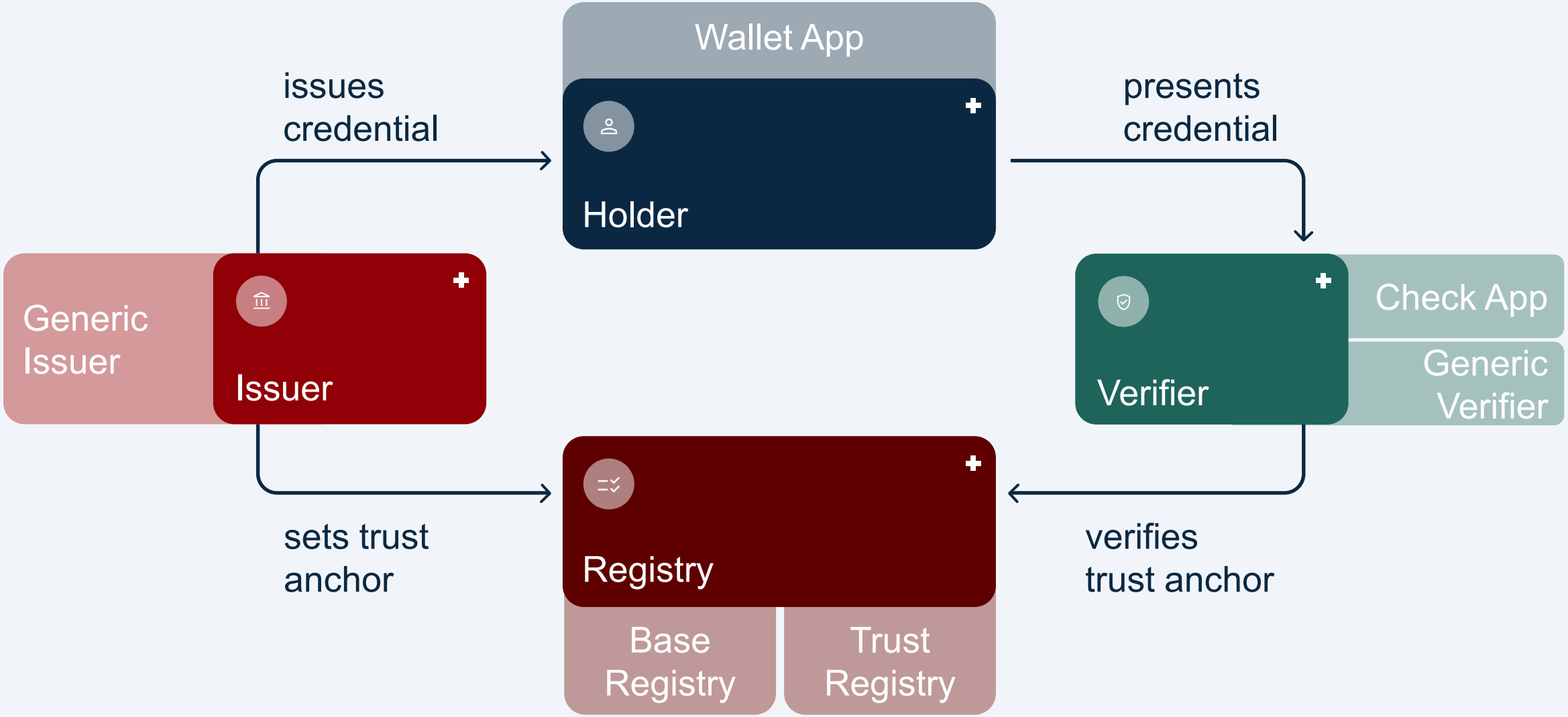
Consultation on the ordinance

- Work on the ordinance is progressing as planned.
- The consultation process for the ordinance is expected to begin before the summer break.

Public Beta

Status and outlook

Public Beta components

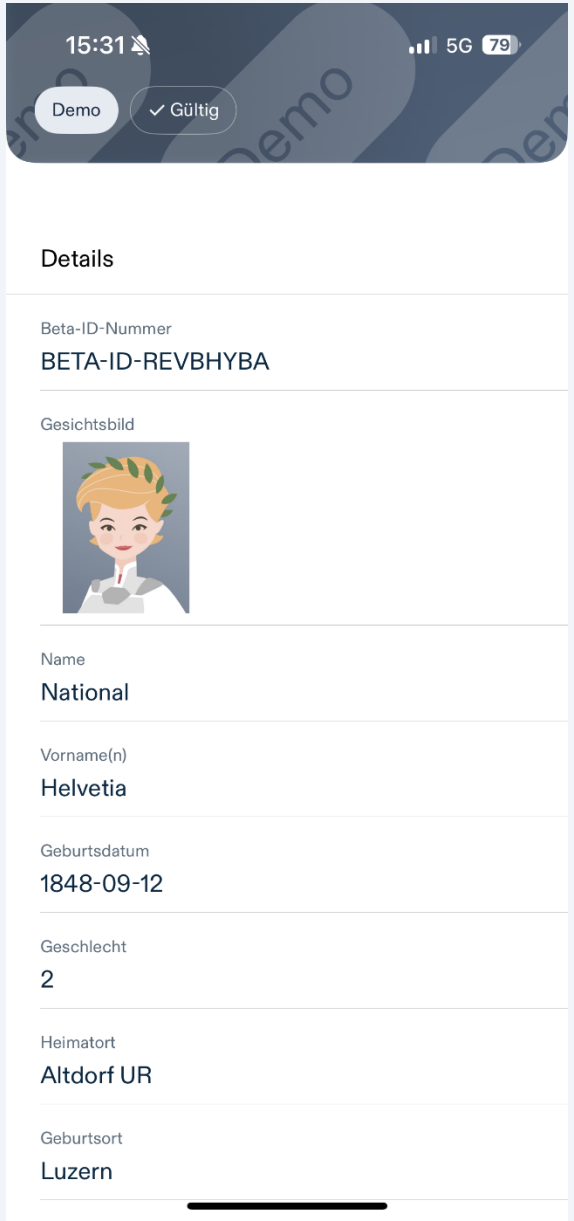


Beta-ID

- Data fields are identical to the data fields of the e-ID:
  - First name(s), surname, date of birth, older than 16/18/65, nationality, AHV number, etc.
  - Also the other data such as: Document number, verification process type, valid until, etc.

- The format of the beta ID is SD-JWT, as defined in swiss-profile (GitHub)
- Holder binding is available (hardware-binded where possible, otherwise software-binded)

- Users can define the content themselves.



Initial figures for the Public Beta

Users

- swiyu downloads: +11,000
- Beta ID issuances: +9,000
- Verification-links: +5,000
- Verifications: +1,500
- Revocations: +350
- Business-Partner on the e-Portal: +125
- Entries into the trust registry: 16

Infrastructure

- CPU usage: less than 2%

GitHub

- Generic Verifier: +450 downloads of the docker images
- Generic Issuer: +600 downloads of the docker images
- Issues and queries in the discussion forum: +30

Public Beta

Initial feedback from the private sector

Public Beta

User-testing

Unlinkable e-ID

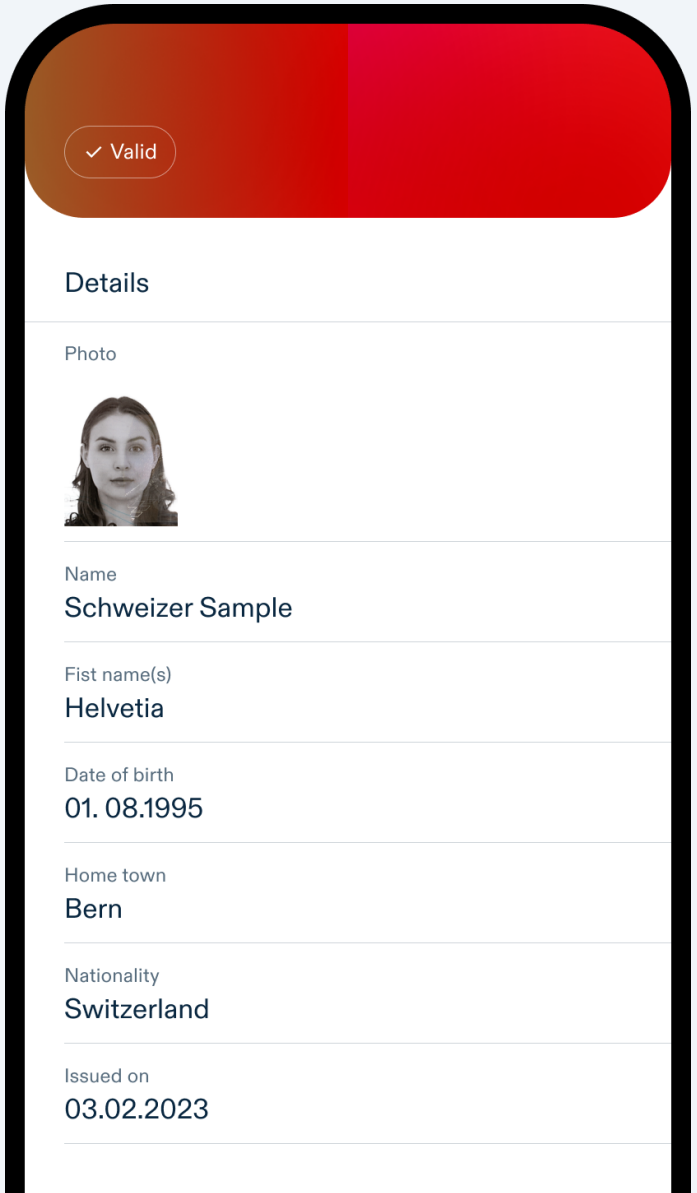
batch issuance and renewal key concept

Initial situation

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)
- This can be done using the **contents,**
  data generated during the communication setup
  or the **cryptographic data**
- Blog post on unlinkability

Content-related linkability of the e-ID



Transmitted content

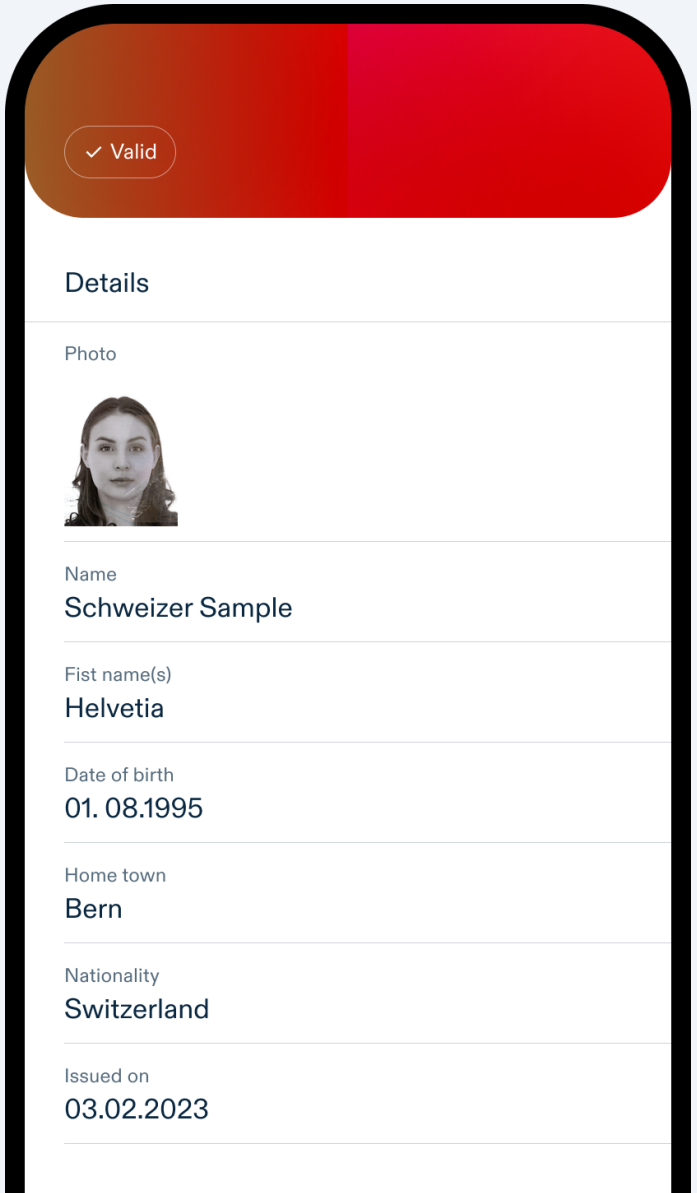
- Schweizer Sample
- Helvetia
- 01.08.1995

Technical data
(relevant for unlinkability)

- Issuer signature of the VC
- Disclosures (Salted/Hashed Claims)
- Public key of the holder
- Revocation information

Verifier

Technical data-related linkability of the e-ID



Transmitted content

- older than 18

Technical data
(relevant for unlinkability)

- Issuer signature of the VC
- Disclosures (Salted/Hashed Claims)
- Public key of the holder
- Revocation information

Even if SD-JWTs are not cryptographically linkable, **edge data** could be misused for **linking**.
Wallet users can also actively avoid fingerprinting and IP correlation.

Review of unlinkability in the e-ID programme

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
of the Federal Council

26.3.2025
linkable Beta ID to Public Beta

Technology decision December 2024

- **e-ID** to be introduced as quickly as possible
- **e-ID** should be **unlinkable** as quickly as possible
- The **introduction** of the **e-ID** is **not** linked to the **implementation** of unlinkability
- Dedicated **funds and team resources** are used to drive the topic forward

Swiss federal authorities EN

News Service Bund
The portal of the Swiss government

Published on 6 December 2024

e-ID: Federal Council takes decision on technical implementation

Bern, 6.12.2024 - 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.

The introduction of the new federal e-ID is currently planned for 2026. In order to meet this schedule, the federal government is already working on the technical implementation, which involves both developing the e-ID and creating the trust infrastructure necessary to operate it. At its meeting on 6 December, the Federal Council defined the principles for its technical implementation.

Go-Live e-ID 2026

From launch: unlinkable e-ID thanks to batch issuance

By issuing several VCs with the same appearance (batch issuance), cryptographic unlinkability is made possible **from the introduction** of the e-ID.

! Linkability on the basis of proven attributes or marginal data cannot be prevented.

Key points of batched e-ID-VCs

e-ID-VC validity:	Validity of the underlying identity document or max. 5 years
Batch size:	25 e-ID VCs per batch
Batch VC utilisation:	• One-time use, automated subscription of additional e-ID-VCs after consent • Incidental use, in the event of refused consent or failed renewal
Purchase of a new batches:	If there are still 2 unused proofs in the wallet
Revocation:	Obtaining a new batch does not lead to revocation → only a new successful e-ID application leads to revocation of all e-ID VCs If possible, revoke the e-ID of several persons together (herd revocation)

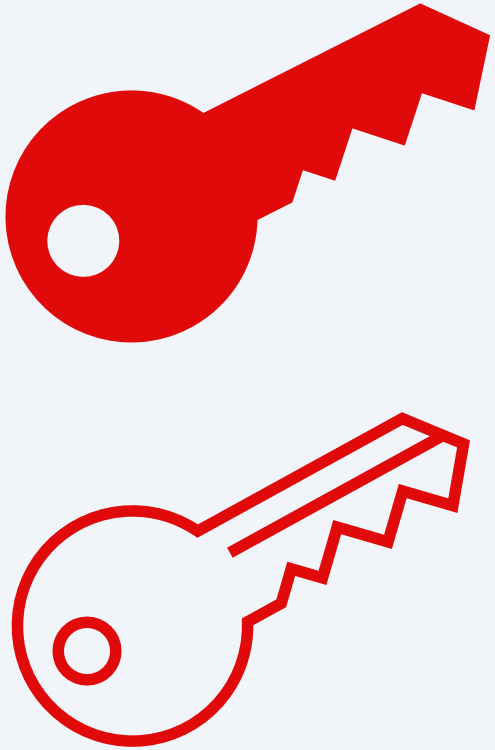
Renewal key concept

Commitment to the owner

- When the e-ID VCs are "used up", the holder or the wallet should be able to **obtain** a **new batch**.
- This means that a **secure connection** must again **be established** between the wallet and the issuer of the e-ID (fedpol).
- When the e-ID is first issued, the **identification of the person** (online or at the counter) is an important element to ensure the link to the correct holder.
- The **renewal key concept** addresses the collection of new e-ID VCs with continued secure binding to the holder

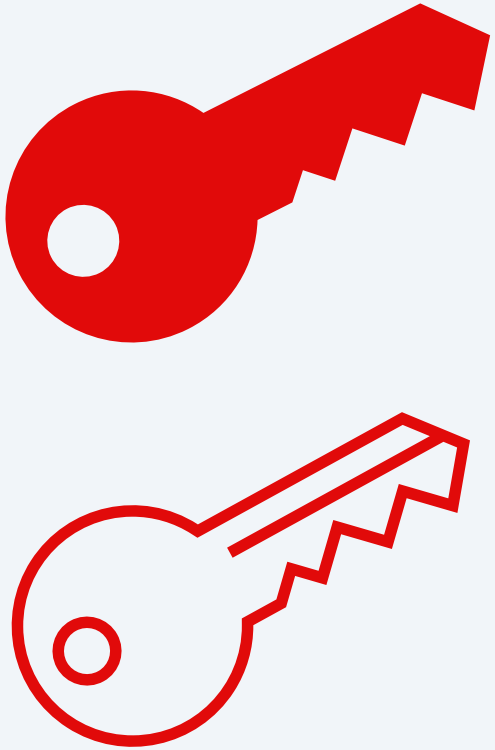
Renewal Key

- **Key pair bound to the holder** (hardware bound) for authentication
- **Exclusively for obtaining additional e-ID VCs.**
- The **public key is recorded by fedpol** when the first e-ID is issued
- The key pair is **not part of the e-ID-VCs**



Why Renewal Key?

- **Enables the purchase of a new batch with a secure bond to the existing owner**
- Generated by Wallet during initial issue and checked by issuer
- No degradation through presentation to other verifiers
- Option to separate the validity period between the renewal cycle and VC validity



Using the Renewal Key

First issue

Binding keys

Renewal key

Issuer key

e-ID

Name: **Alice**

Geburtsdatum: **01.01.1975**

Über 18: **Ja**

Nationalität: **Schweiz**

Binding Public Key:

Ausstellersignatur: **Fedpol**

Signatur der Challenge

e-ID

Name: **Alice**

Geburtsdatum: **01.01.1975**

Über 18: **Ja**

Nationalität: **Schweiz**

Binding Public Key:

Ausstellersignatur: **Fedpol**

Signatur der Challenge

Batch renewal

Renewal

Binding keys

Renewal key

Issuer key

e-ID

Name: **Alice**

Geburtsdatum: **01.01.1975**

Über 18: **Ja**

Nationalität: **Schweiz**

Binding Public Key:

Ausstellersignatur: **Fedpol**

Signatur der Cha

e-ID

Name: **Alice**

Geburtsdatum: **01.01.1975**

Über 18: **Ja**

Nationalität: **Schweiz**

Binding Public Key:

Ausstellersignatur: **Fedpol**

Signatur der Challenge

Renewal key expiry

Reissue

Binding keys

Renewal key

Issuer key

e-ID

Name: **Alice**

Geburtsdatum: **01.01.1975**

Über 18: **Ja**

Nationalität: **Schweiz**

Binding Public Key

Ausstellersignatur: **Fedpol**

Signatur der Cha

e-ID

Name: **Alice**

Geburtsdatum: **01.01.1975**

Über 18: **Ja**

Nationalität: **Schweiz**

Binding Public Key:

Ausstellersignatur: **Fedpol**

Signatur der Challenge

...

Batch renewal

Cryptographic material used

OWNER

Binding of proof				
Secret Key	**Public Key**	**Key Type**	**Key Attestation***	**Signature (of issuer)**
sk_i	pk_i	ECDSA (NIST p-256)	ka_i	sig_i

Renewal			
Secret Key	**Public Key**	**Key Type**	**Key Attestation***
sk_{renew}	pk_{renew}	ECDSA (NIST p-256)	ka_{renew}

EXHIBITORS

Proof of signature		
Secret Key (HSM)	**Public Key**	**Key Type**
sk_{Bund}	pk_{Bund}	EdDSA (Ed448)

Key Attestations are not supported by iOS. Instead, an app attestation will be used, for which the app must be certified by the federal government.

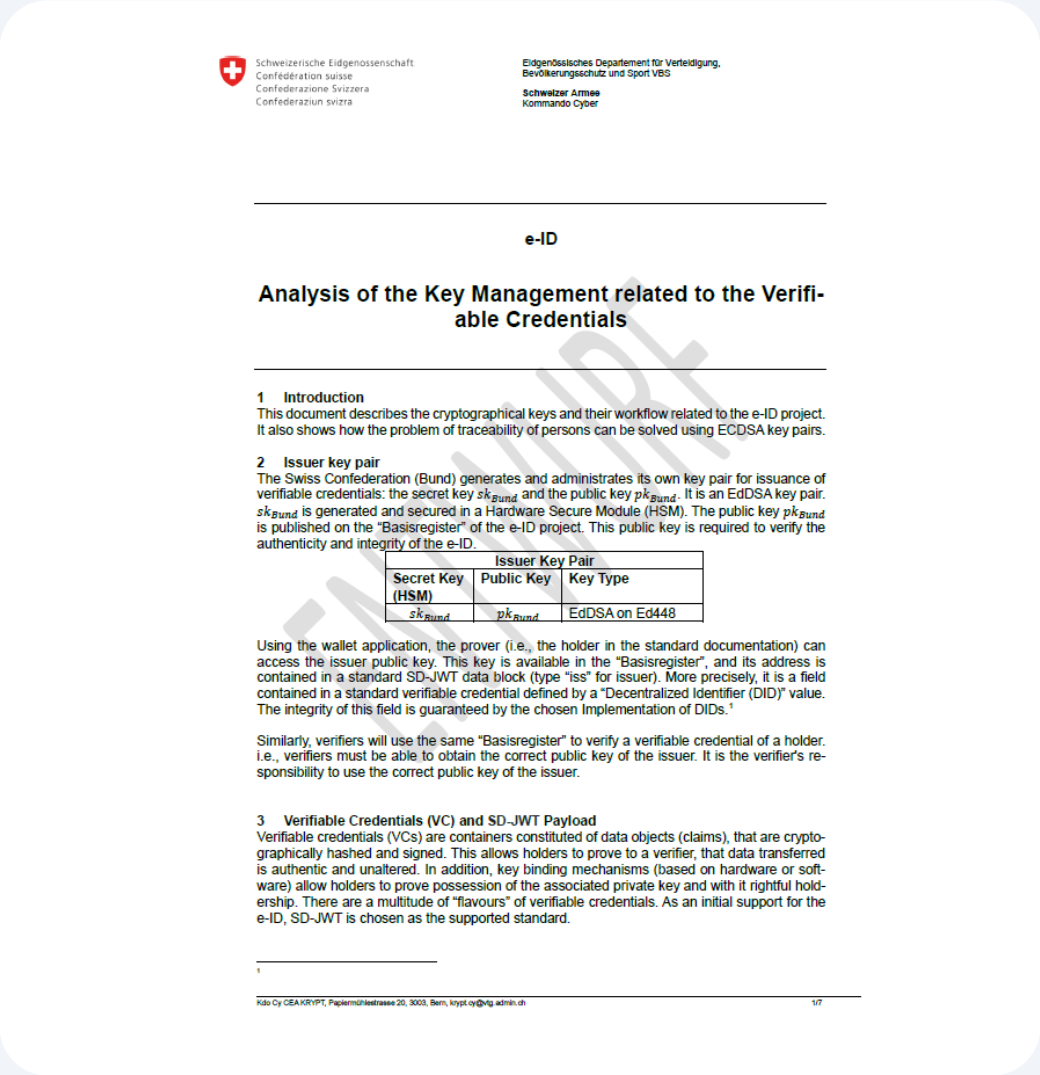
Procedure for the initial issue of an e-ID

1) Wallet generates keys for binding $(\boldsymbol{sk_i}/\boldsymbol{pk_i})$ and renewal $(\boldsymbol{sk_{renew}}/\boldsymbol{pk_{renew}})$. Keys are generated in the Secure Enclave and are therefore bound to the end device
2) Wallet sends "Proofs of Possession" (for $\boldsymbol{sk_i}$ and $\boldsymbol{sk_{renew}}$) and "Key Attestations" ($\boldsymbol{ka_i}$ for $\boldsymbol{pk_i}$ and $\boldsymbol{ka_{renew}}$ for $\boldsymbol{pk_{renew}}$) and a $\boldsymbol{pk_{renew}}$ to the issuer to prove the key binding to the hardware
3) Identification of the holder through identity verification (online, at the counter)
4) Issuer verifies "Proofs of Possession" and "Key Attestations" and defines the attributes (e.g. validity). She signs the $\boldsymbol{JWT_{renew}}$ and sends it to the holder
5) Issuer generates e-ID VCs (salted-hash procedure) and binds them to the wallet ($\boldsymbol{pk_i}$ as an attribute in the VC)

Batch reference process

1) Wallet generates **new** "Binding" key pair(s) ($\boldsymbol{sk_{i+1}}/\boldsymbol{pk_{i+1}}$)
2) Wallet transmits "Proofs of Possession" (for $\boldsymbol{sk_{i+1}}$ and $\boldsymbol{sk_{renew}}$), "Key Attestations" ($\boldsymbol{ka_{i+1}}$ and $\boldsymbol{ka_{i+1}}$) and $\boldsymbol{ka_{i+1}}$ to issuer to authenticate wallet and prove binding of keys to hardware
3) Issuer verified, $\boldsymbol{ka_{i+1}}$, "Proofs of Possessions" and "Key Attestations"
4) Issuer generates e-ID VCs (salted-hash procedure) and binds them to the wallet ($\boldsymbol{pk_{i+1}}$ as an attribute in the VC)

Further details will be published on GitHub



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Schweizer Armee
Kommando Cyber

e-ID

Analysis of the Key Management related to the Verifiable Credentials

1 Introduction

This document describes the cryptographical keys and their workflow related to the e-ID project. It also shows how the problem of traceability of persons can be solved using ECDSA key pairs.

2 Issuer key pair

The Swiss Confederation (Bund) generates and administrates its own key pair for issuance of verifiable credentials: the secret key sk_{Bund} and the public key pk_{Bund}. It is an EdDSA key pair. sk_{Bund} is generated and secured in a Hardware Secure Module (HSM). The public key pk_{Bund} is published on the "Basisregister" of the e-ID project. This public key is required to verify the authenticity and integrity of the e-ID.

Issuer Key Pair		
Secret Key (HSM)	**Public Key**	**Key Type**
sk_{Bund}	pk_{Bund}	EdDSA on Ed448

Using the wallet application, the prover (i.e., the holder in the standard documentation) can access the issuer public key. This key is available in the "Basisregister", and its address is contained in a standard SD-JWT data block (type "iss" for issuer). More precisely, it is a field contained in a standard verifiable credential defined by a "Decentralized Identifier (DID)" value. The integrity of this field is guaranteed by the chosen Implementation of DIDs.[1]

Similarly, verifiers will use the same "Basisregister" to verify a verifiable credential of a holder. i.e., verifiers must be able to obtain the correct public key of the issuer. It is the verifier's responsibility to use the correct public key of the issuer.

3 Verifiable Credentials (VC) and SD-JWT Payload

Verifiable credentials (VCs) are containers constituted of data objects (claims), that are cryptographically hashed and signed. This allows holders to prove to a verifier, that data transferred is authentic and unaltered. In addition, key binding mechanisms (based on hardware or software) allow holders to prove possession of the associated private key and with it rightful holdership. There are a multitude of "flavours" of verifiable credentials. As an initial support for the e-ID, SD-JWT is chosen as the supported standard.

[1]

Kdo Cy CEA KRYPT, Papiermühlestrasse 20, 3003, Bern, krypt.cy@vtg.admin.ch 1/7

Q & A

Questions from the audience

Executive Summary in English

6 pm

Next participation meeting

Thursday, 05.06.2025 4 pm

Thank you for your attention!

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

Links

General information on the e-ID
www.eid.admin.ch

Information on e-ID legislation
www.bj.admin.ch
www.parlament.ch

Discussion platform on the e-ID
www.github.com

Subscribe to the e-ID newsletter
www.eid.admin.ch